ვ. ადამია, ნ. არაბული, ზ. ცირამუა

კომპიუტერული ქსელები

(I ნაწილი)

„ტექნიკური უნივერსიტეტი”

საქართველოს ტექნიკური უნივერსიტეტი

ვ. ადამია, ნ. არაბული, ზ. ცირამუა

კომპიუტერული ქსელები

(I ნაწილი)

დამტკიცებულია სტუ-ს
სარედაქციო-საგამომცემლო საბჭოს
მიერ. 29.04.2009, ოქმი №4

თბილისი
2009

წიგნი წარმოადგენს სახელმძღვანელოს ”კომპიუტერულ ქსელებში”, რომლის მიზანია სტუდენტებს მისცეს ცოდნა და უნარ-ჩვევები კომპიუტერულ სისტემებსა და ქსელებში პროფესიული საქმიანობისათვის, ასევე მისცეს ბაზისური წარმოდგენა კომპიუტერული ქსელებზე იმ სტუდენტებს, რომლებიც სწავლობენ ინფორმაციული ტექნოლოგიების სპეციალობით ან ნებისმიერ პირს ვინც აპირებს კომპიუტერული ქსელის შესწავლას.

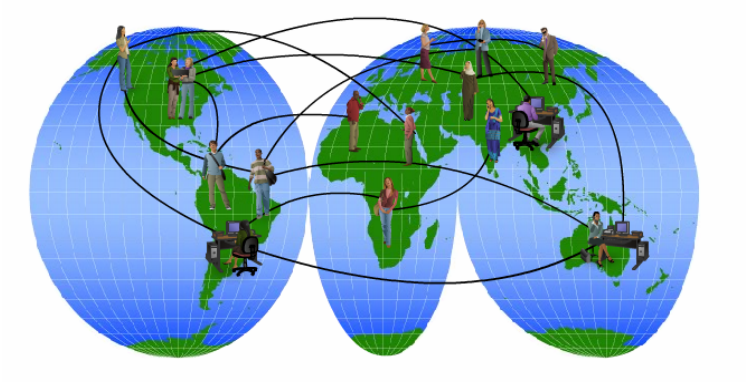
რეცენზენტი: პროფ. ი. მიქაძე

ISBN 978-9941-14-646-6 (ყველა ნაწილი)
ISBN 978-9941-14-647-3 (პირველი ნაწილი)
http://www.gtu.ge/publishinghouse/

შესავალი

კომპიუტერული ქსელების საფუძვლები

ადამანებს შორის კომუნიკაცია მნიშვნელოვან როლს თამაშობს მათ ცხოვრებაში. მათ სჭირდებათ მიიღონ ინფორმაცია ერთმანეთზე, ახალ ამბებზე, ამინდზე, ფინანსურ მაჩვენებლებზე და ა.შ. ინფორმაციის მიღების და გადაცემის მეთოდები იცვლებოდა და ვითარდებოდა წლების განმავლობაში. ინფორმაციულ საუკუნეში რომელშიც ჩვენ ვცხოვრობთ ინფორმაციის დროული მიღება და ფლობა უდიდესად მნიშვნელოვანია. ამიტომ ინფორმაციის მიღებასა და გადაცემაში კომპიუტერული ქსელი უმნიშვნელოვანეს როლს თამაშობს. კომპიუტერული ქსელი ეხმარება ადამიანებს უსწრაფესად გადასცენ ინფორმაცია მსოფლიოს ნებისმიერ ადგილას.



ნახაზი 1. კომუნიკაცია ადამანებს შორის

მსოფლიოში მონაცემების გადაცემა გახდა კომპიუტერული სისტემების ფუნდამენტური ნაწილი. კომპიუტერული ტექნო-

ლოგიების სწრაფმა განვითარებამ მოითხოვა კომპიუტერული სისტემების საიმედო, სწრაფი და დაცული კავშირების უზრუნველყოფა. ამიტომ კომპიუტერული ქსელების დაპრო-ექტების, აგების და მართვის სისტემები მნიშვნელოვან როლს თამაშობს თანამედროვე ინფორმაციულ ტექნოლოგიებში.

სახელმღვანელოს პირველ ნაწილში განხილული იქნება კომპიუტერული ქსელების აგების პრინციპები, კერძოდ კოპიუტერულ ქსელების ტიპები, ტოპოლოგიები, ტექნოლოგიები, ქსელური პროტოკოლები, ადრესაცია.

ქსელების ისტორია

ქსელური ურთიერთქმედების კონცეფციის შექმნასთან დაკავშირებით, თეორიული სამუშაოები პირველი გამომთვლელი მანქანების გამოჩენისთანავე დაიწყო, მაგრამ პრაქტიკულად შედეგების მიღება მხოლოდ გასული საუკუნის 60-იანი წლების ბოლოს მოხერხდა, როდესაც გლობალური ქსელებისა და პაკეტური კომუნიკაციის ტექნოლოგიის საშუალებით შესაძლებელი გახდა ე.წ. სუპერკომპიუტერების ანუ Mainframe კლასის გამოთვლითი მანქანების ურთიერთ დაკავშირება, რამაც მათი ეფექტიურობა მნიშვნელოვნად გაზარდა.

1969 წელს აშშ-ის თავდაცვის სამინისტრომ თავდაცვითი და სამეცნიერ-კვლევითი ცენტრების სუპერკომპიუტერების ერთ საერთო ქსელში გაერთიანების იდეის განხორციელება დაიწყო. ქსელის სახელწოდება გახლდათ ARPANET და სწორედ ეს გახდა პირველი და ყველაზე გავრცელებული გლობალური ქსელის - ინტერნეტის შექმნის საფუძველი.

1974 წელს კომპანია IBM სუპერკომპიუტერებისთვის ქსელური არქიტექტურის შექმნის შესახებ განაცხადა, რომელსაც სისტემური ქსელური არქიტექტურა ანუ SNA ეწოდა. ამავდროულად, ევროპაში სტანდარტების საერთაშორისო ორგანიზაციის (ISO) მიერ აქტიურად მიმდინარეობდა ე.წ. X.25 ქსელების შექმნის და სტანდარტიზირების სამუშაოები. ამგვარად, მომხმარებლის წინაშე პირველად მონაცემთა გადაცემის გლობალური ქსელები წარდგნენ, რომლებიც დიდ ტერიტორიებზე განლაგებულ კომპიუტერებს აერთიანებდნენ.

პირველი გლობალური ქსელების შექმნის მთავარი მიღწევა, იმ დროისთვის, ფართოდ გავრცელებული არხების კომუტაციის პრინციპებზე უარის თქმა გახლდათ, რომლის გამოყენებაც ათწლეულების მანძილზე წარმატებით ხორციელდებოდა სატელეფონო ქსელებში. ექსპერიმენტებმა და მათემატიკურმა მოდელირებამ აჩვენა, რომ პულსირებადი ხასიათის მქონე კომპიუტერული ტრაფიკის გადაცემა გაცილებით უფრო ეფექტურად ხორციელდება ისეთი ქსელების საშუალებით, რომლებშიც პაკეტური კომუტაციის პრინციპი გამოიყენება. ამ დროს მონაცემები იყოფა მცირე ზომის ნაწილებად, ანუ პაკეტებად. ყოველ პაკეტში საბოლოო დანიშნულების ჰოსტის მისამართია გაწერილი და ამის შედეგად ისინი დამოუკიდებლად გადაადგილდებიან ქსელში დანიშნულების ადგილისკენ.

იმის გამო, რომ მაღალხარისხიანი კავშირის ხაზების დიდ მანძილებზე მონტაჟი მნიშვნელოვან ხარჯებთან იყო დაკავში-რებული, წლების განმავლობაში გლობალური კომპიუტერული ქსელებისთვის გამოიყენებოდა არსებული სატელეფონო ხაზები. ასეთ არხებში მონაცემთა გადაცემის სიჩქარე 10-15კბ/წმ-ში არ აღემატებოდა და ამიტომ ასეთი გლობალური ქსელების

მომსახურებები, ძირითადად, მცირე ზომის ფაილებისა და ელფოსტის მიმოცვლით შემოიფარგლებოდა. გარდა მონაცემთა გადაცემის დაბალი სიჩქარისა, ასეთ ქსელებს კიდევ სხვა ნაკლიც ჰქონდათ, კერძოდ, გადაცემული სიგნალების მნიშვნელოვანი დამახინჯება.

გლობალური კომპიუტერული ქსელების ტექნოლოგიის განვითარება ბევრადაა დამოკიდებული სატელეფონო ქსელის პროგრესზე. 60-იანი წლების ბოლოსთვის სატელეფონო ქსელებში სულ უფრო მომრავლდა ხმის ციფრულ ფორმატში გადაცემის ტექნოლოგიის გამოყენების მაგალითები, რის გამოც შემუშავებული იქნება ნახევრადსინქრონული ციფრული იერარქია - PDH (ხმის და მონაცემთა გადაცემის ციფრული მეთოდი, დაფუძნებული არხის დროითი დაყოფის პრინციპზე და სიგნალის იმპულსურ-კოდური მოდულაციის საშუალებით წარმოდგენის ტექნოლოგიაზე), რომელიც მონაცემთა გადაცემას 140 მგბ/წმ-მდე სიჩქარით უზრუნველყოფდა. მოგვიანებით, 80-იანი წლების მიწურულს, გამოჩნდა სინქრონული ციფრული იერარქიის ტექნოლოგია SDH (განეკუთვნება, ოპტიკურ-ბოჭკოვანი არხების მეშვეობით, მონაცემთა გადაცემის ტექნოლოგიებს, რომელიც უზრუნველყოფს სხვადასხვა მოცულობის ციფრული სიგნალის გადაცემას), რომელმაც პრაქტიკულად მთლიანად ჩაანაცვლა წინამორბედი პლეზიქრონული ციფრული იერარქია და ციფრული არხების სიჩქარული დიაპაზონი 10გბ/წმ-მდე გააფართოვა.

დღეს, მონაცემთა გადაცემის გლობალური ქსელები, მრავალფეროვნებითა და მომსახურების ხარისხით ლოკალურ ქსელებს გაუტოლდნენ, რომლებიც, მიუხედავათ იმისა რომ

გაცილებით უფრო გვიან გამოჩნდნენ, დიდი ხნის მანძილზე ინარჩუნებდნენ მოწინავე პოზიციებს

ლოკალური ქსელების სტანდარტული ტექნოლოგიები გასული საუკუნის 80-იანი წლების შუა პერიოდში გამოჩნდა. კომპიუტერების ლოკალურ ქსელებში გააერთიანეს სტანდარტული ტექნოლოგიები, რომელთა საშალებითაც მცირე ზომის ტერიტორიაზე განლაგებული კომპიუტერების ერთმანეთთან დაკავშირება მოხერხდა. მათ შორის იყო: Ethernet, Arenet, Token Ring, Token Bus და ცოტა მოგვიანებით, FDDI.

ლოკალური ქსელების ყველა სტანდარტული ტექნოლოგია დაფუძნებული იყო პაკეტების კომუტაციის პრინციპზე, რომელმაც წარმატებით დაამტკიცა თავისი უპირატესობა გლობალურ ქსელებში მონაცემთა გადაცემის დროს.

სტანდარტული ქსელური ტექნოლოგიების გამოჩენამ ლოკალური ქსელის გაშენების ამოცანა მნიშვნელოვნად გაამარტივა. ამისთვის საჭირო იყო მხოლოდ შესაბამისი სტანდარტული ქსელური ადაპტერის, მაგალითად Erthernet და კაბელის შეძენა, შემდგომ კაბელის და ადაპტერების ერთმანეთთან მიერთება სტანდარტული გადამყვანების მეშვეობით და კომპიუტერზე სპეციალური ქსელური ოპერაციული სისტემის დაყენება (მაგ.:Novell Net Ware). ამის შემდეგ ქსელი ფუნქციონირებას იწყებდა და ყოველი ახალი კომპიუტერის შემდგომი მიერთება შეფერხებას არ იწვევდა.

90-იანი წლების მიწურულს, ლოკალური ქსელების ტექნოლოგიებს შორის, გამოვლინდა აშკარა ლიდერი Erthernet ტექნოლოგიების ოჯახი, რომელშიც შედიოდნენ: კლასიკური Erthernet ტექნოლოგია მონაცემთა გადაცემის 10გბ/წმ სიჩქარით;

100მგბ/წმ სიჩქარიანი Fast Erthernet ტექნოლოგია და Gigabit Erthernet ტექნოლოგია, რომელიც 1000მგბ/წმ სიჩქარეს უზრუნველყოფს. Erthernet ტექნოლოგიის ასეთი წარმატება შეიძლება აიხსნას რამდენიმე მიზეზით: პირველ რიგში, ტექნოლოგიების მუშაობის მარტივმა ალგორითმებმა, Ethernet ტექნოლოგია მუშაობის პრინციპების მიხედვით, ძალიან ახლოსაა ერთმანეთთან, რაც მნიშვნელოვნად ამარტივებს მათ ბაზაზე აგებული ქსელების მომსახურებასა და ერთმანეთთან ინტეგრირებას.

კომპიუტერული ქსელების განვითარების ისტორია გასული საუკუნის 80-იანი წლების დასაწყისში კიდევ ერთ მნიშვნელოვან მოვლენასთანაა დაკავშირებული. შეიქმნა პირველი პერსონალური კომპიუტერები (PC). ეს მოწყობილებები იდეალურ ელემენტებს წარმოადგენენ ლოკალური კომპიუტერული ქსელების შექმნისთვის. ერთი მხრივ, მათი სიმძლავრე საკმარისი იყო ქსელური პროგრამული უზრუნველყოფის მუშაობისთვის, მეორე მხრივ კი, რთული ამოცანების დამუშავების დროს აშკარად ჩანდა მათი გამოთვლითი სიმძლავრეების გაერთიანების საჭიროება. გარდა ამისა, საჭირო იყო ძვირადღირებული ბეჭდვითი მოწყობილობებისა და დიდი მოცულობის ინფორმაციის საცავების საერთო გამოყენების პრობლემის გადაწყვეტა. პერსონალურმა კომპიუტერებმა ფართო გავრცელება პოვეს ლოკალურ სამომხმარებლო ტერმინალების გამოყენების ადგილებში და ინფორმაციის შენახვა-დამუშავების ცენტრებში, ანუ ქსელური სერვერების ფუნქციებიც შეითავსა, რითაც მნიშვნელოვნად შეარყია ერთ დროს გაბატონებული სუპერკომპიუტერების პოზიციები.

პერსონალური კომპიუტერების გამოჩენამ მძლავრი კატალიზატორის როლი შეასრულა ლოკალური ქსელების სწრაფი განვითარების საქმეში, რომელთა ერთმანეთთან დაკავშირების საკითხი ძალზე აქტუალური გახდა მომდევნო წლებში. მნიშვნელოვანია ის ფაქტიც, რომ ყველა TCP/IP პროტოკოლების ოჯახში კომპიუტერულ ქსელებზე საუბრის დროს TCP/IP ქსელური პროტოკოლების ოჯახისთვის გვერდის ავლა შეუძლებელია. ქსელური პროტოკოლების ეს ოჯახი აშშ-ის თავდაცვის სამინისტროს შეკვეთით შეიქმნა გასული საუკუნის 70-იანი წლების მიწურულს და დღეს მსოფლიოში ყველაზე გავრცელებულია. მისი საშუალებით ინტერნეტის ქსელში ერთმანეთთან 100 მილიონზე მეტი კომპიუტერია დაკავშირებული. მართალია, TCP/IP პროტოკოლების ოჯახი განუყოფლადაა დაკავშირებული ინტერნეტის ქსელთან, მაგრამ არსებობს მრავალი ლოკალური, კორპორატიული და ტერიტორიული ქსელები, რომლებიც უშუალოდ ინტერნეტის ნაწილს არ წარმოადგენენ და კომუნიკაციისთვის TCP/IP პროტოკოლების ოჯახს იყენებენ. იმისთვის, რომ ეს ქსელები ერთმანეთისგან განასხვავონ, მათ TCP/IP ან, უბრალოდ, IP ქსელებს უწოდებენ. TCP/IP პროტოკოლების ოჯახის სახელი მისი შემადგენელი ორი ძირითადი TCP და IP პროტოკოლების სახელწოდებიდან გამომდინარეობს. IP, ანუ ინტერნეტ პროტოკოლი უზრუნველყოფს ქსელში კომპიუტერებს შორის პაკეტების გადაცემას, ხოლო TCP, ანუ გადაცემის კონტროლის პროტოკოლი, ქსელში ამ პაკეტების გადაცემის სანდოობას და საჭირო თანმიმდევრობას უზრუნველყოფს.

არსებობის მრავალი წლის მანძილზე TCP/IP პროტოკოლების ოჯახმა დამატებითი პროტოკოლების დიდი რაოდენობა გააერთიანა. მათ რიცხვს განეკუთვნებიან ისეთი პოპულარული

პროტოკოლები, როგორებიცაა: ფაილების გადაცემის პროტოკოლი FTP; ვირტუალური ტერმინალის პროტოკოლი Telnet; ელექტრონული ფოსტის გადაცემის პროტოკოლი SMTP; ჰიპერტექსტური პროტოკოლები WWW და მრავალი სხვა. იმის გამო, რომ TCP/IP პროტოკოლების ოჯახი, თავდაპირველად შემუშავებული იყო ინტერნეტის ქსელში გამოსაყენებლად, მას უამრავი განსაკუთრებული თვისება აქვს, რაც მას უპირატესობას აძლევს სხვა ქსელურ პროტოკოლებთან შედარებით. განსაკუთრებით, როდესაც საუბარია გლობალიური ქსელების შექმნაზე. ამ პროტოკოლის ძალზე მოსახერხებელ თვისებას მონაცემთა პაკეტების ხელახალი ფრაგმენტირების საშუალება წარმოადგენს. ხშირად დიდი გლობალური ქსელი რამდენიმე უფრო მცირე ზომის ქსელებისაგან შედგება. სხვადასხვა შემადგენელ ქსელში გადაცემული პოაკეტების მაქსიმალური ზომა შეიძლება ერთმანეთისგან განსხვავდებოდეს. ასეთ შემთხვევაში, ერთი ქსელიდან მეორეში გადასვლისას, შეიძლება დადგეს გადაცემული პაკეტის რამდენიმე ნაწილად დაშლის აუცილებლობა, რასაც TCP/IP შემადგენელი IP პროტოკოლი ეფექტურად უზრუნველყოფს.

TCP/IP ტექნოლოგიის კიდევ ერთ განსაკუთრებულ თვისებას წარმოადგენს მისამართების მოქნილი სისტემა, რაც ანალოგიური დანიშნულების სხვა პროტოკოლებთან შედარებით, სხვადასხვა ტექნოლოგიებზე აგებული ქსელების გაერთიანებას უფრო მარტივს ხდის. ეს თვისება, აგრეთვე, ხელს უწყობს TCP/IP ტექნოლოგიის გამოყენებას დიდი ჰეტეროგენული ქსელების (ქსელი, რომელშიც სხვადასხვა ოპერაციული სისტემებსა და ოქმებზე მომუშავე კომპიუტერებია გაერთიანებული) შექმნის დროს.

კომპიუტერულმა ქსელებმა არსებობის მანძილზე განვითარების დიდი გზა განვლო. სპილენძის მავთულები ჩაანაცვლა ოპტიკურ-ბოჭკოვანმა კაბელმა. გამოჩნდა მონაცემთა გადაცემის უსადენო სისტემები. ეს განვითარება გრძელდება და არავინ იცის, თუ როგორი იქნება მონაცემთა გადაცემის სისტემები, თუნდაც 2-3 წლის შემდეგ. დაბეჯითებით მხოლოდ ერთის თქმა შეიძლება - მომავალში მონაცემების გადაცემა კომუნიკაციის ინდუსტრიის ერთ-ერთი ყველაზე მნიშვნელოვანი ნაწილი იქნება და ამის საფუძველი უკვე დღეს არსებობს.

კომუნიკაცია კომპიუტერულ ქსელებში

შესაძლელობა იმისა, რომ ურთიერთობა დაამყარო ვინმესთან შორ მანძილზე საკმაოდ მნიშვნელოვანია დღევანდელ პირად და საქმიან ცხოვრებაში. იმისათვის რომ მოხდეს ადაიანებს შორის ინფორმაციის უშეცდომო და სწრაფი გადაცემა მთელ მსოფლიოში, საჭიროა დავეყრდნოთ საინფორმაციო ქსელებს. საინფორმაციო ქსელები ერთმანეთისაგან განსხვავდებიან სხვადასხვა შესაძლებლობებით, მაგრამ ყველა ქსელს გააჩნია ოთხი ძირითადი საერთო ელემენტი:

1. წესები (პროტოკოლი), თუ როგორ უნდა მოხდეს ინფორმაციის გაგზავნა და მიღება;

2. ინფორმაცია ან ინფორმაციის ერთეული, რომელიც იგზავნება ერთი მოწყობილობიდან მეორეში;

3. მედია საშუალება, რომლითაც ხდება ამ მოწყო-ბილობების დაკავშირება;

4. ქსელური მოწყობილობები, რომლებიც ცვლიან ერთმანეთთან ინფორმაციას.

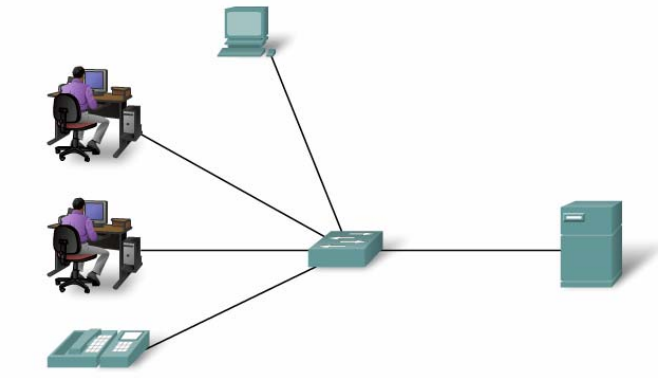
ნახაზი 2. ქსელში საკომუნიკაციო საშუალებები

კომპიუტერული ქსელი წარმოადგენს ურთიერთდაკავშირებულ და შეთანხმებულად ფუნქციონირებად პროგრამული და აპარატურული კომპონენტების რთულ კომპლექსს.

ის არის კომპიუტერების და პერიფერიული მოწყობილობების ერთიანობა, რომლებსაც სპეციალური საკომუნიკაციო საშუალებების და პროგრამული უზრუნველყოფის საშუალებით შეუძლიათ ინფორმაციის გაცვლა.

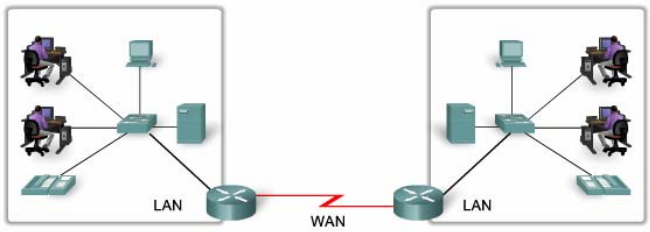
კომპიუტერულ ქსელში კომპიუტერების რაოდენობა ორიდან რამდენიმე ათასამდე შეიძლება იცვლებოდეს. კომპიუტერების რაოდენობისა და ქსელის ზომის მიხედვით არსებობს ლოკალური (LAN) და ფართო არის ქსელი (WAN).

ლოკალურ ქსელში კომპიუტერების და პერიფერიული მოწყობილობების რაოდენობა შეზღუდულია. ისინი განლაგებულნი არიან შემოსაზღვრულ არეზე.



ნახაზი 3. ლოკალური ქსელი

”ფართო არის ქსელი” არის ქსელი, რომელიც აერთიანებს რამოდენიმე ლოკალურ ქსელს ერთმანეთთან გეოგრაფიულად დაშორებულ ადგილებში. ფართო არის ქსელში კომპიუტერების რაოდენობა რამდენიმე ათასმდე შეიძლება იცვლებოდეს. ისინი სხვადასხვა ქალაქებსა და სახელმწიფოებშიც კი შეიძლება იყვნენ განლაგებულნი. ყველაზე გავრცელებული ფართო არის ქსელია inEtherneto. ფართო არის ქსელები ძირითადად აგებულნი არიან სატელეფონო და ოპტიკურ-ბოჭკოვანი ხაზების გამოყენებით.

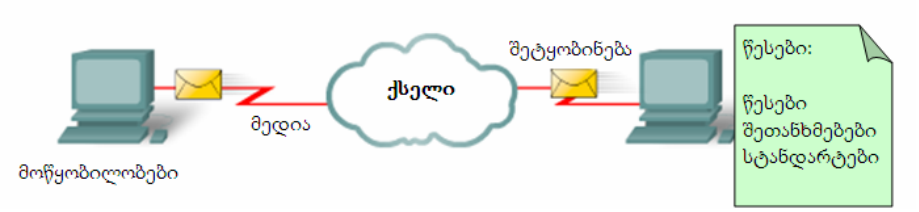


ნახაზი 4. გლობალური ქსელი

კომპიუტერული ქსელების ძირითადი დანიშნულებაა - ქსელში ჩართული ყველა კომპიუტერისათვის რესურსების შეთავსებით გამოყენება და მუდმივი კავშირი რეალურ დროში. რესურსები ესაა მონაცემები, პროტოკოლები და პერიფერიული მოწყობილობები.

კომპიუტერული ქსელის ელემენტები

სურათზე მოცემულია კომპიუტერული ქსელის ელემენტები რომლებიც მონაწილეობენ კომუნიკაციაში. იგი შეიცავს: მოწყობილობებს, მედიას (საშუალება რითაც ხედება მონაცემების გადაცემა ფიზიკურ გარემოში), რომლებიც ერთმანეთთან მუშაობენ გარკვეული წესების დაცვით, იმისათვის, რომ მოხდეს ინფორმაციის მიღება და გადაცემა.



ნახაზი 5. ინფორმაციის გადაცემა ქსელში

ინფორმაციის გადაცემა ხდება სხვადასხვა ტიპის კომპიუტერებიდან. მაგ. PC, laptop, სერვერი, IP ტელეფონი.

ეს მოწყობილობები ლოკალურ ქსელში ერთმანეთთან დაკავშირებულია (მედია საშუალებით) რადიო ან საკომუნიკაციო ხაზებით.

მოწყობილობებს, რომლებიც ერთმანეთთან არიან დაკავშირებულნი და ცვლიან ერთმანეთს შორის ინფორმაციას, უნდა ქონდეთ საერთო გაცვლის წესები ანუ პროტოკოლები.

პროტოკოლი - ეს არის წესები, რომელსაც იყენებენ ქსელური მოწყობილობები ერთმანეთთან დასაკავშირებლად. დღესდღეობით სტანდარტად მიღებულია პროტოკოლები რომლებსაც ეწოდება TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP პროტოკოლები განსაზღვრავენ ფორმატიზაციას, დამისამართებას და მარშუტიზაციას, რომლებიც იძლევა გარანტიას, რომ ინფორმაციის მიწოდება მოხდება დანიშნულ ადგილას და უშეცდომოდ.

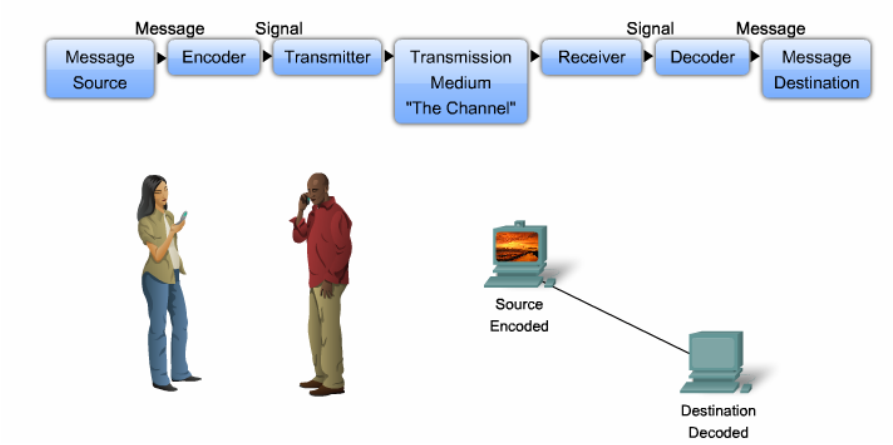
პირველი საფეხურზე, სანამ ინფორმაცია გადაეცემა მიმღებს, ხდება ინფორმაციის მომზადება ქსელში მის გადასაცემად. შემდგომ შეტობინების გადაყვანა ისეთ ფორმატში, რომელიც შესაძლებელი იქნება გადაიცეს ქსელში. შემდგომ ეტაპზე ყველა ტიპის ინფორმაცია გარდაიქმნება და დაიყოფა ინფორმაციულ ბლოკებად, რომელსაც ზოგადად პაკეტებს უწოდებენ. შემგომ განესაზღვრებათ გამგზავნის და მიმღების მისამართები და ბოლო ეტაპზე ის დაიყვანება ბიტებად, ციფრული სიგნალის ბინარულ კოდში და ამის შემდეგ ინფორმაცია მზადაა ქსელში გადასაცემად.

კომუნიკაცია

კომუნიკაცია არის შეტყობინების ან ინფორმაციის გადაცემა ერთი მოწყობილობიდან (ან ადამიანიდან) მეორესთვის. ადამიანები ერთმანეთს შორის იდეების გასაცვლელად იყენებენ მრავალ სხვადასხვა საკომუნიკაციო მეთოდებს. ყველა ამ მეთოდს აქვს სამი საერთო ელემენტი. პირველი ესაა ინფორმაციის წყარო ან გადამცემი. იგი შეიძლება იყოს როგორც პიროვნება ასევე

ელექტრონული მოწყობილობა, რომელსაც სურს გადასცეს ინფორმაცია სხვა პიროვნებას ან მოწყობილობას. მეორე - ესაა ინფორმაციის მიმღები, რომელიც იღებს ინფორმაციას და ინტერპრეტაციას უკეთებს მას. მესამე - არხი, რომელიც შეიცავს მედია საშუალებებს, რომლის მიხედვითაც ხდება ინფორმაციის გაგზავნა გადამცემიდან მიმღებამდე.

ნებისმიერი ინფორმაცია, იქნება ეს სიტყვა, მუსიკა თუ სურათი, მედიაში გადაიცემა ბიტების სახით. კომპიუტერულ ქსელებში მედია საშუალებებს წარმოადგენს რაიმე ტიპის კაბელი, ან უკაბელო გადაცემა.



ნახაზი 6. შეტყობინების გადაცემა (კომუნიკაცია)

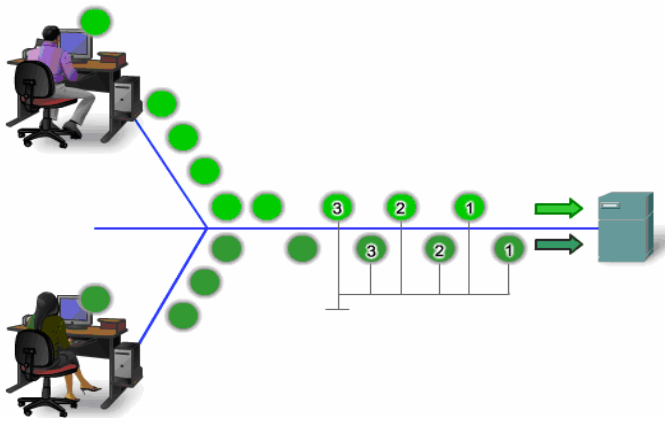
თეორიულად, ინფორმაცია (მუსიკა, ვიდეო, ფოსტა) გადაიცემა ქსელში გადამცემიდან მიმღებამდე როგორც ერთი უწყვეტი ბიტების მასივის ნაკადი. თუ ინფორმაცია გადაიცემა ქსელში ამ მეთოდით, ეს ნიშნავს, რომ არცერთ სხვა მოწყობილობას არ შეუძლია გადასცეს ან მიიღოს ინფორმაცია იგივე ქსელში მანამ,

სანამ მიმდინარეობს ამ ინფორმაციის გადაცემა, იმიტომ რომ ქსელური მოწყობილობები იყენებენ საერთო მედიას. ინფორმაციის ასეთმა დიდმა ნაკადმა შეიძლება გამოიწვიოს მნიშვნელოვანი შეფერხება ინფორმაციის გადაცემაში. თუ მოხდება ინფორმაციის დამახინჯება ან დაკარგვა გადაცემის დროს, საჭიროა მოხდეს მთლიანად მისი ხელმეორედ გადაცემა.

საუკეთესო მიდგომა მდგომარეობს იმაში, რომ მოხდეს ინფორმაციის დაყოფა პატარა ნაწილებად და ისე გაგზავნა ქსელში. ასეთ ნაწილებს სეგმენტებს უწოდებენ. სეგმენტაციის უპირატესობა მდგომარეობს შემდეგში:

1. ინფორმაციის პატარა ნაწილების გაგზავნისას შესაძლებელია ბევრი სხვადასხვა კომუნიკაცია დამყარდეს ერთდაიგივე არხის გამოყენებით. ეს შესაძლებელია იმიტომ, რომ როდესაც ხდება საერთო არხის გამოყენება დროითი კვანტის გამოყოფის პრინციპით, სხვადასხვა წყაროდან გამოგზავნილი სეგმენტები რიგრიგობით იყენებან ამ არხს. პროცესს, რომელშიც გამოიყენება ერთდაიგივე არხი მრავალი კომუნიკაციის დასამყარებლად ეწოდება მულტიპლექსირება.

2. სეგმენტაცია ზრდის ქსელში კომუნიკაციის საიმედოობას. არ არის აუცილებლობა ინფორმაციის თითოეული ნაწილმა გაიაროს ერთიდაიგივე გზა გადამცემიდან მიმღებამდე. თუ რომელიმე გზა გადატვირთულია ან ინფორმაცია განიცდის წარუმატებლობას, საჭიროა მოხდეს ინფორმაციის ცალკეული ნაწილების და არა მთლიანი ინფორმაციის გადაცემა.



ნახაზი 7. შეტყობინების სეგმენტაცია

სხვა მხრივ სეგმენტაციის და მულტიპლექსირების გამოყენება ართულებს და ზრდის ინფორმაციის მოცულობას. წარმოიდგინეთ, თქვენ გსურთ გააგზავნოთ 100 გვერდიანი წერილი, მაგრამ თითოეულ კონვერტში ჩადის მხოლოდ ერთი გვერდი. გამომდინარე აქედან ამ 100 კონვერტის დამისამართების, მარკირების, გაგზავნის, მიღების პროცესი იქნება დიდი დროის ხარჯვა როგორც გამგზავნისათვის ასევე მიმღებისათვის.

ქსელში კომუნიკაციისას ინფორმაციის თითოეული სეგმენტმა უნდა გაიაროს ერთგვარი პროცესი, რათა უზრუნველყოფილ იქნას ინფორმაციის დაყოფის და გადაცემის სისწორე და მისი აწყობა, რათა მოხდეს მისი გარდაქმნა მიმღების მხრიდან ორიგინალურ ინფორმაციად.

სხვადასხვა ტიპის მოწყობილობები მთელი ქსელის მაშტაბით უზრუნველყოფენ ინფორმაციის უშეცდომოდ გადაცემას გამგზავნიდან ადრესატამდე.

მოწყობილობები

როცა ჩვენ ვსარგებლობთ Ethernet-ით ვიყენებთ კომპიუტერს, თუმცა კომპიუტერი - ეს არის მხოლოდ ერთი ტიპის მოწყობილობა, რომლითაც შესაძლებელია მოხდეს ინფორმაციის მიღება და გაგზავნა ქსელში. ბევრი სხვა ტიპის მოწყობილობა შესაძლებელია გამოყენებული იქნას ქსელში. ასეთ მოწყობილობებს განეკუთვნებიან ტელეფონები, კამერები, პრინტერები და მუსიკალური სისტემები. ყველა ზემოთ ჩამოთვლილ მოწყობილობას, რომელიც შეიძლება იყოს გადამცემი ან ადრესატი (მიმღები) ეწოდებათ საბოლოო მოწყობილობები (End Device).

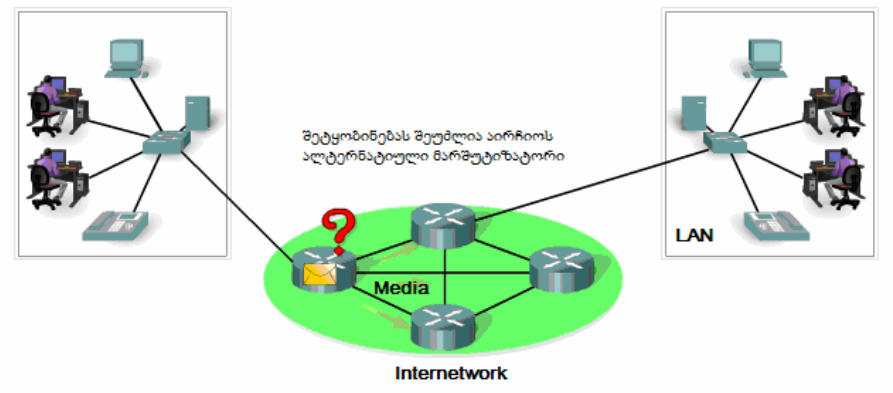
კომპიუტერებთან ერთად დამატებით არსებობს მრავალი კომპონენტები, რომლებიც საშუალებას იძლევა ჩვენი ინფორმაცია გაიგზავნოს დიდ მანძილზე მიწისქვეშ გაანლაგებული კაბელებით, საჰაერო და კოსმოსური საშუალებებით. ასეთ მოწყობილობებს უწოდებენ შუალედურს. ერთ-ერთი ყველაზე მნიშვნელოვანი შუალედური მოწყობილობაა მარშუტიზატორი. მარშუტიზატორი უერთდება ორ ან მეტ ქსელს და გადასცემს ინფორმაციას ერთი ქსელიდან მეორეში.

საბოლოო მოწყობილობები და მათი როლი ქსელში

ქსელური მოწყობილობებს, რომლებიც ადამიანისთვის ყველაზე კარგადაა ცნობილი ეწოდებათ საბოლოო მოწყობილობები. ეს მოწყობილობები აწესრიგებენ ინტერფეისს ადამიანურ ურთი-ერთობასა და საკომუნიკაციო ქსელს შორის. საბოლოო მოწყობილობებია:

- კომპიუტერები (work stations, laptops, file servers, web servers);
- ქსელური პრინტერები;
- VoIP ტელეფონები;
- უსაფრთხოების სათვალთვალო კამერები;
- და სხვა.

საბოლოო მოწყობილობები ქსელში მოიხსენიება როგორც ჰოსტი. ჰოსტი არის ინფორმაციის გამგზავნი ან მიმღები მოწყობილობა. იმისათვის რომ განვასხვავოთ ერთი ჰოსტი მეორისგან, თითოეულს გააჩნია უნიკალური მისამართი. როცა ჰოსტი იწყებს ინფორმაციის გადაცემას, იგი იყენებს მიმღების მისამართს რათა მიუთითოს თუ სად უნდა გაიგზავნოს ინფორმაცია.



ნახაზი 8. საბოლოო მოწყობილობები ქსელში

თანამედროვე ქსელებში ჰოსტი შესაძლებელია მოქმედებდეს როგორც კლიენტი, სერვერი ან ორივე ერთად. ჰოსტზე დაყენებული პროგრამული უზრუნველყოფა განსაზღვრავს მის როლს ქსელში.

სერვერები არიან ჰოსტები, რომლებზეც დაყენებულია პროგრა-მები რომლებიც საშუალებას იძლევა უზრუნველყოს სხვა ჰოსტები ისეთი მომსახურებით როგორიცაა ელ-ფოსტა ან web გვერდები.

კლიენტები არიან ჰოსტები, რომლებზეც დაყენებულია პროგრამები, რომლებიც საშუალებას აძლევს მათ რომ მოითხოვონ და აჩვენონ სერვერიდან მიღებული ინფორმაცია.

შუალედური მოწყობილობები და მათი როლი ქსელში

გარდა საბოლოო მოწყობილობებისა, რომლებსაც ადამიანები ხშირად იყენებენ, ქსელში არსებობს შუალედური მიწყობილობები რომლებიც უზრუნველყოფენ კავშირს და მუშაობენ მანამ სანამ მონაცემები გადაიცემა ქსელში. ეს მოწყოილობები აკავშირებენ ინდივიდუალურ ჰოსტს ქსელთან და აგრეთვე შეუძლიათ მრავალი ინდივიდუალური ქსელის ერთმანეთთან დაკავშირება, რათა შექმნან ქსელების გაერთიანება. შუალედური მოწყობილობებია:

- ქსელში შეღწევის მოწყობილობა (ჰაბი, კომუტატორი, უსადენო წვდომის წერტილი);
- მარშუტიზატორი;
- საკომუნიკაციო სერვერი;
- მოდემი;

- ფაირვოლი და სხვა.

შუალედური მოწყობილობების ერთერთი ფუნქციაა ქსელში მონაცემების გადაცემისას მათი მართვა. ეს მოწყობილობები იყენებენ მიმღები ჰოსტის მისამართს, რათა განსაზღვრონ გზა, რომელიც უნდა გაიაროს მონაცემმა.

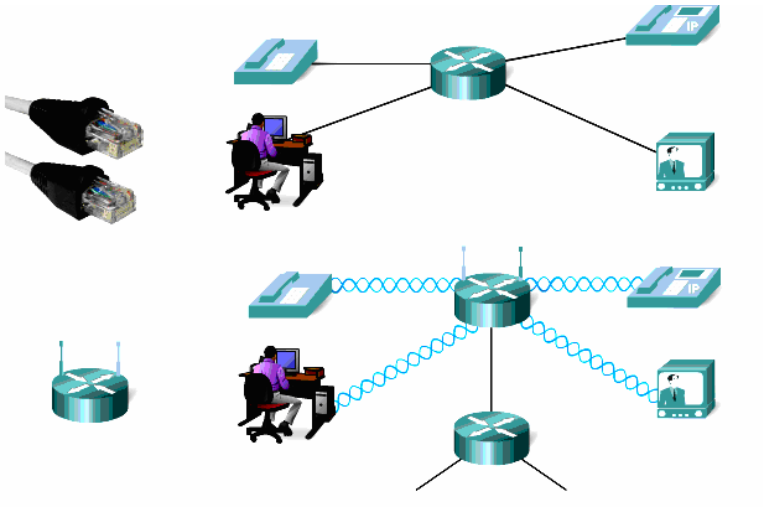
ქსელური მედია

ქსელებში კომუნიკაცია ხორციელდება ქსელური მედიის გამოყენებით. იმისათვის რომ გავაგზავნოთ ინფორმაცია, კომპიუტერი უნდა იყოს ჩართული საკაბელო ან რადიო ლოკალურ ქსელში. ასეთი ქსელები შესაძლებელია დამონტაჟებული იყოს სახლში ან სამსახურში, სადაც ისინი საშუალებას აძლევენ კომპიუტერებს და სხვა მოწყობილობებს რომ გაცვალონ ინფორმაცია ერთმანეთთან. თანამედროვე ქსელი იყენებს სამი ტიპის მედია საშუალებას, რომლითაც ხდება ინფორმაციის გადაცემა. ეს მედია საშულებებია:

- სპილენძის გამტარიანი კაბელები;
- ოპტიკურ-ბოჭკოვანი კაბელები;
- უკაბელო გდაცემები.

უკაბელო (რადიო) ქსელები საშუალებას იძლევიან გამოვიყენოთ ქსელური მოწყობილობები ნებისმიერ ადგილას: სახლში ან ოფისში, ასევე სივრცეში. ოფისის და სახლს გარეთ უკაბელო

ქსელი ხელმისაწვდომია ისეთ საზოგადოებრივ ადგილებში, როგორიცაა კაფეტერია, სასტუმრო, აეროპორტი.



ნახაზი 9. ქსელური კავშირები

ქსელების უმეტესობა კავშირისათვის იყენებს საკომუნიკაციო კაბელებს. ლოკალურ ქსელებში უმეტესად გამოიყენება საკაბელო ქსელური ტექნოლოგია. კაბელები აერთიანებენ კომპიუტერებს და სხვა მოწყობილობებს და ისინი ქმნიან ქსელს. ასეთი ქსელები წარმატებით გამოიყენება იმ შემთხვევებში როცა საჭიროა დიდი ზომის ინფორმაციის გადაცემა დიდ სიჩქარეზე.

მედია უზრუნველყოფს არხის შექმნას გამგზავნიდან მიმღებამდე მონაცემების გადასაცემად.

ნახაზი 10. ქსელური მედია

მედიაში მონაცემების გადაცემისას საჭიროა სიგნალების კოდირება, რომელიც სხვადასხვა ტიპის მედიაში არის განსხვავებული. სპილენძის გამტარში მონაცემების კოდირება ხორციელდება ელექტრული იმპულსების სახით. ოპტიკურ მედიაში - სინათლის სხივის გადაცემის სახით, უკაბელო გადაცემისას - ელექტრომაგნიტური ტალღების სახით.

გამოთვლით ტექნიკაში მონაცემების წარმოსადგენად გამოიყენება ორობითი კოდი. მონაცემების წარმოდგენას ელექტრული ან ოპტიკური სიგნალების სახით ეწოდება კოდირება. არსებობს 1 და 0 ის კოდირების რამოდენიმე საშუალება, მაგალითად, პოტენციალური მეთოდი, რომლის დროსაც 1-იანს შეესაბამება პოტენციალის ერთი დონე, ხოლო 0-ს მეორე, ან იმპულსური მეთოდი, როდესაც ციფრების წარმოსადგენად გამოიყენება განსხვავებული ან ერთი პოლარობის იმპულსები.

ანალოგიური მიდგომები შეიძლება იქნას გამოყენებული მონაცემთა კოდირებისათვის და მათი გადაცემისათვის ორ კომპიუტერს შორის კავშირის ხაზის გამოყენებით. მაგრამ ეს ხაზები განსხვავდება თავისი ელექტრული მახასიათებლებით, იმისგან რომელიც გამოიყენება კომპიუტერის შიგნით. მთავარი განსხვავება გარე ხაზებს და შიდა ხაზებს შორის მდგომარეობს იმაში, რომ ისნი დიდ მანძილზე არიან გაყვანილი, ასეევე იმაში რომ, ისინი არ არიან დაფარული ეკრანირებული კორპუსით, რაც იწვევს სიგნალის დაზიანებას გარე ელექტრომაგნიტური გამოსხივების გამო. ყველაფერი ეს იწვევს მართკუთხედი იმპულსის მნიშვნელოვან დამახინჯებას. ამიტომ მიმღები მხარის მიერ იმპულსის საიმედოდ ამოსაცნობად, სიგნალების კოდირება და გადაცემის სიჩქარე რომელიც გამოიყენება კომპიუტერში და ასევე სიგნალების კოდირება და გადაცემის სიჩქარე რომლებიც გადაიცემა კავშირის ხაზებში განსხვავებულია.

კომპიუტერულ სისტემების მედია საშუალებებში გამოიყენება მონაცემების როგორც პოტენციალური, ასევე იმპულსური კოდირება. ასევე გამოიყენება სპეციფიური მეთოდი ინფორმაციის წარმოსადგენად, როგორიცაა მოდულაცია, რომელიც არასოდეს გამოიყენება კომპიუტერის შიგნით. მოდულაციის დროს დისკრეტული ინფორმაცია წარმოდგება სინუსოიდური სიგნალების სახით და იმ სიხშირით რომელსაც ყველაზე უკეთ გადასცემს არსებული ხაზი.

განსხვავებული ტიპის მედიებს აქვთ განსხვავებული მახასიათებლები და გამოყენება. ყველა ქსელურ მედიას არ აქვს ერთნაირი ნიშანთვისებები და ისინი გამოიყენება განსხვავებული მიზნებით. კრიტერიუმი რის მიხედვითაც ხდება მედიის შერჩევა არის შედეგი:

- დისტანცია, სადაც სიგნალის გადაცემა შესაძლებელია წარმატებით;
- გარემო, სადაც მედია იქნება გამოყენებული;
- მონაცემების რაოდენობა და სიჩქარე, რომელიც უნდა გადაიცეს.

გზა, რომელსაც გადის ინფორმაცია გამგზავნიდან მიმღებამდე, შესაძლებელია იყოს მარტივი, მაგალითად როგორიც არის ორი კომპიუტერის გაერთიანება ერთი კაბელით, ან რთული, როგორიცაა ქსელი რომელიც მოიცავს მთელ დედამიწას. ქსელის ეს ინფრასტრუქტურა არის პლატფორმა რომელიც უზრუნველყოფს გარანტირებულ და საიმედო კავშირს, რომელშიც ხდება კომუნიკაცია.

მოწყობილობები და მედია არის ქსელის ფიზიკური ელემენტები ან აპარატურული საშუალებები. აპარატურული საშუალებები ძირითადად არის ქსელური პლატფორმის ხილვადი კომპონენტები. ასეთებია laptop, PC, switch ან კაბელი, რომელიც აერთებს მოწყობილობებს. ხანდახან ზოგიერთი კომპონენტი შესაძლებელია იყოს უხილავი. უკაბელო ინტერნეტის დროს ინფორმაცია გადაეცემა ატმოსფეროს საშუალებით და იყენებს არახილვად რადიოსიხშირეს ან ინფრაწითელ ტალღებს.

მომსახურება და სერვისები

მომსახურება და პროცესები არის საკომუნიკაციო პროგრამები ანუ პროგრამული უზრუნველყოფა, რომლებიც ეშვება ქსელურ მოწყობილობებზე. ქსელური მომსახურება უზრუნველყოფს მოთხოვნაზე ინფორმაციის მიღებას. იგი მოიცავს ბევრ საერთო გამოყენებით მომსახურებას, რომელსაც ადამიანები ყოველდღე იყენებენ. მაგ. ელექტრონული ფოსტა, web გვერდები და სხვა. პროცესები უზრუნველყოფენ ქსელური მოწყობილობების ფუნქციონირებას, რომლებიც აგზავნიან ინფორმაციას ქსელში. პროცესები ნაკლებად შესამჩნევია ჩვენთვის, მაგრამ მნიშვნელოვანია ქსელის მუშაობისთვის.

პროტოკოლები

ერთერთ ყველაზე მნიშვნელოვან ასპექტს ქსელში ინფორმაციის გადაცემისას წარმოადგენს წესები ანუ პროტოკოლები. ეს წესები არის სტანდარტული და ისინი განსაზღვრავენ თუ როგორ უნდა მოხდეს ინფორმაციის გადაცემა ქსელში. ქსელში მუშაობა ესაა მონაცემთა გადაცემა ერთი კომპიუტერიდან მეორეზე. ამ პროცესში შეიძლება რამდენიმე საკითხის გამოყოფა:

მონაცემთა გამოცნობა, მონაცემთა დაყოფა მმართველ ბლოკებად, თვითოეული ბლოკისთვის ინფორმაციის დამატება, რათა მიუთითოთ მონაცემთა მდებარეობა და მივუთითოთ მიმღები, დავუმატოთ სინქრონიზაციის და შეცდომების შესწორების შესახებ ინფორმაცია, მოვათავსოთ მონაცემები ქსელში და გავგზავნოთ ისინი მითითებულ მისამართზე. ამ ოპერაციების შესრულება ხდება პროტოკოლებით. არ არის იმის აუცილებელობა, რომ ქსელში გამოყენებული პროტოკოლები იყოს

სტანდარტული, მაგრამ ქსელების ექსპლოატაციის დროს პრაქტიკაში მიღებულია, რომ ისინი იყვნენ სტანდარტულნი. ეს შეიძლება იყოს საფირმო, ნაციონალური ან საერთაშორისო სტანდარტი.

პროტოკოლი აკონტროლებს მონაცემების მიმოცვლის ყველა ასპექტს, რომელიც მოიცავს შემდეგს:

- როგორ არის ფიზიკური ქსელი აგებული;
- როგორ არიან კომპიუტერები დაკავშირებული ქსელთან;
- როგორ არის მონაცემები წარმოდგენილი გადაცემისას;
- როგორ იგზავნება მონაცემები;
- როგორ აღმოიფხვრას შეცდომები.

ქსელის წესები არის შექმნილი და დამტკიცებული სხვადასხვა ორგანიზაციების მიერ. ამ ჯგუში შედიან : Institute of Electrical and Electronic Engineers (IEEE), American National Standards Institute (ANSI), Telecommunications Industry Association (TIA), Electronic Industries Alliance (EIA) და International Telecommunications Union (ITU), Comité Consultatif International Téléphonique et Télégraphique (CCITT).

ქსელების ტოპოლოგია

ქსლის ტოპოლოგია განსაზღვრავს ქსელის სტრუქტურას. ტოპოლოგია ორი ნაწილისგან შედგება, ერთი ნაწილია

ფიზიკური ტოპოლოგია, რომელიც ძირითადად განსაზღვრავს კაბელის ტიპს და მათ ფიზიკურ დაკავშირების პრინციპს. მეორე ნაწილი კი განსაზღვრავს ლოგიკურ ტოპოლოგიას, რომელიც ადგენს, თუ როგორ უნდა მოხდეს გარემოში შეღწევა და მონაცემების გადაცემა.

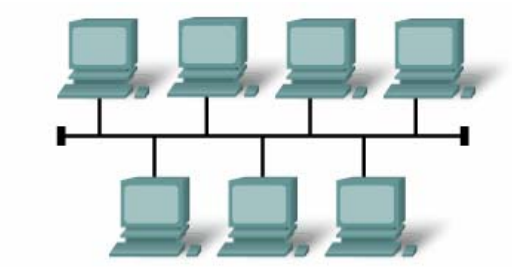
ტოპოლოგიის არჩევა მნიშვნელოვნად მოქმედებს ქსელის მრავალ ნიშანთვისებაზე. მისი არჩევა გავლენას ახდენს საჭირო ქსელური მოწყობილობების შემადგენლობაზე, ქსელის გაფართოების შესაძლებლობაზე და ა.შ.

ნებისმიერი ქსელი შედგება სამი ძირითადი ტოპოლოგიის საფუძველზე: სალტე (bus), ვარსკვლავი(star) და წრე(ring).

სალტე ტოპოლოგიის შემთხვევაში, კომპიუტერები ერთი კაბელის გასწვრივ არიან შეერთებულნი. ვარსკვლავი ტოპოლოგიის შემთხვევაში, კომპიუტერები სხვადასხვა კაბელში არიან შეერთებულნი, ეს კაბელები კი ერთი წერტილიდან კონცეტრატორიდან (Hub) გამოდიან. წრე ტოპოლოგიის შემთხვევაში, კომპიუტერები ჩაკეტილ წრეზე არიან ჩართულნი.

სალტე ტოპოლოგიაში გამოიყენება ერთი კაბელი, რომელსაც მაგისტრალი ჰქვია. სალტე ტოპოლოგია თავისი სიმარტივის გამო, ერთ-ერთ ყველაზე გავრცელებულ ტოპოლოგიას წარმოადგენს. ასეთი ტიპილოგიის დროს ელექტრული სიგნალებით მონაცემები გადაეცემა მთელ ქსელს, მაგრამ ინფორმაციას იღებს ის კომპიუტერი, რომლის მისამართიც შეესაბამება მომხმარებლის მიერ მითითებულ მისამართს. დროის ყოველ მომენტში ინფორმაციის გადაცემა შეუძლია მხოლოდ ერთ კომპიუტერს. რადგან მონაცემთა გადაცემა შეიძლება მხოლოდ ერთი კომპიუტერის მიერ, მისი მწარმოებლურობა დამოკიდებულია

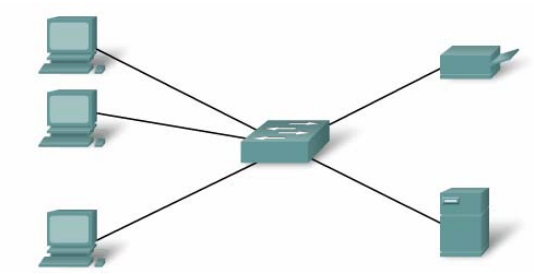
სალტეზე მიერთებული კომპიუტერების რაოდენობაზე. რაც მეტია კომპიუტერების რიცხვი, მით მეტი კომპიუტერი იმყოფება ლოდინის მდგომარეობაში და მით ნელია ქსელი.



ნახაზი 11. სალტე ტოპოლოგია

სალტე ტოპოლოგიის შემთხვევაში, ელექტრონული სიგნალები ვრცელდება კაბელის თავიდან ბოლომდე. კაბელის ბოლოს მიღწეული სიგნალი აირეკლება და უკან ბრუნდება ქსელში. ეს კი იწვევს ქსელში გადაცემული ინფორმაციის დამახინჯებას. ამიტომ კაბელის ბოლოს მიღწეული სიგნალი აუცილებლად უნდა ჩაქრეს. ამისათვის, კაბელის ბოლოს აყენებენ ტერმინატორს, რომელიც ახშობს ამ სიგნალებს.

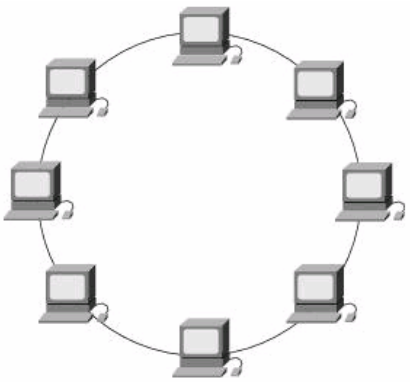
ვარსკვლავი ტოპოლოგიის შემთხვევაში კომპიუტერი კაბელის სეგმენტით უერთდება კონცენტრატორს. მისი საშუალებით ხდება დანარჩენ კომპიუტერებზე სიგნალების გადაცემა. თუ ერთი კომპიუტერი (ან კაბელი რომელიც კონცენტრატორს და კომპიუტერს ერთმანეთთან აკავშირებს) გამოვა მწყობრიდან, მაშინ მხოლოდ მას არ შეუძლია გადასცეს ან მიიღოს მონაცემები. სხვა დანარჩენი კომპიუტერები მუშაობენ ნორმალურად. მათ მუშაობაზე ეს დაზიანება გავლენას არ ახდენს, მაგრამ თუ დაზიანდა კონცენტრატორი, ქსელი წყვეტს მუშაობას.



ნახაზი 12. ვარსკვლავური ტოპოლოგია

ვარსკვლავურ ტოპოლოგიაში კონცენტრატორი(Hub) არის ცენტრალური ჰოსტი. განასხვავებენ აქტიურ და პასიურ კონცენტრატორებს. აქტიური კონცენტრატორები სიგნალს უკეთებენ აღდგენას გამმეორებლის მსგავსად და ისე გადასცემენ ქსელში. მათ კომპიუტერთან მისაერთებლად აქვთ პორტები. პასიური კონცენტრატორები არ აღადგენენ სიგნალებს ისინი მხოლოდ გადასაცემენ მათ. კონცენტრატორზე აგებული ქსელების გაფართოება მარტივია - ეს ხდება დამატებითი კონცენტრატორების მიერთებით.

წრე ტოპოლოგიაში კომპიუტერები შეერთებულნი არიან ერთმანეთთან ჩაკეტილ წრეზე. კაბელს არ აქვს თავისუფალი ბოლო და სიგნალები გადაიცემიან ერთი მიმართულებით და გადიან ყველა კომპიუტერზე, მაგრამ თუ მწყობრიდან გამოვიდა რომელიმე კომპიუტერი ქსელი წყვეტს მუშაობას. ასეთი სახის ქსელებში მონაცემთა გადაცემა ხდება მარკერით. მარკერი მოძრაობს წრეზე (კომპიუტერიდან კომპიუტერზე) მანამ, სანამ მას არ მიიღებს ის კომპიუტერი რომელსაც სურს მონაცემთა გაგზავნა.



ნახაზი 13. წრე ტოპოლოგია

გადამცემი კომპიუტერი მარკერს მიამაგრებს გადასაცემ მონაცემებს და აგზავნის წრეზე. მონაცემები მოძრაობენ წრეზე მანამ სანამ მას არ მიიღებს მიმღები კომპიუტერი(ანუ კომპიუტერი რომლის მისამართიც ემთხვევა მიმღების მისამართს). ამის შემდეგ მიმღები კომპიუტერი გზავნის გადამცემ კომპიუტერთან შეტყობინებას მონაცემთა მიღების შესახებ. მიიღებს რა თანხმობას, გადამცემი კომპიუტერი ქმნის ახალ მარკერს და აბრუნებს ქსელში. მარკერის გადაცემის სიჩქარე ძალიან მაღალია.

პრაქტიკაში გვხვდება უფრო რთული კომბინაციები, რომლებიც ერთდროულად რამდენიმე ტოპოლოგიას აერთიანებს ე.წ. კომბინირებული ტოპოლოგიები: ვარსკვლავი-სალტე ტოპო-ლოგია (star-bus).ეს არის სალტის და ვარსკვლავი ტოპოლოგიის კომბინაცია. ჩვეულებრივ ასეთი ტოპოლოგიის დროს რამდენიმე ვარსკვლავი ტოპოლოგია არის გაერთიანებული მაგისტრალური წრფივი სალტით. ასეთი ტოპოლოგიის დროს ერთი კომპიუტერის მწყობრიდან გამოსვლა არ ახდენს გავლენას ქსელის მუშაობაზე.

კონცენტრატორის მწყობრიდან გამოსვლა გათიშავს მხოლოდ უშუალოდ მასთან შეერთებულ კომპიუტერებს.

ტოპოლოგიის არჩევისას უნდა გავითვალისწინოთ შემდეგი ფაქტორები:

ტიპოლოგიის უპირატესობანი და უარყოფითი მხარეები:

კოაქსიალური კაბელის ეკონომიური დანახარჯი - ინფორმაციის გადაცემა შედარებით იაფია და მისი გაფართოება მარტივია; დიდი ზომის ტრაფიკის დროს მცირდება ქსელის შესაძლებლობანი. ტოპოლოგიის ძირითადი უპირატესობაა მისი სიიაფე და კაბელიზაციის სიმარტივე. ყველაზე მნიშვნელოვანი ნაკლოვანება არის მისი დაბალი საიმედოობა: სადენის ნებისმიერი დეფექტი ან კონექტორის ნებისმიერი დაზიანება, სრულიად იწვევს ქსელის მუშაობის პარალიზებას. სხვა ნაკლოვანება არის მისი დაბალი მწარმოებლურობა. რადგანაც ასეთი კავშირის გამოყენების შემთხვევაში მხოლოდ ერთ კომპიუტერს შეუძლია ინფორმაციის გადაცემა დროის ერთ მომენტში. ამიტომაც, არხის გამტარობა ყოველთვის იყოფა ქსელში ჩართულ ყველა კომპიუტერზე.

წრე ტოპოლოგიის შემთხვევაში ყველა კომპიუტერი თანასწორ-უფლებიანია. კომპიუტერების რიცხვი თითქმის არ ახდენს გავლენას ქსელის მწარმოებლურობაზე. ქსელის გაფართოები-სათვის მთელი ქსელი უნდა გაითიშოს.

ვარსკვლავი ტოპოლოგიის ქსელის მოდიფიკაცია მარტივად ხდება. ერთი კომპიუტერის მწყობრიდან გამოსვლა არ იწვევს ქსელის გათიშვას. კონცენტრატორის გათიშვა კი იწვევს ქსელის გათიშვას.

კომპიუტერულ ქსელებში კომპიუტერების ერთმანეთთან შესაერთებლად გამოიყენება, როგორც ინდივიდუალური (გამოყოფილი), ასევე საერთო (Shared) ხაზები. საერთო ხაზების მაგალითია ტოპოლოგია "საერთო სალტე", რომელშიც ერთი კაბელი გამოიყენება ქსელში ჩართული ყველა კომპიუტერის მიერ მონაცემთა გადასაცემად.

ლოკალური და გლობალური ქსელები

კლასიფიკაციის მიხედვით კომპიუტერულ ქსელებს ყოფენ ქსელით დაფარული ტერიტორიის სიდიდის მიხედვით. ქსელური ინფრასტრუქტურა შეიძლება შეიცვალოს შემდეგი მონაცემების მიხედვით:

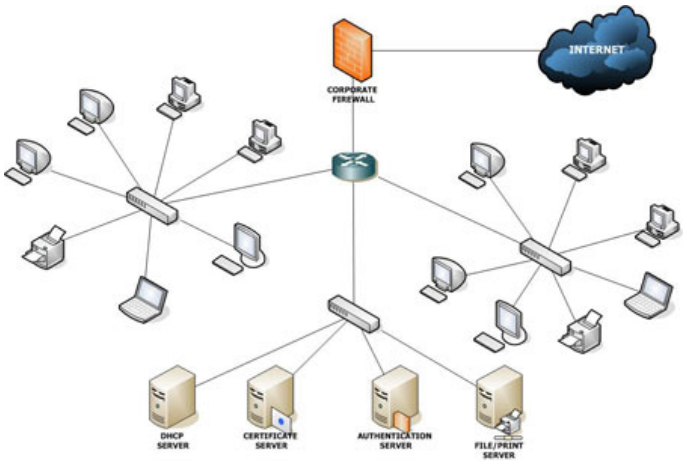
- ქსელით დაფარული ტერიტორიის ზომა;
- მომხმარებლების რაოდენობა;
- მომსახურების რაოდენობა და ტიპი.

ლოკალური და გლობალური ქსელების ტექნოლოგიების დაახლოების მიუხედავად არსებობს მათ შორის მნიშვნელოვანი განსხვავებაც. განვიხილოთ თითოეული მათგანი.

ლოკალური ქსელები

ლოკალური ქსელები – Local Area Networks (LAN). ლოკალურ ქსელებს მიეკუთვნება მცირე ტერიტორიაზე თავმოყრილი კომპიუტერული ქსელები. ისინი ძირითადად წარმოადგენენ ერთი ორგანიზაციის კუთვნილ საკომუნიკაციო სისტემას.

ლოკალური ქსელებისათვის დამახასიათებელი მცირე მანძილები შესაძლოს ხდის გამოყენებული იქნას შედარებით ძვირად-ღირებული მაღალხარისხიანი კავშირის ხაზები, რაც საშუალებას გვაძლევს მივაღწიოთ მონაცემთა გადაცემის მაღალ სისწრაფეს.

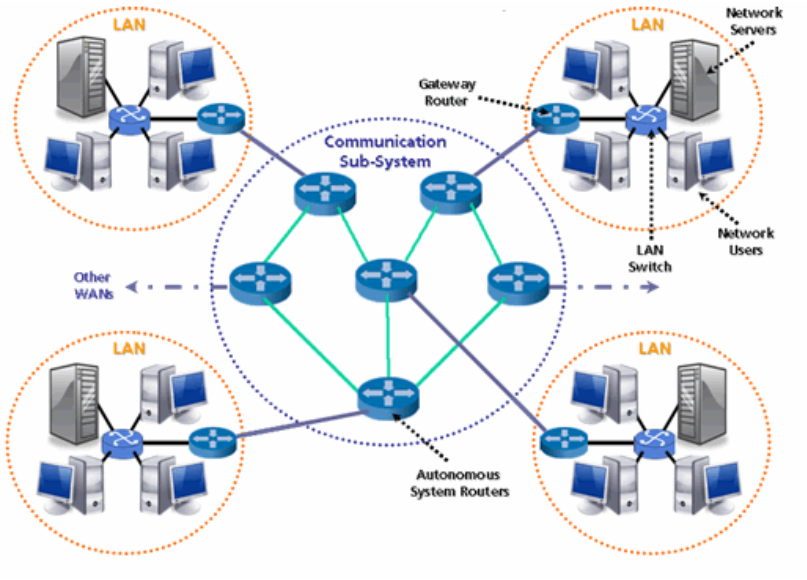


ნახაზი 14. ლოკალური ქსელები – Local Area Networks (LAN)

გლობალური ქსელები

გლობალური ქსელები – Wide Area Networks (WAN). იგი აერთიანებს ტერიტორიულად განცალკევებულ კომპიუტერებს, რომლებიც განლაგებულნი არიან სხვადასხვა ქალაქებსა და ქვეყნებში. რადგანაც დიდ მანძილზე მაღალხარისხიანი კავშირის ხაზების გაყვანა ძვირი ჯდება, ამიტომ გლობალურ ქსელებში გამოიყენება უკვე არსებული კავშირის ხაზები მაგ. საერთო დანიშნულების სატელეფონო და სატელეგრაფო ხაზები. ასეთ ხაზებში ხდება მონაცემთა გადაცემა დაბალი სისწრაფით (ათობით კბ/წმ). უხარისხო კავშირის ხაზების გამო მონაცემთა უდანაკარგოდ გადაცემისათვის გამოიყენება კონტროლის და

მონაცემების აღდგენის რთული პროცედურები, რადგანაც ასეთი არხებით მონაცემთა გადაცემა დაკავშირებულია სიგნალის დამახინჯებასთან.



ნახაზი 15. გლობალური ქსელები – Wide Area Networks (WAN)

საქალაქო ქსელები – Metropolitan Area Networks (MAN). ასეთი ტიპის ქსელები ნაკლებადაა გავრცელებული. იგი განკუთვნილია მსხვილი ქალაქის – მეგაპოლისის ტერიტორიის მომსახურებისათვის. საქალაქო ქსელებს უკავიათ შუალედური მდგომარეობა ლოკალურ და გლობალურ ქსელებს შორის. ისინი იყენებენ კავშირის ხაზების ციფრულ მაგისტრალებს, ხშირად ოპტიკურბოჭკოვანს, რომელიც განკუთვნილია ლოკალური ქსელების დასაკავშირებლად და ლოკალური და გლობალური ქსელების შესაერთებლად. თავდაპირველად ეს ქსელები მონაცემთა გადასაცემად იყო დამუშავებული, მაგრამ ამჟამად

გადაიცემა ვიდეოკონფერენციები და ხმის ან ტექსტის ინტეგრალური გადაცემები.

განსხვავება ლოკალურ და გლობალურ ქსელებს შორის

1. კავშირის ხაზების სიგრძე და ხარისხი.

როგორც უკვე ავღნიშნეთ ლოკალური ქსელი შეიძლება აგებული იქნას პატარა მანძილზე, რაც საშუალებას იძლევა გამოვიყენოთ ხარისხიანი კავშირის ხაზები როგორიცაა კოაქსიალური კაბელი, ხვეული წყვილი, ოპტიკურბოჭკოვანი, რომლებიც მიუღებელია (ეკონომიური თვალსაზრისით) დიდი მაძილებისათვის, რაც ახასიათებს გლობალურ ქსელებს.

2. მონაცემთა გადაცემის მეთოდები.

ფიზიკური არხების დაბალი საიმედოობის გამო გლობალურ ქსელებს ესაჭიროება მონაცემთა გადაცემის უფრო რთული მეთოდები, ვიდრე ლოკალურ ქსელებს. გლობალურ ქსელებში ფართოდ გამოიყენება მოდულაცია, ასინქრონული მეთოდები, ხარვეზიანი კადრების განმეორებით გადაცემა, საკონტროლო ჯამის გათვლის რთული მეთოდები. ლოკალურ ქსელებში კი ხარისხიანი კავშირის ხაზების გამოყენება მონაცემთა გადაცემის გამარტივების საშუალებას იძლევა, რაც განპირობებულია არამოდულირებული სიგნალების და პაკეტის მიღების დადასტურებაზე უარის თქმის ხარჯზე.

3. მომსახურების მრავალფეროვნება

ლოკალური ქსელები, როგორც წესი, გვთავაზობენ მრავალფეროვან მომსახურებას – ფაილური და ფაქსიმილური

გადაცემის მომსახურება, მონაცემთა ბაზების მომსახურება ელ-ფოსტით და ა.შ. გლობალური ქსელები ძირითადად გვთავაზობენ საფოსტო მომსახურებას და იშვიათად შეზღუდული საშუალებების ფაილურ მომსახურებას.

4. მოთხოვნების შესრულების ოპერატიულობა

ლოკალურ ქსელში პაკეტის გადაცემის დრო შეადგენს რამდენიმე მილიწამს, მაშინ როცა გლობალურ ქსელებში პაკეტის გადაცემა შეიძლება რამდენიმე წამი გაგრძელდეს. გლობალურ ქსელებში მონაცემთა გადაცემის დაბალი სისწრაფე ართულებს ონ-ლაინ მომსახურების რეჟიმის რეალიზაციას.

5. პაკეტების კომუტაციის მეთოდების გამოყენება

ლოკალურ ქსელებში მნიშვნელოვან თავისებურებად მიჩნეულია დატვირთვის არათანაბარი განაწილება. პიკური დატვირთვის შეფარდებამ საშუალოსთან შეიძლება შეადგინოს 100:1. ასეთ ტრაფიკს უწოდებენ პულსაციურს. ტრაფიკის ამ თავისებურების გამო კვანძების შეერთებისათვის გამოიყენება პაკეტების კომუტაციის მეთოდი, რომელიც უფრო ეფექტურია პულსაციური ტრაფიკისთვის ვიდრე გლობალურ ქსელში არხების კომუტაციის მეთოდი. პაკეტების კომუტაციის მეთოდი მდგომარეობს იმაში, რომ ქსელი დროის ერთეულში მეტ მონაცემს გადასცემს თავის აბონენტებს. პაკეტის კომუტაციის მეთოდი გლობალურ ქსელებშიც გამოიყენება.

6. მაშტაბურობა

ლოკალურ ქსელებს გააჩნიათ ცუდი მაშტაბურობა საბაზო ტოპოლოგიის გამო. ტოპოლოგია განსაზღვრავს სადგურების

შეერთების წესებს და ხაზების სიგრძეს. ლოკალურ ქსელში კვანძების რაოდენობის ან კავშირის ხაზების სიგრძისთვის განკუთვნილი ზღვრის მიღწევისას, მკვეთრად უარესდება ქსელის მახასიათებლები. გლობალური ქსელი კი კარგად ექვემდებარება მაშტაბებს, რადგან ისინი შექმნილნი არიან ნებისმიერ ტოპოლოგიასთან სამუშაოდ.

ლოკალური ქსელების სპეციალისტები, რომელთა წინაშე დადგა ამოცანა გაეერთიანებინათ რამოდენიმე ლოკალური ქსელი განლაგებული სხვადასხვა გეოგრაფიულ პუნქტში, იძულებულნი გახდნენ შეესწავლათ მათთვის უცნობი გლობალური ქსელები და ტელეკომუნიკაციები. მეორეს მხრივ, მონაცემთა გადაცემის სისწრაფის გაზრდის და მომსახურეობის ხარისხის გაზრდის მისწრაფებამ, აიძულა გლობალურ ქსელებში მომუშავე სპეციალისტებს ყურადღება მიეპყროთ ლოკალურ ქსელებში გამოყენებულ ტექნოლოგიებზე. ამან განაპირობა ქსელების სამყაროში ურთიერთმიმართულებითი მოძრაობა. ამის შედეგს წარმოადგენს საქალაქო ქსელების გამოყენება (MAN).

გლობალური ქსელების განვითარებამ გამოიწვია უარის თქმა მონაცემთა გადაცემის პერმანენტული შემოწმების დაცვის პრინციპებზე. მაგ. Frame Relay ქსელებში ბიტის დამახინჯება ისე იშვიათად ხება, რომ პაკეტი რომელშიც შეცდომაა უბრალოდ ნადგურდება. ეს დანაკარგი გვარდება ტრანსპორტის ან გამოყენებითი დონის პროგრამებით. ამ ქსელში მონაცემთა გადაცემის სისწრაფე საკმაოდ მაღალია.

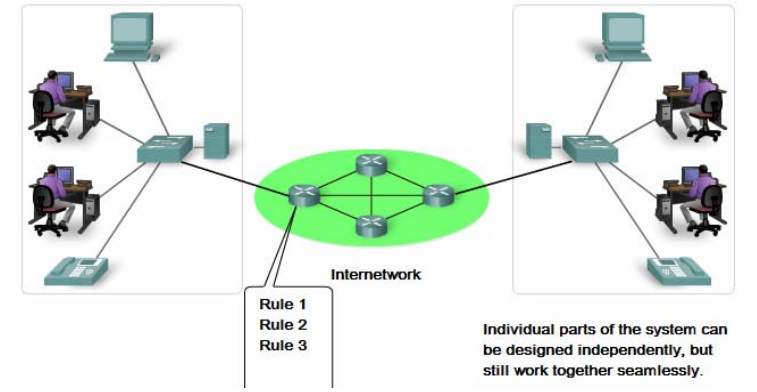
OSI მოდელი

ინფორმაციის გადაცემისას ერთი მოწყობილობიდან მეორეზე, ინფორმაცია გადის მომზადების რთულ პროცესს, სადაც აღწერილია, თუ რა ეტაპები უნდა გაიაროს ინფორმაციამ, რომ მოხდეს მისი ისეთი მომზადება, რომ შესაძლებელი იყოს მისი ფიზიკურ მედიაში გადაიცემა, და შესამაბისად, რა ეტაპები უნდა გაიაროს, რომ მოხდეს ფიზიკური მედიიდან ორიგინალური ინფორმაციის მისაღებად.

ეს ეტაპები კომპიუტერულ ქსელებში წარმოდგენილია დონეების სახით. თითოეულ დოენზე მუშაობს გარკვეული ტიპის პროტოკოლი, რომელიც პასუხისმგებელია მის ზემოთ არსებული დონიდან მიღებული ინფორმაცია დაამუშაოს და გადასცეს მის ქვემდგომ დონეს. ამ პროცესს ენკაფსულაციას უწოდებენ. აღნიშნული დონეები ქმნიან პროტოკოლების ნაკრებს (სტეკს). ანუ სტეკი არის პროტოკოლების ნაკრები, რომელიც უზრუნველყოფს ნებისმიერი ტიპის ინფორმაციის მომზადებას და გადაგზავნას ფიზიკურ მედიაში და პირიქით - ფიზიკური მედიიდან მის აღდგენას იმ სახით რა სახითაც იქნა გადაცემული.

კომპიუტერულ ქსელებში არსებობს პროტოკოლების სხვადასხვა ნაკრები. როგორც წესი ისინი არათავსებადი არიან ერთმანეთთან.

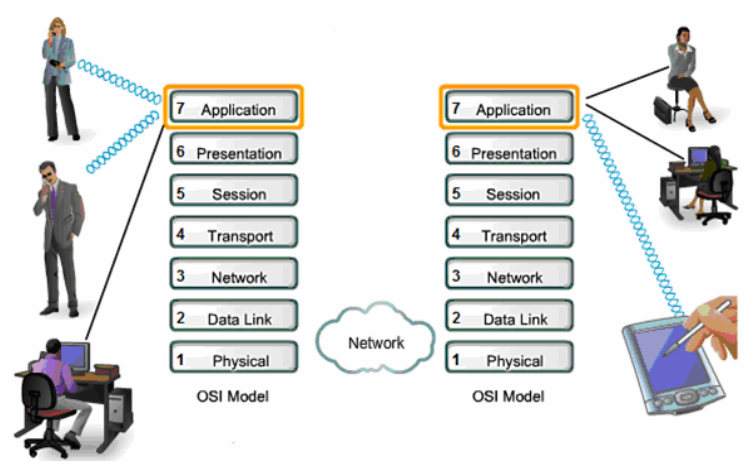
რათა წარმოვსახოთ ურთიერთქმედება სხვადასხვა პროტოკოლებს შორის, გამოიყენება დონეებად დაყოფის მოდელი. იგი აღწერს პროტოკოლების ოპერაციებს, რომლებსაც ადგილი აქვთ თითოეულ დონეზე, და ასევე ურთიერთქმედებას მის ზედა და ქვედა დონეებთნ.



ნახაზი 16. OSI მოდელის გამოყენება

80-იან წლებში საერთაშორისო ორგანიზაციებმა ISO დაამუშავეს OSI (Open System Interconnection) – ღია სისტემების ურთიერთკავშირის მოდელი, რომელმაც დიდი როლი ითამაშა ქსელების განვითარებაში. ამ მოდელის შემუშავებაში გარკვეული როლი ითამაშა შემდეგმა ფაქტორმა. სანამ ამ მოდელზე დაიწყებდნენ ფიქრს, მანამდე კომპანიები რომლებიც იმ დროისთვის აწარმოებდნენ ქსელურ აპარატურას, გასაიდუმლოებულ ვითარებაში ქმნიდნენ პროტოკოლებს რათა გაეერთიანებინათ ქსელური მოწყობილობები. ამიტომ სხვადასხვა მწარმოებელმა შექმნა ინფორმაციის გაცვლის სხვადასხვა დონიანი ინფორმაციის გაცვლის პროტოკოლების სტეკი. აღსანიშნავია ის, რომ სხვადასხვა მწარმოებლის მიერ შექმნილი ქსელური მოწყობილობები ერთმანეთთან ვერ ცვლიდნენ ინფორმაციას. ეს კი იმ პერიოდისთვის მნიშვნელოვანი შემაფერხებელი გარემოება იყო. ამიტომ გახდა საჭირო შემუშავებულიყო ისეთი პროტოკოლების სტეკი, რომელიც საერთო იქნებოდა ყველა სისტემისთვის.

OSI არის ეტალონური მოდელი, რომელმაც მნიშვნელოვანი როლი შეასრულა თანამედროვე კომპიუტერული ქსელების კონცეფციების განვითარებაში. OSI მოდელში ურთიერთქმედების საშუალებები იყოფა შვიდ დონედ: გამოყენებითი, წარმოდგენითი, სეანსის, ტრანსპორტის, ქსელის, არხის და ფიზიკური. ყოველ დონეს სხვადასხვა ქსელური ოპერაციები შეესაბამება. ყოველი დონე გადამცემ კომპიუტერზე მუშაობს ისე, თითქოს ის შეესაბამებოდეს მიმღები კომპიუტერის შესაბამის დონეს. ეს ლოგიკური ანუ ვირტუალური კავშირი ნაჩვენებია ნახ.17-ზე. რეალური კავშირი კი მხოლოდ მეზობელ დონეებს შორის ხორციელდება.

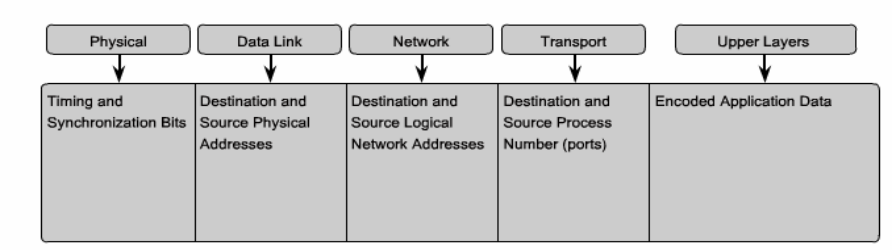


ნახაზი 17. OSI მოდელის ვირტუალური კავშირი

OSI მოდელი აღწერს მხოლოდ სისტემურ საშუალებებს, რომელიც ოპერაციული სისტემისა და სისტემური უტილიტების მიერ არის რეალიზებული.

OSI მოდელი აღწერს პროცესების კოდირებას, ფორმატირებას, სეგმენტაციას და მონაცემთა ენკაფსულაციას, რათა მოხდეს მათი

გადაცემა ქსელში. მონაცემთა ნაკადი, რომელიც იგზავნება გამგზავნიდან ადრესატამდე შესაძლებელია დაიყოს ნაწილებად. მილიონი ასეთი ინფორმაციის ნაწილი მოძრაობს ქსელში დროის ერთ ერთეულში. მნიშვნელოვანია, რომ თითოეული მონაცემთა ნაწილი შეიცავდეს იდენტიფიკაციის საკმარისი რაოდენობის ინფორმაციას, რათა მან მიაღწიოს სწორ მისამართს.



ნახაზი 18. OSI მოდელის დომეების აღწერა

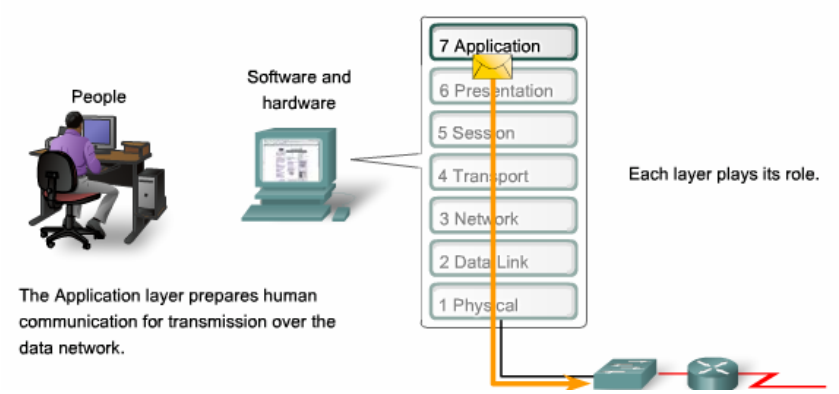
არსებობს სხვადასხვა ტიპის მისამართები, რომლებიც საჭიროა რათა ინფორმაცია წარმატებით იქნას გადაცემული ქსელში. OSI მოდელის გამოყენებით ჩვენ შეგვიძლია ვნახოთ სხვადასხვა მისამართები და იდენტიფიკატორები რომლებიც აუცილებელია თითოეული დონისათვის.

გამოყენება

OSI მოდელი ყოფს ქსელურ ფუნქციებს დონეებად. მისი ყოველი დონე შეიცავს მხოლოდ მისთვის საჭირო ფუნქციებს და ემსახურება მხოლოდ საკუთარი პროცესების ურთიერთქმედებას. ჩვეულებრივ, ქვედა დონეებს ემსახურება აპარატურული ნაწილი, ხოლო ზედა დონეების დამუშავება ხდება პროგრამული მეთოდით.

OSI მოდელს ხშირად იყენებენ კომპიუტერული ქსელების აგებისას. მისი მთავარი თვისებაა სხვადასხვა დონეების ერთმანეთთან დაკავშირება, რაც ასევე უზრუნველყოფს ერთ დონეზე მომუშავე მწარმოებლის მიერ შემუშავებული აპარატურის სხვა დონეზე მომუშავე აპარატურასთან მუშაობას, თუ ამ აპარტურის ყოველი პროტოკოლი დოკუმენტირებულია და მისი აღწერილობა არსებობს. ეს აღწერილობა TCP/IP-ზე მომუშავე საზოგადოებისთვის ჩვეულებრივ ცნობილია როგორც RFC-ს დოკუმენტაცია (Request for Comments).

OSI მოდელი			
	მონაცემების ერთეული	**დონე**	**ფუნქცია**
პროგრამული	მონაცემები	გამოყენებითი	ინფორმაციის მომზადება ქსელში გადასაცემად
		წარმოდგენითი	მონაცემების შიფრაცია და წარდგენა
		სესიის	კვანძთაშორისი კავშირი
	სეგმენტები	ტრანსპორტის	კავშირი ორ უკიდურეს წერტილს შორის და საიმედოობა
აპარატურული	პაკეტები	ქსელის	გზის განსაზღვრა და ლოგიკური დამისამართება (IP)
	კადრები	არხის	ფიზიკური მისამართები (MAC და LLC)
	ბიტები	ფიზიკური	მატარებელი ხაზი(მედია), სიგნალი და ორობითი გადაცემა



ნახაზი 19. OSI დონეებზე ინფორმაციის გადაცემა

დონე 7: გამოყენებითი დონე

გამოყენებითი დონე უზრუნველყოფს ქსელურ პროგრამებს ქსელური სერვისებით. გამოყენებითი დონე ესაა სხვადასხვა პროტოკოლების ნაკრები, რომლის საშუალებით ქსელის მომხმარებელი უკავშირდებიან საერთო რესურსებს, როგორიცაა ფაილები, პრინტერი ან web გვერდები. პროტოკოლების მაგალითებია: Telnet, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) და Hypertext Transfer Protocol (HTTP) პროტოკოლები.

დონე 6: წარმოდგენითი დონე

წარმოდგენითი დონე გარდაქმნის მონაცემებს პროგრამული დონის სტანდარტული ინტერფეისისათვის გასაგებ ენაზე. MIME

კოდირება, მონაცემების შეკუმშვა, მონაცემების კოდირება და ზემდგომი დონის მოთხოვნის ფარგლებში მისი წარმოდგენა. მაგალითად: EBCDIC-ით კოდირებული ტექსტური ფაილის ASCII-კოდირებულ ფაილად გარდაქმნა, ობიექტების და სხვა მონაცემთა სტრუქტურის XML-ში გარდაქმნა და ა.შ.

დონე 5: სესიის დონე

სესიის დონე აკონტროლებს დიალოგს (სესიებს) კომპიუტერებს შორის. ის იწყებს, მართავს და წყვეტს კავშირებს ადგილობრივ და შორეულ პროგრამებთან. ის იძლევა დუპლექსური ან ნახევრადდუპლექსური კავშირის დამყარების საშუალებას და ახდენს საბოლოო კავშირის შესრულების შემოწმებას, რეგულირებას, შეწყვეტას და განახლებას. OSI მოდელში ეს დონე პასუხისმგებელია სესიების "მშვიდობიან დახურვაზე", რაც TCP პროტოკოლის და ინტერნეტიპროტოკოლის უმნიშვნელოვანესი ნაწილია.

დონე 4: ტრანსპორტის დონე

ტრანსპორტის დონე უზუნველყოფს მომხმარებლებს შორის მონაცემების გამჭვირვალე, ეფექტურ გადაცემას და ამ დავალებისგან ზედა დონეების განთავისუფლებას. ტრანსპორტის დონე ამოწმებს საიმედოობას ნაკადების მართვით, სეგმენტირებით/დესეგმენტირებით და შეცდომების შემოწმებით. მეოთხე დონის ზოგიერთი პროტოკოლი მოითხოვს ორმაგი კავშირის დამყარებას. ეს ნიშნავს, რომ ტრანსპორტის დონეს შეუძლია პაკეტების დროებით შენახვა და დანაკარგების შემთხვევაში მათი თავიდან გაგზავნა. მსგავსი პროტოკოლია (TCP) Transmission Control Protocol. ეს არის დონე, რომელიც

გარდაქმნის შეტყობინებებს TCP, (UDP) User Datagram Protocol, (SCTP) Stream Control Transmission Protocol და სხვა პაკეტებში.

დონე 3: ქსელის დონე

ქსელური დონე უზრუნველყოფს მონაცემების მიმდევრობების წყაროდან დანიშნულების ადგილამდე ერთი ან რამოდენიმე ქსელის გავლით გადაცემას ტრანსპორტის დონის მიერ მოთხოვნილი მომსახურების ხარისხის (QoS) დაცვით. ქსელური დონე აწარმოებს ქსელური მარშრუტიზაციის ფუნქციებს, და ასევე შეუძლია სეგმენტირება/დესეგმენტირება და შეცდომების შეტყობინება. მარშრუტიზატორები მუშაობენ სწორედ ამ დონეზე და აგზავნიან პაკეტებს ერთი ქსელიდან მეორეში, რაც საბოლოოდ შეიძლება ქსელის მომხმარებლის ინტერნეტამდე წვდომას უზრუნველყოფდეს (ასევე არსებობს მესამე დონის კომუტატორები (ხშირად მათ IP-კომუტატორებს უწოდებენ). ეს არის მისამართების ლოგიკური სქემა – მნიშვნელობები შეირჩევა ქსელური ინჟინერის მიერ, მისამართების სქემა იერარქიულია. მესამე დონის პროტოკოლის საუკეთესო მაგალითია ინტერნეტიპროტოკოლი (IP).

დონე 2: მონაცემთა გადაცემის არხის დონე

მონაცემთა გადაცემის არხის დონე უზრუნევლყოფს ქსელურ ობიექტებს შორის მონაცემების ელემენტარულ გადაცემას და ფიზიკურ დონეზე მომხდარი შეცდომების აღმოჩენას და შესაძლო აღმოფხვრას. მისამართების სქემა ფიზიკურია (MAC მისამართები) რაც ნიშნავს, რომ ისინი აპარატურულ ნაწილში ფიქსირდება წარმოების დროს. მეორე დონის პროტოკოლის მაგალითიებია: Ethernet, HDLC, ADCCP. (შენიშნვა: IEEE 802 სტანდარტის ლოკალურ ქსელებში და ზოგიერთ არა-IEEE 802 ქსელებში,

მაგალითად FDDI-ში, ეს დონე იყოფა ორად: MAC დონედ და IEEE 802.2 LLC დონედ, ამ დონეზე მუშაობენ ქსელური ხიდები და კომუტატორები. არსებობს არგუმენტი, რის მიხედვითაც ამ დონეს უწოდებენ "2.5 დონეს", რადგან თვისობრივად ის მეორე დონეს მკაცრად არ უტოლდება).

დონე 1: ფიზიკური დონე

ფიზიკური დონე განსაზღვრავს მოწყობილობების ყველა ფიზიკურ და ელექტრულ თვისებებს. ის მოიცავს კაბელების ტიპს, მის განლაგებას, კაბელის პარამეტრებს, ტალღის სიხშირეს და ა.შ. კონცენტრატორები პირველი დონის მოწყობილობებია. ფიზიკური დონის ძირითადი ფუნქცია და დანიშნულებაა:

- ელექტრული კავშირის დამყარება და გაწყვეტა მატარებელთან;
- მრავალ მომხმარებელს შორის საკომუნიკაციო რესურსების ეფექტურად განაწილება. მაგალითად, კავშირის მოთხოვნა და დინების მართვა;
- მოდულაცია, ან ციფრული მონაცემების გადამცემა არხებში გასატარებლად. მაგალითად ეს არის სიგნალები ფიზიკურ კაბელში (როგორც მავთული, ასევე ოპტიკურ-ბოჭკოვანი) და ეთერში.

TCP/IP პროტოკოლი

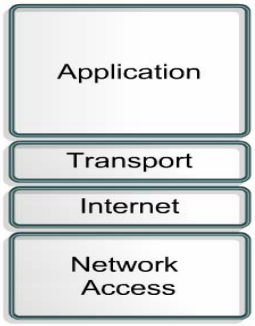
ინტერნეტი შეიქმნა და განვითარდა იმისათვის, რომ მომხდარიყო სხვადასხვა ტიპის ქსელები გააერთიანება. ინტერნეტი მუშაობს TCP/IP პროტოკოლის გამოყენებით. TCP/IP პროტოკოლის დიზაინი იდელაურია ინტერნეტის დეცენტრალიზაციისა და განვითარებისთვის.

საჭიროა ვიცოდეთ ორივე TCP/IP და OSI ქსელური მოდელი. ყოველ მოდელს გააჩნია საკუთარი სტრუქტურა, თუ როგორ უნდა იმუშაოს ქსელმა. მაგრამ ორივე მოდელს ასევე აქვს ბევრი საერთო.

მოწყობილობა რომელსაც სურს ინტერნეტთან დაკავშირება უნდა გააჩნდეს უნიკალური იდენთიფიკატორი. იდენთიფიკატორი ცნობილია როგორც IP მისამართი. მიმდინარე IP ვერსია არის IPv4.

ყოველ კომპიუტერს, გარდა ფიზიკური მისამამართის (MAC) სჭირდება დამატებით IP მისამართი, რომელიც არის ინტერნეტის ნაწილი. არსებობს რამოდენიმე გზა IP მისამართის მისანიჭებლად. ზოგ მოწყობილობას ენიჭება მუდმივად, ზოგს დინამიურად, ინტერნეტში შესვლის დროს.

ამერიკის თავდაცვის დეპარტამენტმა შექმნა TCP/IP მოდელი, რადგანაც მას ჭირდებოდა ქსელი რომელიც გადაიტანდა ინფორმაციას სხვადასხვა ადგილას. ამ მიზნით მათ შექმნეს საიმედო გადაცემის პროტოკოლი რომელიც საფუძვლად დაედო შემდგომში ინტერნეტს.



ნახაზი 20. TCP/IP მოდელი

TCP/IP მოდელი შედგება 4 დონისგან: გამოყენებითი; ტრანსპორტის; ინტერნეტის და ქსელში შეღწევის დონე. ზოგიერთ TCP/IP მოდელის დონეს აქვს საერთო დასახელება, როგორიც აქვს OSI მოდელს. TCP/IP მოდელი იქნა სტანდარტიზებული 1981 წლის სექტემბერში.

გამოყენებითი დონე

გამოყენებითი დონეში შედის მაღალი დონის პროტოკოლები, რომლებიც უზრუნველყოფენ მონაცემების წარმოდგენას, კოდირებას და სეანსის კონტროლს. ამ დონის პროტოკოლებია:

- **File Transfer Protocol (FTP)** - FTP არის კავშირზე ორიენტირებული, გარანტირებული გადაცემის სერვისი, რომელიც ტრანსპორტის დონეზე იყენებს TCP პროტოკოლს;
- **Trivial File Transfer Protocol (TFTP)** – TFTP არის კავშირზე არაორიენტირებული, არაგარანტირებული გადაცემის სერვისი, რომელიც ტრანსპორტის დონეზე იყენებს UDP პროტოკოლს;

- **Simple Mail Transfer Protocol (SMTP)** – SMTP უზრუნველყოფს ელექტრონული ფოსტის გადაგზავნას ქსელის საშუალებით;

- **Telnet** – Telnet უზრუნველყოფს ერთი კომპიუტერიდან მეორე კომპიუტერში შესვლას და ბრძანებების გაშვებას რომელის სრულდება დაშორებულ კომპიუტეერში.

ტრანსპორტის დონე

ტრანსპორტის დონე უზრუნველყოფს ლოგიკურ კავშირს ინიციატორ ჰოსტსა და ადრესატ ჰოსტს შორის. სატრანსპორტო პროტოკოლი უკეთებს სეგმენტაციას ზედა დონის პროტოკოლიდან მოსულ ბაიტურ ნაკადს და უზრუვველყოფს მის ასწყობას მეორე მხარეს, რათა გადასცეს ის ზედა დონეს მთლიან ინაკადად.

ტრანსპორტის დონის ძირითადი ფუნქციაა - უზრუნველყოს გადაცემაში მონაწილე ჰოსტებს შორის კონტროლი და მონაცემების გარანტირებული გადაცემა ქსელში. ტრანსპორტის დონის პროტოკოლებია TCP და UDP.

TCP და UDP ფუნქციები:

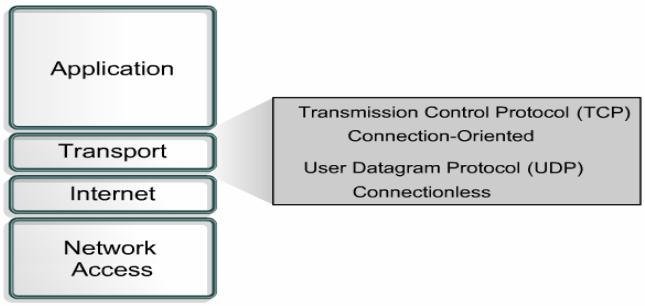
- გამოყენებითი დონის მონაცემების სეგმენტაცია;

- სეგმენტების გადაცემა ერთი ჰოსტიდან მეორეში.

TCP ფუნქციაა:

- ჰოსტებს შორის კავშირის დამყარება;

- მონაცემთა ნაკადის მართვა მცოცავი ფანჯრის გამოყენებით;
- საიმედოობის უზრუნველყოფა სპეციალური სისტემის გამოყენებით.



ნახაზი 21. ტრანსპორტის დონე

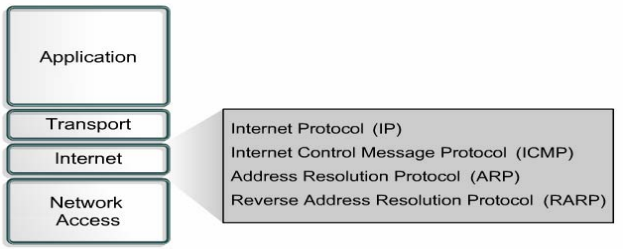
ინტერნეტის დონე

ინტერნეტის დონის ფუნქციაა უზრუნველყოს საუკეთესო გზის არჩევა ინტერნეტში პაკეტების მარშუტიზაციისას. მთავარი პროტოკოლი რომელიც ამ დონეზე მუშაობს არის IP.

TCP/IP-ში ინტერნეტის დონეზე მუშაობს შემდეგი პროტოკოლები:M

- IP უზრუნველყოფს კავშირზე არაორიენტირებულ, მაგრამ საუკეთეესო გზით პაკეტების გადაცემას;
- Internet Control Message Protocol (ICMP) უზრუნველყოფს კონტროლისა და შეტყობინებების გაგზვნას;

- Address Resolution Protocol (ARP) უზრუველყოფს IP მისამართის საშუალებით ფიზიკური MAC მისამართის დადგენას;
- Reverse Address Resolution Protocol (RARP) უზრუველყოფს IP მისამართის დადგენას ცნობილი ფიზიკური MAC მისამართის საშუალებით.



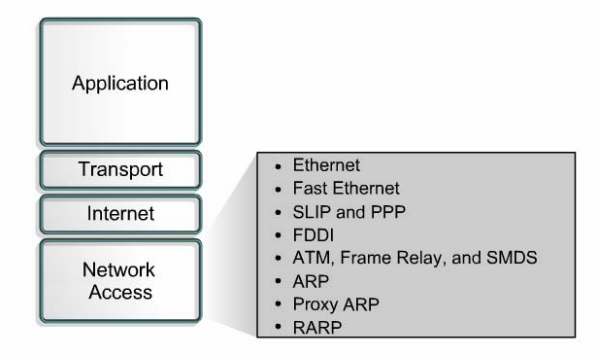
ნახაზი 22. ინტერნეტის დონე

IP წყვეტს შემდეგ ოპერაციებს:

- განსაზღვრავს პაკეტების დამისამართების სქემას;
- უზრუნველყოფს მონაცემების გადაცემას ინტერნეტის დონიდან ქსელური შეღწევის დონეზე;
- უზრუნველყოფს პაკეტების მარშუტიზაციას.

ქსელში შეღწევის დონე

ქსელში შეღწევის დონე უზრუნველყოფს პაკეტების გადაცემას ფიზიკურ გარემოში. ამ დონეზე მუშაობს, როგორც ლოკალური ასევე გლობალური ქსელის ტექნოლოგიები.



ნახაზი 23. ქსელში შეღწევის დონე

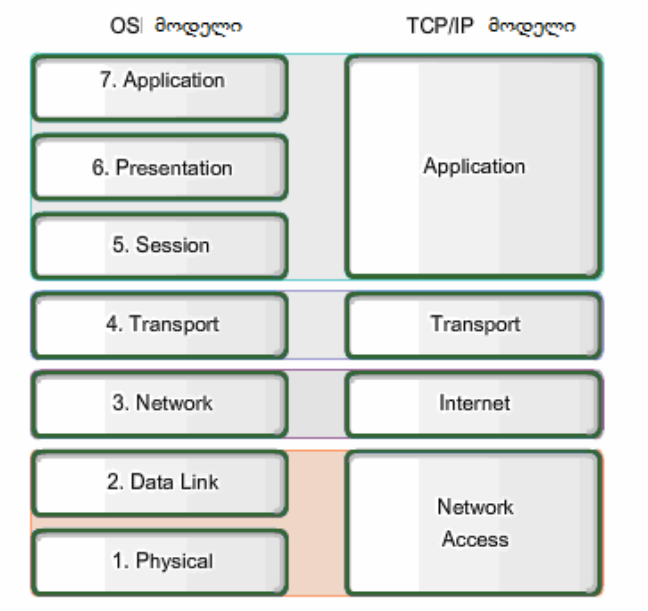
ქსელში შეღწევის დონე აგრეთვე აკეთებს IP პაკეტების ენკაპსულაციას ფრეიმებში. ეს დონე განსაზღვრავს ფიზიკური მედიის კავშირის ტიპს დამოკიდებულს ფიზიკურ მოწყობილობაზე და ქსელურ ინტერფეისზე.

შედარება OSI და TCP/IP მოდელს შორის

პროტოკოლები რომლებიც შედიან TCP/IP მოდელის შენადგენლობაში შესაძლებელია იქნან აღწერილი OSI მოდელის განმარტებით. OSI მოდელში ქსელში შეღწევის დონე და TCP/IP მოდელის გამოყენებითი დონე არის დაყოფილი რათა აღვწეროთ ფუნქციები რომლებსაც ადგილი ექნებათ ამ დონეებზე.

ქსელური შეღწევის დონეზე TCP/IP პროტოკოლების ნაკრები არ განსაზღვრავს თუ რომელი პროტოკოლი გამოიყენება ფიზიკურ გარემოში ინფორმაციის გადასაცემად. ის მხოლოდ აღწერს დამოკიდებულებას ინტერნეტ დონიდან ქსელის ფიზიკურ პროტოკოლებამდე. OSI მოდელის 1 და 2 დონეები განიხილავენ აუცილებელ პროცედურებს, რათა მიიღონ შეღწევის უფლება

მედიაზე და ფიზიკურ საშუალებებზე, რათა გააგზავნოს მონაცემი ქსელში.



ნახაზი 24. OSI და TCP/IP მოდელების შედარება

ძირითადი განსხვავება ორ ქსელურ მოდელს შორის ხდება OSI მოდელის 3 და 4 დონეზე. OSI მოდელის 3 დონე ეს არის ქსელური დონე, რომელიც უნივერსალურად გამოიყენება რათა განიხილოს და დოკუმენტაცია გაუკეთოს პროცესების დიაპაზონს, რომლებიც ხდება ყველა ინფორმაციის გადამცემ ქსელში, რათა დაამისამართოს და დაამარშუტიროს შეტყობინება ქსელში გადასაცემად. ინტერნეტ პროტოკოლი (IP) წარმოადგენს TCP/IP პროტოკოლების ნაკრებს, რომელიც შეიცავს 3 დონის ფუნქციონალურ შესაძლებლობებს.

OSI მოდელის 4 დონე არის ტრანსპორტის დონე. იგი ხშირად გამოიყენება რათა აღიწეროს საერთო ფუნქციები ან მომსახურებები, რომელსაც განსაზღვრავენ (მართავენ) გამგზავნი და მიმღები ჰოსტები ერთმანეთში ინდივიდუალური ურთიერთობისას. ეს ფუნქციები შეიცავენ დასტურს (acknowledgement), შეცდომების აღმოფხვრას (error recovery) და თანმიმდევრობას(sequencing). ამ დონეზე TCP/IP პროტოკოლების TCP (Transmission Control Protocol) და UDP (User Datagram Protocol) პროტოკოლები უზრუნველყოფენ აუცილებელ ფუნქციებს.

TCP/IP გამოყენებითი დონე შეიცავს ბევრ პროტოკოლს, რომლებიც უზრუნველყოფენ სპეციფიურ ფუნქციონალურ შესაძლებლობებს.

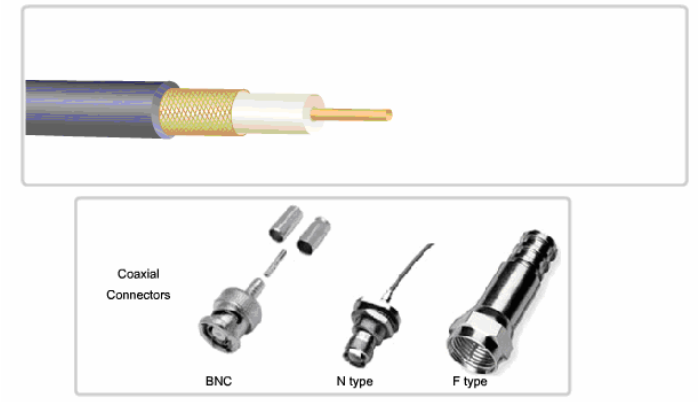
ფიზიკური დონე

ინფორმაციის გადაცემის გარემო ესაა კომპიუტერების ერთმანეთთან დაკავშირების საშუალება, რომლითაც ხდება ინფორმაციის გაცლა. კომპიუტერულ ქსელებში გადაცემის გარემოდ გამოყენებულია კაბელები და უგამტარო კავშირები.

არსებობს კაბელების სამი ძირითადი ტიპი: კოაქსიალური, ხვეული წყვილი და ოპტიკურბოჭკოვანი

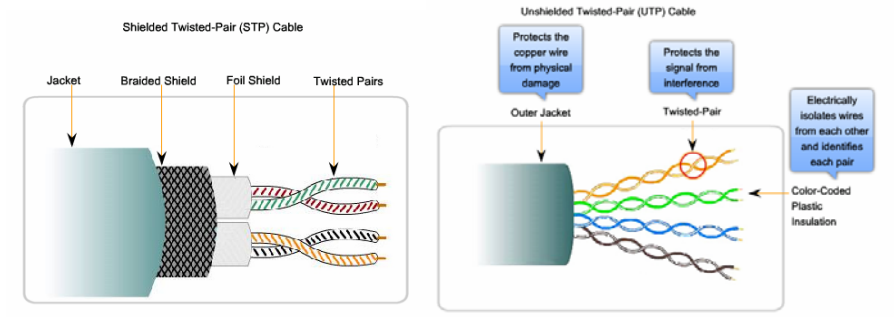
კოაქსიალური კაბელი ყველაზე მეტად იყო გავრცელებული მისი სიიაფის, სიმსუბუქის და გამოყენებისთვის მოხერხებულობის გამო, ასევე მისი დაყენების სიმარტივის გამო. მარტივი კოაქსიალური კაბელი შედგება სპილენძის გამტარისაგან, იზოლაციისაგან, რომელიც ირგვლივ აქვს გამტარს, მეტალური

წნულისაგან (ეკრანისაგან) და გარეთა გარსისაგან. ზოგჯერ მეტალური წნულის გარდა აქვს ფოლგის ფენა. მაშინ მას ქვია კაბელი ორმაგი ეკრანიზაციით. ძლიერი შეფერხებების დროს შეიძლება გამოყენებული იქნას კაბელი ოთხმაგი ეკრანიზაციით. იგი შედგება ფოლგის ორი ფენისაგან და მეტალური წნულის ორი ფენისაგან. ელექტრული სიგნალები გადაიცემა გამტარში. გამტარი მზადდება სპილენძისაგან. გამტარი გარშემორტყმულია დიალექტრიკული ფენით, რომელიც მას მეტალური წნულისაგან გამოყოფს. "წნული" მიწის როლს ასრულებს და იგი იცავს გამტარს ელექტრული სიგნალისაგან და გადამკვეთი შეფერხებებისაგან. გადამკვეთი შეფერხებები ესაა ელექტრული დაზიანება, რომელსაც იწვევს მეზობელ გამტარებში სიგნალები. გამტარი და მეტალის წნული ერთმანეთს არ უნდა ეხებოდეს, რადგან წარმოიქმნება მოკლე ჩართვა და მონაცემები დამახინჯდება. კოაქსიალური კაბელი შეფერხებების მიმართ უფრო მდგრადია ვიდრე ხვეულა წყვილი. მასში სიგნალების მილევა უფრო მცირეა. სიგნალის მილევა – ეს არის სიგნალების შესუსტება მისი კაბელში გავლისას.



ნახაზი 25. კოაქსიალური კაბელი

არსებობს კოაქსიალური კაბელის ორი ტიპი: წვრილი კოაქსიალური კაბელი (Thinnet) და მსხვილი კოაქსიალური კაბელი (Thicknet). წვრილი კოაქსიალური კაბელი მოქნილი კაბელია დიამეტრით 0.5 სმ-დე. იგი გამოიყენება ნებისმიერი ტიპის ქსელისთვის და უშუალოდ უერთდება ქსელის ადაპტერის პლატას. ასეთ კაბელებს დაუმახინჯებლად ინფორმაციის გადაცემა შეუძლია 185 მ-დე. სქელი კოაქსიალური კაბელი შედარებით ხისტი კაბელია დიამეტრით 1სმ-მდე. რაც მეტია სასიგნალო გამტარის სისქე, მით მეტ მანძილზე შეუძლია მას სიგნალების გადაცემა დაუმახინჯებლად. სქელ კოაქსიალურ კაბელს მონაცემთა გადაცემა დაუმახინჯებლად შეუძლია 500 მეტრამდე მანძილზე. ამიტომ მას იყენებენ როგორც მაგისტრალი, რომელიც რამდენიმე პატარა ქსელს ერთმანეთთან აერთიანებს. ასეთი კაბელების მისაერთებლად ქსელის ადაპტერის პლატასთან გამოიყენება ტრანსივერი.

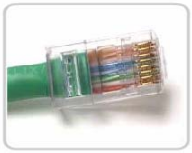


ნახაზი 26. STP და UTP კაბელები

ყველაზე მარტივი ხვეულა წყვილი არის ორი ერთმანეთისგან გამოყოფილი სასიგნალო გამტარი. არსებობს ხვეულა წყვილის ორი ტიპი: ეკრანირებული(STP), როდესაც სპილენძის გამტარები

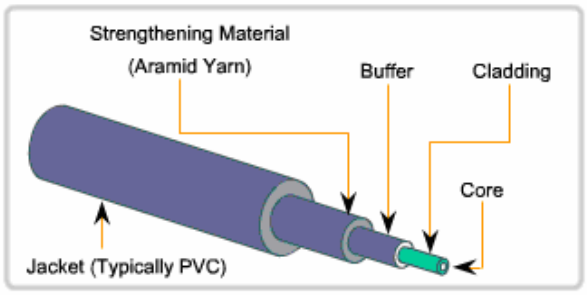
ერთმანეთისგან იზოლაციით (ეკრანით) არიან გამოყოფილი და არაეკრანირებული (UTP), როდესაც ეკრანი არ არსებობს.

ხვეულა წყვილის მისაერთებლად კომპიუტერთან გამოიყენება კონექტორი RG-45.



ნახაზი 27. კონექტორი RG-45

ოპტიკურბოჭკოვანი კაბელში მონაცემთა გადაცემა ხდება მოდულირებული სინათლის იმპულსების სახით. იგი მონაცემთა გადაცემის შედარებით დაცული ხერხია.



ნახაზი 28. ოპტიკურბოჭკოვანი კაბელი

ასეთი ტიპის ხაზები გამოიყენება დიდი მოცულობის მონაცემების გადასაცემად მაღალი სისწრაფით (10 გიგაბაიტი და მეტი). მათში სიგნალების მილევა და დამახინჯება თითქმის არ ხდება. ოპტიკური ბოჭკო – წვრილი შუშის ცილინდრია (5-60 მიკრონი),

რომელსაც ქვია სასიგნალო გამტარი და რომელიც დაფარულია სარკის მაგვარი შავი ფენით.

ძირითადად ყოველი ოპტიკური ბოჭკო სიგნალს გადაცემს ერთი მიმართულებით, ამიტომ ყოველი კაბელი შედგება მინიმუმ ორი ოპტიკური ბოჭკოსგან, რომლებსაც აქვთ დამოუკიდებელი კონექტორები. ერთი გამოიყენება გადასაცემად, მეორე – მიმღებად.

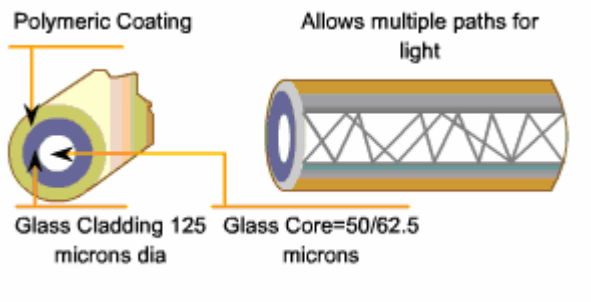
ნახაზი 29. ოპტიკურბოჭკოვანი კაბელის დიზაინი

დღეს-დღეობით, კომპიტერულ ქსელებში გამოიყენება სამივე ტიპის კაბელი, მაგრამ ყველაზე პერსპექტიულია ოპტიკურ-ბოჭკოვანი კაბელი. იგი გამოიყენება მაგისტრალების ასაგებად.

ოპტიკურ-ბოჭკოვანი კაბელი არის ორი ტიპის: ერთმოუდიანი და მრავალმოუდიანი.

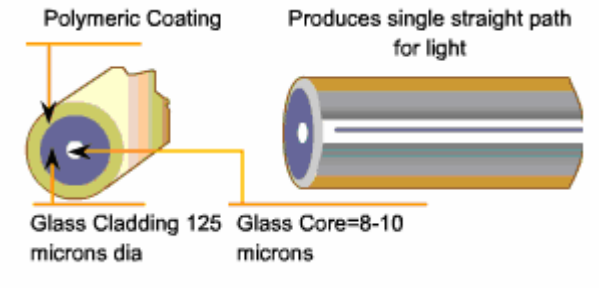
მრავავალმოუდიანი ოპტიკური კაბელი ატარებს სხივის რამოდენიმე კონას, რაც მნიშვნელოვან შეფერხებას იწვევს დიდ მანძილზე სიგნალის გადაცემისას. ამიტომ როგორც წესი ის გამოიყენება 2კმ მანძილის ფარგლებში.

ბოჭკოსი და მისი გარსაკრავის მიხედვით არსებობს ორი ტიპის კაბელი 125/62.5 და 125/50 მიკრონი. 125 მიკრონი არის გარსაკრავის დიამეტრი, ხოლო 50 და 62.5 ბოჭკოსი.



ნახაზი 30. მრავალმოუდიანი ოპტიკური კაბელი

ერთმოუდიანი ოპტიკური კაბელი ატარებს სხივის მხოლოდ ერთ კონას, ამიტომ სხივი ფაქტიურად დაბრკოლების გარეშე მოძრაობს გამტარში. ასეთი ტიპის კაბელების გამოყენება შესაძლებელია დიდ მანძილზე. როგორც წესი ის გამოიყენება 100კმ მანძილის ფარგლებში. ოპტიკური ბოჭკოსა და მისი გარსაკრავის მიხედვით არის 125/10 მიკრონიანი კაბელი. 125 მიკრონი არის გარსაკრავის დიამეტრი, ხოლო 10 ოპტიკური ბოჭკოსი.



ნახაზი 31. ერთმოუდიანი ოპტიკური კაბელი

ოპტობოჭკოვანი კაბელით გადაცემაზე არ მოქმედებს ელექტრუ-ლი შეფერხებები, ნაკლებია სიგნალის დამახინჯება და მილევა. ამიტომ გადაცემა ხდება ძალიან მაღალი, წამში ასობით მეგაბიტი

სიჩქარით, რომლის თეორიული ზღვარი 200000მბ/წმ-ის ტოლია. სინათლის იმპულსი დაუმახინჯებლად ვრცელდება დიდ მანძილზე.

უგამტარო შეერთებები გამოიყენება მონაცემთა გადასაცემად ლოკალურ გამოთვლით ქსელებში, გაფართოებულ ლოკალურ გამოთვლით ქსელებში და მობილურ ქსელებში. ტიპიური უგამტარო ქსელი მუშაობს ისე როგორც კაბელური ქსელი. უგამტარო ადაპტერის პლატა ყენდება ყოველ კომპიუტერზე და მომხმარებლები მუშაობენ ისე თითქოს კომპიუტერები შეერთებულნი არიან კაბელის საშუალებით.

უსადენო ლოკალურ ქსელებში გამოყენებულია მონაცემთა გადაცემის ოთხი პრინციპი:

- ინფრაწითელი გამოსხივება;
- ლაზერი;
- რადიო გადაცემა ვიწრო ზოლში;
- რადიო გადაცემა ფართო ზოლში.

ინფრაწითელი და ლაზერული გადაცემები მოითხოვენ ობიექტის პირდაპირ ხედვას. გადამცემი და მიმღები უნდა ,,ხედავდნენ˜ ერთმანეთს.

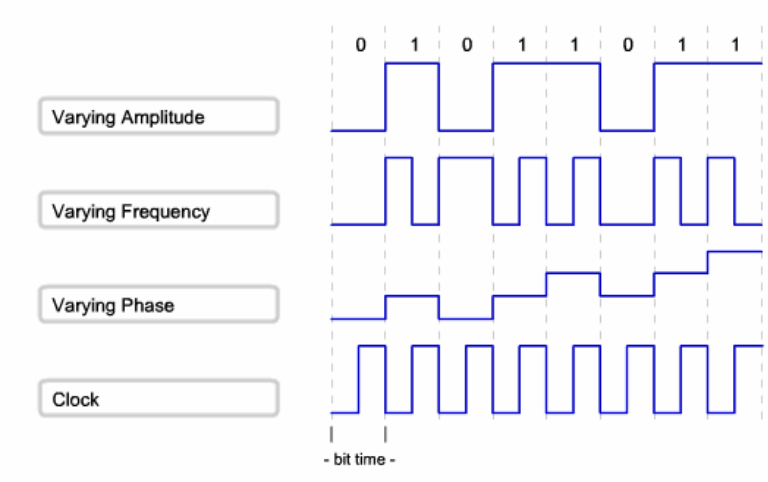
უსადენო მობილურ ქსელებში გადაცემის გარემოდ გამოყენებულია სატელეფონი სისტემები, რომლებშიც ჩართულია პაკეტური რადიოგადაცემა, ფიჭური ქსელი და თანამგზავრის სადგურები.

უსადენო ქსელების დანერგვა განსაკუთრებით ისეთ ადგილებშია მიზანშეწონილი, რომლებშიც საკაბელო ინფრასტრუქტურა სუსტად არის განვითარებული.

უგამტარო ქსელი იყენებს ინფრაწითელ გამოსხივებას, ლაზერს, ვიწრო დიაპაზონის ან ფართო სპექტრის რადიო გადაცემებს.

სიგნალების გადაცემა

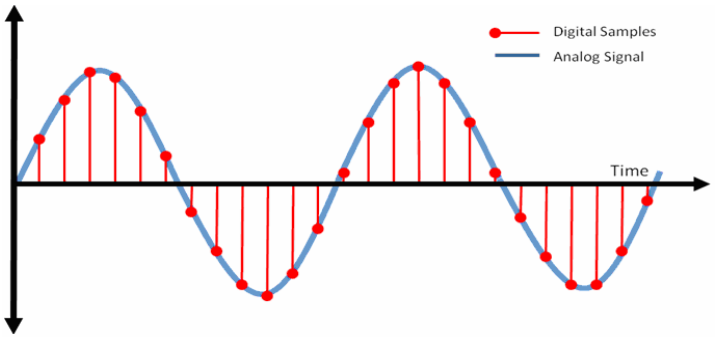
კოდირებული სიგნალების გადასაცემად კაბელში გამოიყენება არამოდულირებული და მოდულირებული გადაცემა.



ნახაზი 32. არამოდულირებული გადაცემა (ციფრული სიგნალი)

არამოდულირებული სისტემები მონაცემებს გადასცემენ ციფრული სიგნალების სახით. სიგნალები წარმოადგენენ ელექტრულ დისკრეტულ ან სინათლის იმპულსებს.

კომუნიკაციური არხის მთელი მოცულობა გამოიყენება ერთი იმპულსის გადასაცემად გატარების ზოლზე. კაბელში სიგნალის გავლისას ხდება მისი თანდათანობითი მილევა. თუ კაბელი ძალიან გრძელია სიგნალი შეიძლება ისე მიილიოს, რომ მისი გამოცნობა შეუძლებელი გახდეს. ამის თავიდან ასაცილებლად, არამოდულირებულ სისტემებში, გამოიყენება გამმეორებელი, რომელიც აღადგენს სიგნალებს და ისე გადასცემს ქსელში.



ნახაზი 33. მოდულური გადაცემა (ანალოგური სიგნალი)

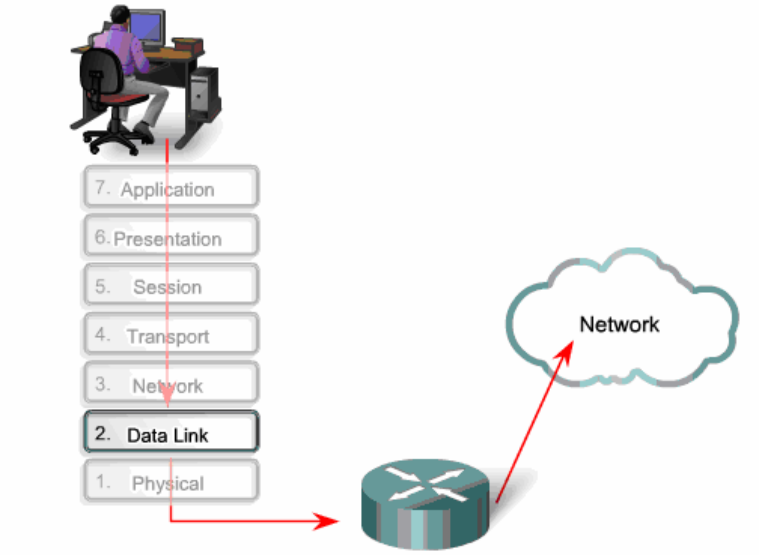
მოდულირებული გადაცემისას სისტემები გადაცემენ მონაცემებს ანალოგური სიგნალების სახით. მოდულირებული სიგნალების გადაცემისას სიგნალების აღსადგენად გამოიყენება გამაძლიერებელი.

დისკრეტული მონაცემების გადასაცემად სატელეფონო ხაზებში გამოიყენება ანალოგური მოდულაცია, რომელიც ხდება მოდემის საშუალებით. მოდემი, გადამცემი კომპიუტერის მხრიდან მიღებულ ციფრულ სიგნალს გარდაქმნის ანალოგურ სიგნალად, ანუ აკეთებს მოდულაციას, ხოლო მიმღები მოდემი მიღებულ ანალოგურ სიგნალს გარდაქმნის ციფრულ სიგნალად, ან ანხორციელებს დემოდულაციას.

არხის დონე

მონაცემთა არხის დონე გვაძლევს საშუალებას მონაცემები გავცვალოთ საერთო ლოკალურ გამტარზე. ის აწარმოებს ორ ძირითად მომსახურეობას:

- აძლევს საშუალებას ზედა დონეებს, განახორციელონ წვდომა გამტარზე ისეთი ხერხების გამოყენებით როგორიც არის ”framing ” ფრეიმების ფორმირება;
- მართავს, თუ როგორ ხდება მონაცემების გაგზავნა და მიღება გამტარზე ისეთი ხერხების გამოყენებით, როგორიცაა გამტარზე დაშვების კონტროლი და შეცდომების აღმოჩენა (Media Access Control and Error Detection).



ნახაზი 34. მონაცემთა არხის დონე

ისევე როგორც სხვა OSI მოდელის დონეებში, ასევე ამ დონეშიც არის გარკვეული მახასიათებლები, როგორიცაა:

- ფრეიმი (Frame) - არხის დონის პაკეტის მონაცემთა ერთეული (PDU- Packet Data Unit);
- ჰოსტი (Node) - მეორე დონის დასახელება ქსელური მოწყობილობებისა, რომლებიც დაკავშირებული არიან საერთო გამტარზე;
- გამტარი (Media/medium) - ფიზიკური საშუალება ორ კვანძს შორის სიგნალის გადასაცემად;
- ქსელი - ორი ან მეტი ჰოსტი ერთმანეთთან დაკავშირებული საერთო გამტარით.

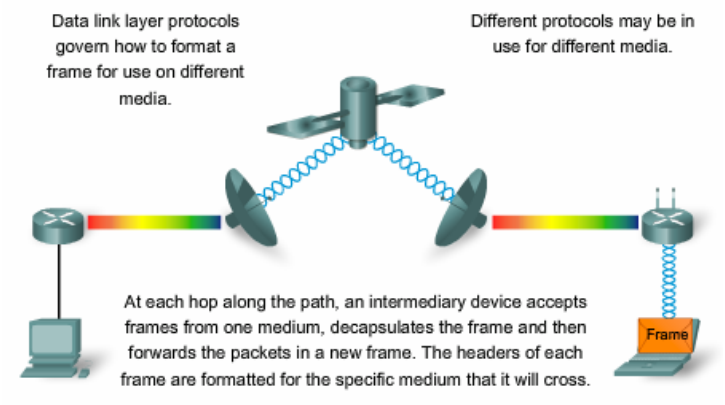
მონაცემთა არხის დონე პასუხისმგებელია ჰოსტებს შორის ფრეიმების ფიზიკური ქსელის გამტარში გადაცემაზე.

შენიშვნა:

* აუცილებელია ამ თავის კონტექსტში გავიაზროთ სიტყვა გამტარის მნიშვნელობა. აქ ეს სიტყვა არ ნიშნავს იმ მასალას, რომელზეც მოგზაურობს ინფორმაციის აღმნიშვნელი სიგნალი. ის შეიძლება იყოს სპილენძის კაბელი, ოპტიკურ-ბოჭკოვანი კაბელი, ან თუნდაც ატმოსფერო.

* ფიზიკური ქსელი განსხვავდება ლოგიკური ქსელისაგან. ლოგიკური ქსელები იქმნებიან ქსელურ დონეზე იერარქიული დამისამართების სქემის გამოყენებით, ხოლო ფიზიკური ქსელი წარმოადგენს ურთიერთ დაკავშირებულ კვანძებს საერთო გამტარზე. ზოგჯერ ფიზიკურ ქსელს ასევე უწოდებენ ქსელურ სეგმენტს (Network Segment).

როგორც ზემოთ იყო აღნიშნული ქსელური მოდელი საშუალებას აძლევს თითოეულ დონეს იფუნქციონიროს მინიმალური დამოკიდებულებით სხვა დონეებთან. მონაცემთა არხის დონე ათავისუფლებს ზედა დონეებს მონაცემთა გაგზავნის და მიღების პასუხისმგებლობიდან. ეს დონე გვაწვდის მომსახურეობას კომუნიკაციის მხარდასაჭერად თითოეულ გამტარზე, რომელზე უნდა მოხდეს მონაცემების გადაცემა. ქსელური დონის პაკეტების გადაცემისას, პაკეტმა შესაძლებელია გაიაროს რამდენიმე სხვადასხვა ტიპის გამტარი, ამ დროს მესამე დონის მოწყობილობა, როგორც წესი-მარშრუტიზატორი, როდესაც მიიღებს ფრეიმს მოახდენს მის დეკაპსულაციას და შემდეგ გააგზავნის ახალ ფრეიმს სხვა ქსელური სეგმენტის შესაბამის გამტარზე.



ნახაზი 35. მონაცემთა არხის დონე

წარმოვიდგინოთ კომუნიკაცია ორ კომპიუტერს შორის, რომელთაგან ერთი მდებარეობს ტოკიოში, ხოლო მეორე პარიზში. იმის მიუხედავად, რომ კომპიუტერები იყენებენ ალბათ ერთნაირ მესამე დონის პროტოკოლს (IP), ინფორმაციას შეიძლება შეხვდეს ბევრი სხვადასხვა ტიპის გამტარი და ტექნოლოგია. ამის გამო

საჭიროა მონაცემთა არხის დონეს ქონდეს დიდი რაოდენობით სხვადასხვა ტექნოლოგიის მხარდაჭერა .

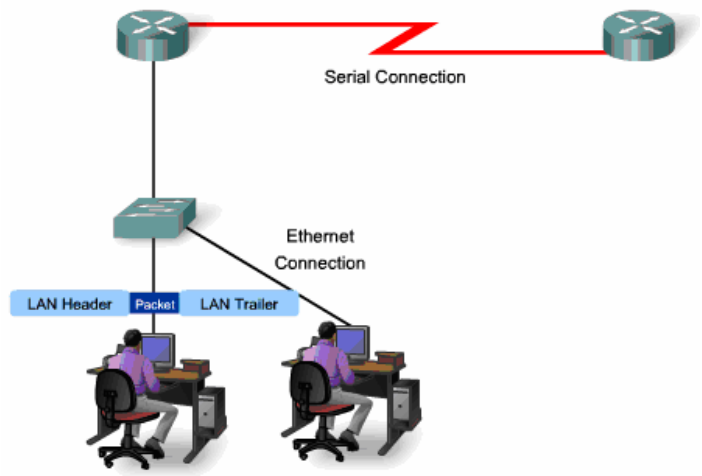
მონაცემთა არხის დონე ეფექტურად ახდენს იზოლირებას ზედა დონის კომუნიკაციის პროცესებსა და გამტარში გადაცემას შორის. როდესაც ხდება პაკეტის მიღება და გადაგზავნა ზედა დონეზე მაგ. IPv4 ან IPv6-ზე, მათ არ სჭირდებათ იცოდნენ თუ როგორი ტიპის გამტარიდან იქნა მიღებული პაკეტი.

მონაცემთა არხის დონე რომ არ არსებობდეს, ქსელურ პროტოკოლს მაგ. IP-ს მოუწევდა ქონოდა ყველა ტიპის გამტარის მხარდაჭერა და ახალი ტექნოლოგიების გამოსვლის შემდეგ მოუწევდა მოეხდინა მასთან ადაპტირება. ეს პროცესი შეაფერხებდა ინოვაციას და ქსელური ტექნოლოგიების განვითარებას. ეს არის მრავალ დონიანი მოდელის ერთერთი უმნიშვნელოვანესი უპირატესობა.

მონაცემთა არხის დონეს უნდა ჰქონდეს ყველა ტიპის გამტარის მხარდაჭერა რომელიც არსებობს. მრავალფეროვნების გამო რთული იქნებოდა მოგვეყვანა მაგალითი. შესაბამისად ნებისმიერ კონკრეტულ პროტოკოლს შეიძლება ჰქონდეს ან არ ჰქონდეს ყველა ტიპის სერვისის მხარდაჭერა რომლებიც გამოიყენება არხის დონეზე.

მეორე დონის პროტოკოლები საზღვრავენ პაკეტის ენკაპსულაციას კადრში და მისი გაგზავნა-მიღების ხერხს. მონაცემების გაგზავნა-მიღების ხერხს ეწოდება გამტარზე წვდომის კონტროლის მეთოდი (Media Access Control Method). იმისთვის რომ მოხდეს მონაცემის გადაგზავნა რამდენიმე სხვადასხვა გამტარზე, შეიძლება მოგვიწიოს სხვადასხვა ტიპის წვდომის კონტროლის მეთოდის გამოყენება ერთი კომუნიკაციის პერიოდში. თითოეული

ქსელური გარემო რომელზეც პაკეტები მოგზაურობენ შეიძლება ფლობდეს სხვადასხვა ტიპის მახასიათებლებს. მაგ. ერთ ქსელში გარემო შეიძლება შედგებოდეს მრავალი ჰოსტისაგან, რომლებიც შეჯიბრებითობის პრინციპით ცდილობენ მოიპოვონ პრიორიტეტი მონაცემების გადასაგზავნად, ხოლო სხვა გარემო შეიძლება შეიცავდეს მხოლოდ ორ ერთმანეთთან დაკავშირებულ კვანძს და მონაცემები მუდმივად მოგზაურობდნენ მათ შორის რიგობრივი წესით.



ნახაზი 36. ფრეიმების გადაცემა

გამტარზე წვდომის კონტროლის მეთოდები აღწერილები მონაცემთა არხის დონის პროტოკოლზე განსაზღვრავენ პროცესს რომლის მიხედვითაც ქსელურ მოწყობილობებს შეუძლიათ წვდომა განახორციელონ და კადრები გადასცენ სხვადასხვა ტიპის ქსელურ გარემოებში.

ჰოსტი რომელიც არის ”ბოლო მოწყობილობა” (End Device) ქსელთან დასაკავშირებლად იყენებს ადაპტერს. მაგ. ლოკალურ ქსელთან დასაკავშირებლად მოწყობილობა იყენებს შესაფერის ქსელურ ადაპტერს. ადაპტერი მართავს ფრეიმის მომზადებას ”Framing” და გამტარზე წვდომის კონტროლს.

შუამავალი მოწყობილობები, როგორიც არის მარშრუტიზატორი, იყენებს სხვადასხვა ფიზიკურ ინტერფეისებს პაკეტის ფრეიმში’ შესაფუთად (ენკაპსულაცია), რადგანაც მასთან შეიძლება იყოს დაკავშირებული სხვადასხვა გამტარი სხვადასხვა ქსელში. მაგ. მარშრუტიზატორს შეიძლება ჰქონდეს Ethernet პორტი, რომლითაც უკავშირდება ლოკალურ ქსელს და სერიალური პორტი რომლითაც უკავშირდება ფართო არის ქსელს. როდესაც მარშრუტიზატორი მიიღებს ფრეიმს ის გაუკეთებს მას დეკაპსულაციას, შედეგად მიიღებს მესამე დონის პაკეტს. შემდგომ შეფუთავს მას ისე, როგორც სჭირდება სხვა ქსელში გადასაგზავნად.

ფრეიმის აღწერა თითოეული არხის დონის პროტოკოლისთვის არის მთავარი ელემენტი. ყველა არხის დონის პროტოკოლებს ესაჭიროებათ საკონტროლო ინფორმაცია რათა იმუშაონ უშეცდომოდ.

საკონტროლო ინფორმაცია შესაძლოა შეიცავდეს :

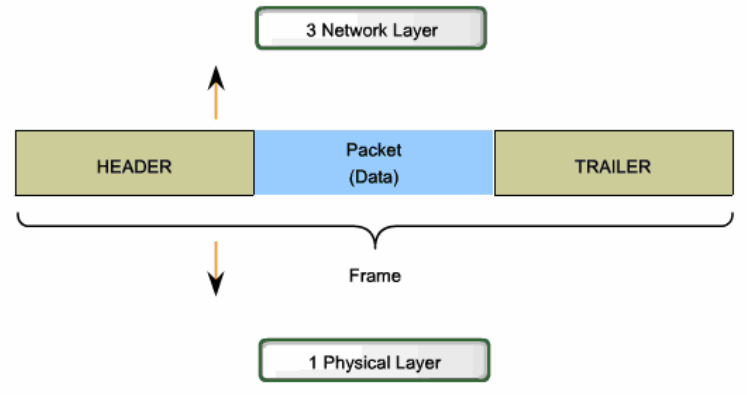
- რომელი კვანძები უკავშირდებიან ერთმანეთს;
- როდის იწყება კავშირი ინდივიდუალურ კვანძებთან და როდის მთავრდება;
- რა შეცდომები მოხდება კავშირის დროს;

- რომელი კვანძები დაამყარებენ კავშირს შემდეგნი.

მონაცემთა არხის დონე ამზადებს პაკეტს ლოკალურ გამტარზე გადასაცემად, და შეფუთვისას ფრეიმს უმატებს თავსართს და ბოლოსართს.

მონაცემთა არხის ფრეიმი შეიცავს :

- Data - მონაცემი (მესამე დონის პაკეტი);
- Header - თავსართი (თავსართის საკონტროლო ინფორმაცია , ადრესაცია. იგი განლაგებულია ფრეიმის დასაწყისში);
- Trailer - ბოლოსართი (შეიცავს საკონტროლო ინფორმაციას რომელიც არის დამატებული ფრეიმის ბოლოს).

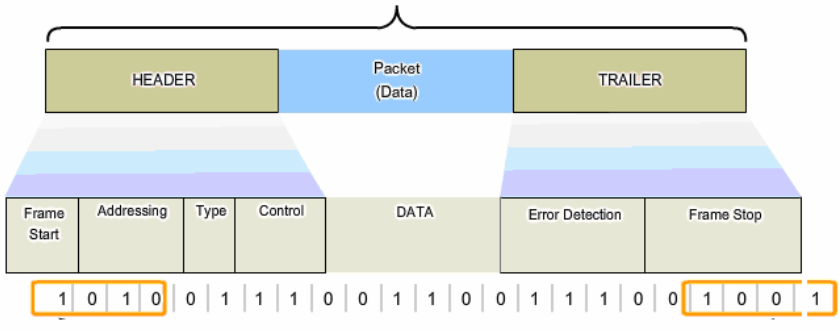


ნახაზი 37. მონაცემთა არხის ფრეიმი

როდესაც მონაცემები მოგზაურობენ გამტარზე, ისინი მოგზაურობენ როგორც ბიტების ნაკადები (1-იანები და 0-იანები).

თუ კი ჰოსტი იღებს ასეთი ბიტების გრძელ ნაკადს, როგორ უნდა განასხვავოს სად იწყება ფრეიმი და სად მთავრდება, ან რომელი ბიტები წარმოადგენენ მისამართს?

Framing ანაწილებს ნაკადებს წაკითხვად ჯგუფებში, საკონტროლო ინფორმაციასთან ერთად რომელიც ისმევა სხვადასხვა ველებში თავსართსა და ბოლოსართიში.



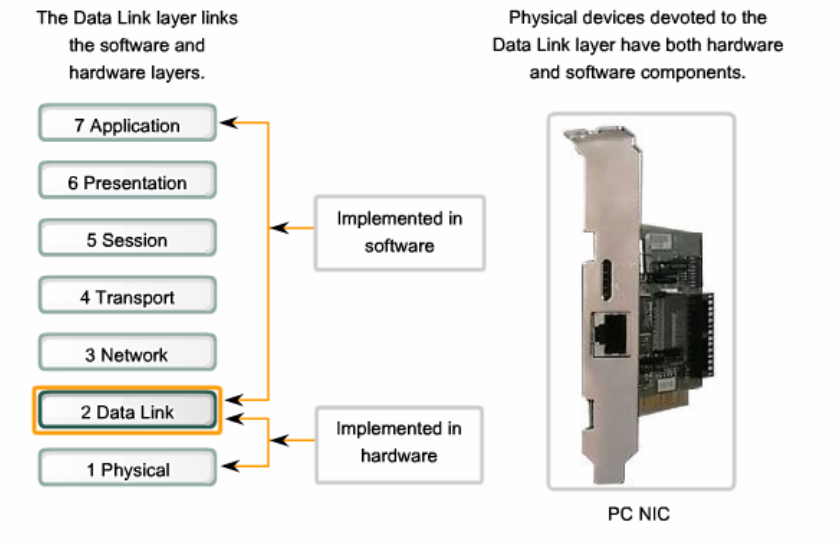
ნახაზი 38. ფრეიმის ველის ტიპები

ტიპიური ველების ტიპები შეიცავენ:

- დასაწყისის და დასასრულის ინდიკატორ ველებს;
- დასახელების და დამისამართების ველებს;
- ტიპის ველს - ანუ რა ტიპის არის პაკეტი, რომელიც არის შეფუთული ჩვენს კადრში;
- კონტროლს - ნაკადების კონტროლის მომსახურეობა;
- მონაცემთა ველს - ანუ თვით ქსელური დონის პაკეტი.

თუმცა ყველა პროტოკოლის ფრეიმი ესე არ გამოიყურება და ისინი შეიძლება განსხვავდებოდნენ.

მონაცემთა არხის დონე არსებობს როგორც მაკავშირებელი დონე პროგრამული პროცესების, რომლებიც მდებარეობენ ზედა დონეებზე და ფიზიკურ დონეს შორის რომელიც მდებარეობს მის ქვეშ. ამის შედეგად იგი ამზადებს ქსელური დონის პაკეტებს გარკვეული ტიპის გამტარზე გადაცემისათვის, იქნება ეს სპილენძი, ბოჭკო თუ ატმოსფერო.



ნახაზი 39. ზედა დონეების სერვისების ფიზიკურ მედიასთან მიერთება

მრავალ შემთხვევაში, მონაცემთა არხის დონე არის წარმოსახული როგორც ფიზიკურ ერთეული მაგ. როგორც Ethernet ქსელური ადაპტერი, რომელიც იდგმება კომპიუტერში და აკავშირებს პროგრამულ უზრუნველყოფას ფიზიკურ გამტართან. ქსელური

ადაპტერი არ არის უბრალოდ ფიზიკური ერთეული. მას გააჩნია თავისი დრაივერი, რომელიც აძლევს მას საშუალებას მოამზადოს მონაცემები გამტარზე გადასაცემად.

მონაცემთა არხის ქვედონეები

იმისთვის რომ მხარდაჭერილი იქნას მრავალი ქსელური ფუნქცია, ხშირად ხდება მონაცემთა არხის დონის დაყოფა ორ ქვედონედ. ზედა და ქვედა ქვედონედ.

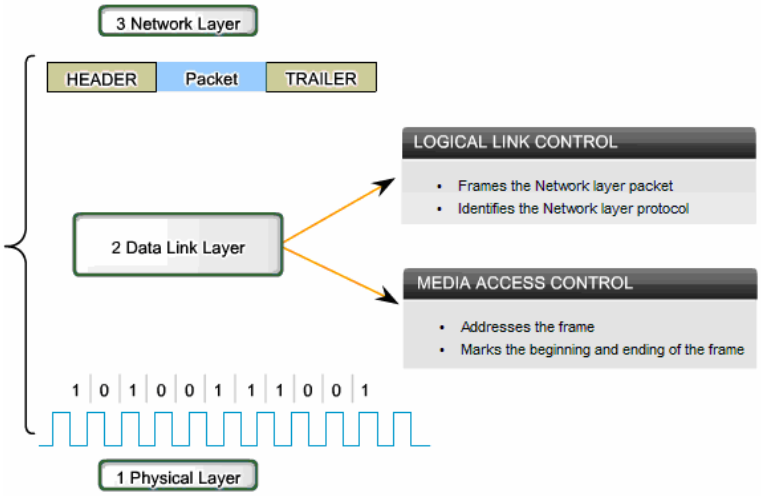
ზედა ქვედონე აღწერს პროგრამულ პროცესს, რომელიც საშუალებას გვაძლევს დაუკავშირდეთ ქსელური დონის პროტოკოლებს.

ქვედა ქვედონე აღწერს გამტარზე წვდომის პროცესს, რომელიც ხორციელდება აპარატურულად.

ორი ყველაზე გავრცელებული ლოკალური ქსელის ქვედონეებია: არხის ლოგიკური მართვა (LLC- Logical Link Control) და გამტარზე წვდომის მართვა (MAC - Media Access Control).

LLC ანთავსებს ინფორმაციას კადრში, სადაც განსაზღვრულია თუ რომელი ქსელური დონის პროტოკოლიდან არის წამოსული ეს ინფორმაცია. ეს გვაძლევს საშუალებას გამოვიყენოთ რამდენიმე ტიპის მესამე დონის პროტოკოლი, როგორიც არის IP და IPX.

MAC უზრუნველყოფს არხის დონის დამისამართებას და მონაცემების დანაწილებას, ფიზიკური გამტარის მოთხოვნისა და არხის დონონის პროტოკოლის ტიპის შესაბამისად.

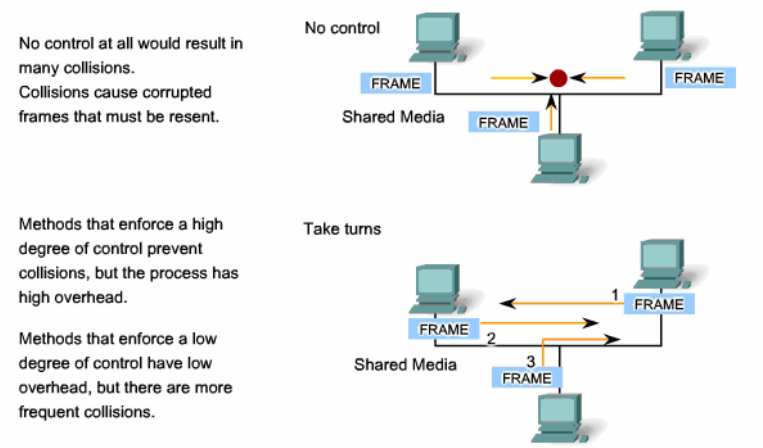


ნახაზი 40. არხის დონის ქვედონეები

კადრების გამტარზე განთავსების რეგულირებას ეწოდება გამტარზე წვდომის კონტროლი. გამტარზე წვდომის მეთოდები მონაცემთა არხის სხვადასხვა პროტოკოლში სხვადასხვაგვარად არის განხორციელებული. ეს ხერხები განსაზღვრავენ თუ როგორ ხდება გამტარის განაწილება კვანძებს შორის.

გამტარზე წვდმოის კონტროლი შეგვიძლია შევადაროთ წესების ერთობლიობას (შუქნიშანს), რომელიც ახორციელებს გზებზე მანქანების დაშვებას. ამ კონტროლის არარსებობის შემთხვევაში მივიღებდით იმას, რომ მანქანები არ დააკვირდებოდნენ შეიძლება თუ არა წარმოიქმნას რაიმე შეფერხება გზაზე შესვლისას, ეს კი იწვევს ავარიებს და საცობებს. თუმცა აღსანიშნავია ის რომ, ყველა გზა, ნიშანი და შესასვლელი არ არის ერთნაირი. მანქანას შეუძლია გზაზე შევიდეს, მას შემდეგ რაც დაუცდის თავის ჯერს გაჩერების ნიშანზე, ან დაელოდება შუქნიშანზე მწვანე შუქს. მძღოლი

მისდევს სხვადასხვა ტიპის წესების ერთობლიობას სხვადასხვა ტიპის შესასვლელისათვის.



ნახაზი 41. გამტარზე წვდომის კონტროლის მეთოდები

ასევე არსებობენ სხვადახვა გზები რათა მოვახდინოთ კადრების გამტარზე განთავსების რეგულირება. ზოგიერთი პროტოკოლი იყენებს მკაცრად კონტროლირებულ მეთოდს გამტარზე კადრების უსაფრთხოდ განსათავსებლად. ეს მეთოდი არის განხოციელებული და ჩამოყალიბებული პროტოკოლებში, თუმცა ამ მექანიზმის მიერ ხდება გარკვეული ზედნადები ინფორმაციის დამატება ქსელში.

გამტარზე წვდომის კონტროლის მეთოდი დამოკიდებულია:

- გამტარის განაწილებაზე - თუ როგორ ინაწილებენ კვანძები გამტარს;
- ტოპოლოგიაზე - როგორ არის კავშირები განხორციელებული კვანძებს შორის მონაცემთა არხის დონეზე.

ზოგიერთ ქსელურ ტოპოლოგიაში ხდება საერთო გამტარის გამოყენება რამდენიმე ჰოსტის მიერ. დროის ნებისმიერ მოცემულ მომენტში შესაძლოა რამდენიმე კვანძს ერთდროულად უნდოდეს ინფორმაციის გაგზავნა და მიღება. შესაბამისად არსებობენ წესები რომელთა დაცვითაც ხდება გადაწყვეტა, თუ როგორ მოხდეს გამტარის განაწილება.

არსებობს განაწილებულ გამტარზე წვდომის კონტროლის მეთოდების ორი ძირითადი ტიპი :

- კონტროლირებული - თითოეულ კვანძს აქვს თავისი დრო გამტარის გამოყენებისათვის;
- შეჯიბრებითობის მეთოდზე დაფუძნებული - ყველა ჰოსტი ეჯიბრება ერთმანეთს გამტარის გამოყენებისათვის.

კონტროლირებული მეთოდი

როდესაც გამოიყენება წვდომის კონტროლირებული მეთოდი, ქსელური მოწყობილობები რიგრიგობით (თანმიმდევრობით) ახდენენ წვდომას გამტარზე. ეს მეთოდი ასევე ცნობილია, როგორც დადგენილი (განსაზღვრული) ანუ დაგეგმილი წვდომის მეთოდი მაგალითად ასეთი წესს იყენებს ტექნოლოგია Token Ring. თუ მოწყობილობას არ სჭირდება გამტარის გამოყენება, ჯერი გადადის შემდგომ მოწყობილობაზე. როდესაც ერთი მოწყობილობა ანთავსებს ფრეიმს გამტრაზე, არცერთ სხვა მოწყობილობას არ შეუძლია გააგზავნოს ინფორმაცია სანამ ის ფრეიმი არ მიაღწევს დანიშნულების ადგილს და არ იქნება დამუშავებული. იმის მიუხედავად, რომ წვდომის კონტროლირებული მეთოდი არის კარგად დალაგებული და გვთავაზობს წინასწარმეტყველებად გამტრაუნარიანობას, ის შეიძლება იყოს არაეფექტური, რადგანაც

მოწყობილობას უწევს მისი ჯერის ლოდინი სანამ შეძლებს გამტარის გამოყენებას.

შეჯიბრებითობის მეთოდი

ამ მეთოდის გამოყენებისას, ნებისმიერ მოწყობილობას ეძლევა უფლება სცადოს წვდომის განხორციელება გამტარზე, როდესაც მას აქვს მონაცემები გასაგზავნად. რათა თავიდან აიცილოს სრული ქაოსი, ეს მეთოდი იყენებს Carrier Sense Multiple Access (CSMA) პროცესს, რათა ჯერ დაადგინოს ხდება თუ არა ქსელში მონაცემების გადაცემა. თუ სიგნალი არის ნაპოვნი ეს ნიშნავს, რომ სხვა მოწყობილობა ახდენს მონაცემების გადაცემას. თუ ინფორმაციის მატარებელი სიგნალი აღმოჩნდა გამტარზე პროცესი ხვდება რომ გამტარი ”დაკავებულია”. სიგნალის აღმოჩენის შემთხვევაში მოწყობილობა იცდის, მოკლე დროის მონაკვეთის გავლის შემდეგ კიდევ ცდის შეღწევას. თუ სიგნალი არ არის ნაპოვნი, მოწყობილობა დაიწყებს მონაცემების გადაცემას. Ethernet და უკაბელო ქსელები იყენებენ შეჯიბრებითობის მეთოდს გამტარზე წვდომის კონტროლისათვის.

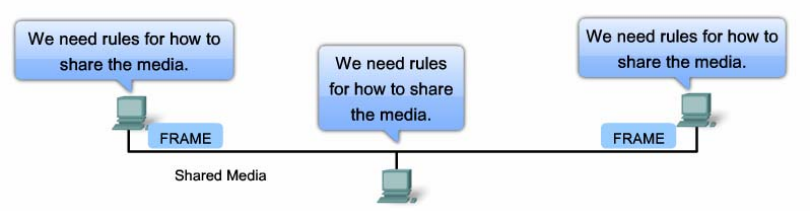
შესაძლებელია ამ პროცესმა განიცადოს მარცხი იმ შემთხვევაში, როდესაც ორი მოწყობილობა დაიწყებს მონაცემების გადაცემას ერთდროულად. ამას ეწოდება მონაცემთა **კოლიზია**.

თუ ეს მოხდება, მონაცემი გაგზავნილი ორივე მოწყობილობის მიერ იქნება დაზიანებული და საჭირო იქნება მისი თავიდან გადაცემა. შეჯიბრებითობის მეთოდზე დაფუძნებულ გამტარზე წვდომის კონტროლის მეთოდს არ აქვს ის ზედმდები, რომელიც მარკერის სახით არის წარმოდგენილი, რაც კონტროლირებულ მეთოდში გვხდება. თუმცა შეჯიბრებითობის მეთოდს უჭირს მუშაობა გამტარზე დიდი დატვირთვისას. კვანძების

რაოდენობასთან ერთად იზრდება მონაცემთა გადაცემის საჭიროების სიხშირეც, ხოლო კლებულობს კოლიზიის გარეშე წვდომის განხორციელების ალბათობა გამტარზე. მექანიზმები, რომლებიც გამოიყენება შეცდომების აღმოსაფხვრელად, კიდევ დამატებით ამცირებენ გამტარუნარიანობას. როგორც წესი CSMA გამოყენება ხდება იმ მეთოდთან ერთად, რომელიც გამოიყენება გამტარზე კამათის აღმოსაფხვრელად.

ორი ხშირად გამოყენებადი მეთოდი არის:

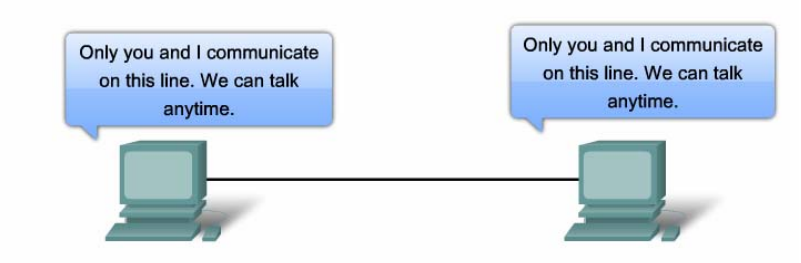
CSMA/Collision Detection (კოლიზიის აღმოჩენა). მოწყობილობა ამოწმებს გამტრს, სიგნალის არსებობის შესახებ. თუ სიგნალი არ არის ინფორმაციიის მატარებელი სიგნალი, მოწყობილობა იწყებს მონაცემების გადაცემას, თუ იქნა შემჩნეული ინფორმაციიის მატარებელი სიგნალი, ის გვაუწყებს რომ სხვა მოწყობილობაც ცდილობდა იგივე დროს მონაცემების გადაცემას, ასეტ შემთხვევაში მოწყობილობა წყვეტს გადაცემას და მოგვიანებით განაახლებს მას.



ნახაზი 42. გამტარზე წვდომის კონტროლი განაწილებული გამტარის დროს

CSMA/Collision Avoidance (კოლიზიის თავიდან აცილება). ამ მეთოდში, მას შემდეგ რაც მოწყობილობა მოისმენს და დაადგენს

რომ გამტრაზე არ ხდება ინფორმაციის გადეცემა, ის გააგზავნის შეტყობინებას იმის შესახებ, რომ აპირებს ინფორმაციის გაგზავნას და ამის შემდეგ დაიწყებს მონაცემების გადაცემას, ანუ წინასწარ აფრთხილებს ქსელში ჩართულ ყველა მოწყობილობას, რომ ის იწყებს გადაცემას, ეს არის სიგნალი რომ სხვებმა თავი შეიკავონ იმ მომენტში ინფორმაციის გადაცემისაგან. ეს მეთოდი როგორც წესი გამოიყენება 802.11 უკაბელო ქსელების ტექნოლოგიებში.



ნახაზი 43. გამტარზე წვდომის კონტროლი არაგანაწილებული გამტარის დროს

გამტარზე წვდომის კონტროლის პროტოკოლები არაგანაწილებული გამტარის დროს ნაკლებ კონტროლს საჭიროებს ან საერთოდ არ საჭიროებს კადრების გამტარზე გადაცემამდე. ამ პროტოკოლებს აქვთ უფრო მარტივი წესები და პროცედურები გამტარზე წვდომის კონტროლისათვის. ასეთი ტოპოლოგიის მაგალითი არის point-to-point. ამ ტოპოლოგიაში გამტარით ურთიერთდაკავშირებულია მხოლოდ ორი ჰოსტი. ამ ტოპოლოგიაში ჰოსტები არ ანაწილებენ გამტარს სხვა ჰოსტებთან და არსჭირდებათ დადგენა თუ ვისდამი არის განკუთვნილი ინფორმაცია. შესაბამისად მონაცემთა არხის დონის პროტოკოლს არაგანაწილებულ გამტარზე წვდომის შემთხვევაში კონტროლისთვის ძალიან ცოტა საქმე აქვს.

სრული და ნახევარ დუპლექსი

point-to-point ტოპოლოგიაში მონაცემთა არხმა უნდა გაითვალისწინოს არის თუ არა კომუნიკაცია სრულ ან ნახევარ დუპლექსური. ნახევარ დუპლექსური კომუნიკაცია ხორციელდება მაშინ, როდესაც მოწყობილობას შეუძლია ინფორმაციის გადაცემაც და მიღებაც, თუმცა არა ერთდროულად. Ethernet აქვს გარკვეული წესების ერთობლიობა რომელიც აღმოფხვრის კონფლიკტებს, რომლებიც წარმოიშვება მაშინ, როდესაც ერთზე მეტი მოწყობილობა ცდილობს გადასცეს ინფორმაცია ერთდროულად.

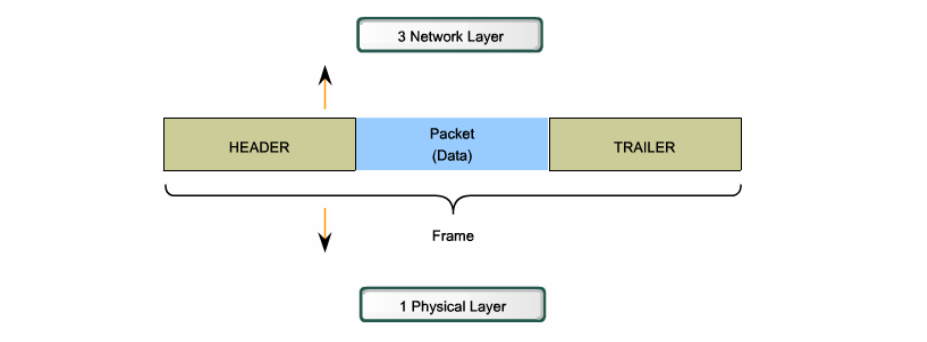
სრული დუპლექსის დროს ორივე მოწყობილობას შეუძლია მოახდინოს მონაცემების გადაცემა და მიღება ერთ გამტარზე ერთდროულად.

მიუხედავად იმისა, რომ არსებობს მრავალი ტიპის ფრეიმი მონაცემთა არხის დონეზე, ყველა მათგანს გააჩნია სამი ძირითადი ველი:

- თავსართი;
- მონაცემები (მაგ. IP პაკეტი);
- ბოლოსართი.

ენკაპსულაციის ყველა მეთოდი ფუთავს OSI მოდელის მესამე დონის მონაცემთა ერთეულს (იქნება ეს IP, IPX თუ სხვა რამ). თუმცა ველები, რომლებსაც შეიცავს თავსართი და ბოლოსართი, განსხვავდება ერთმანეთისაგან. როდესაც ფრეიმი აღწევს თავის დანიშნულების ადგილს, მონაცემთა არხის დონის პროტოკოლი იღებს ფრეიმს გამტარიდან და კითხულობს ინფორმაციას მასში. არ არსებობს ფრეიმის ისთი ფორმატი, რომელიც იმუშავებდა

ყველა ტექნოლოგიასთან. ეს ყველაფერი დამოკიდებულია გარემოზე, რომელშიც უწევს ფრეიმს მოგზაურობა და ლოგიკურ ტოპოლოგიის მოთხოვნებზე.



ნახაზი 44. მონაცემთა არხის დონის სერვისები

ფრეიმის საკონტროლო ინფორმაცია

ფრეიმის საკონტროლო ინფორმაცია დამოკიდებულია პროტოკოლის ტიპზე რომელსაც ვიყენებთ. მას იყენებს მეორე დონის პროტოკოლი რათა მოგვაწოდოს ის საშუალებები რომლებსაც ითხოვს კომუნიკაციის გარემო.

- ტიპიური ფრეიმის თავსართი შეიცავს შემდეგ ველებს: Start Frame Field - ფრეიმის დასაწყისი ველი. გვაუწყებს იმის შესახებ რომ ფრეიმი იწყება;
- Source And Destination Address Fields - წყარო და დანიშნულების ადგილის მისამართების ველი;
- Priority/Quality Of Service Field - პრიორიტეტის და მომსახურეობის ხარისხის ველი;
- Type Field - ტიპის ველი, გვაუწყებს თუ რომელი ზედა დონონის მომსახურეობა გამოიყენება;

- Logical Connection Control Field - ლოგიკური კავშირის კონტროლის ველი, გამოიყენება კვანძებს შორის ლოგიკური კავშირის დასამყარებლად;
- Physical Link Control Field - ფიზიკური კავშირის კონტროლის ველი;
- Flow Control Field - ნაკადის კონტროლის ველი. გამოიყენება ტრეფიკის დასაწყებად და შესაჩერებლად;
- Congestion Control Field - გადატვირთულობის კონტროლის ველი. გვატყობინებს თუ არის ქსელში გადატვირთულობა.

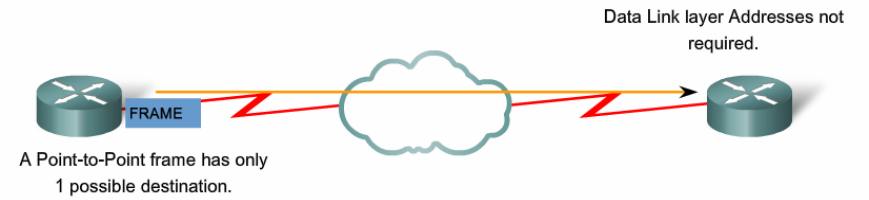
ზემოთ ჩამოთვლილი სია არის მხოლოდ მაგალითები, ხოლო კონტრკრეტული ფრეიმი შეიძლება იყენებდეს სხვადასხვა კომბინაციას.

ნახაზი 45. ფრეიმი

დამისამართება, რომელიც გამოიყენება მეორე დონეზე არის ფიზიკური მისამართები (MAC მისამართები). თავსართი შეიცავს როგორც დანიშნულების ადგილის, ასევე წყაროს მისამართს და ამ მისამართების გამოყენებით ფრეიმს შეუძლია იმოგზაუროს ლოკალურ ქსელში.

მესამე დონონის მისამართებისგან გასხვავებით ეს მისამართები არ არიან იერარქიულები და არ გვაძლევენ ინფორმაციას თუ რომელ ქსელში იმყოფება კომპიუტერი.

კომპიუტერის გადატანით სხვა ქსელში, მათ არ ეცვლებათ მისამართი. შესაბამისად, ამ ფრეიმებს შეუძლიათ იმოგზაურონ მხოლოდ ლოკალურ ქსელში და თუ გახდა საჭირო მათი გადაგზავნა სხვა ქსელში, შუამავალმა მოწყობილობამ (მარშრუტიზატორი) უნდა იკისროს ფრეიმის გადატანის ფუნქცია ერთი ქსელიდან მეორე ქსელში. მარშუტიზატორმა უნდა მოახდინოს ფრეიმის დეკაპსულაცია, წაიკითხოს მესამე დონის მისამართები, გადაწყვიტოს რომელი მიმართულებით გადასცეს ეს პაკეტი და შემდეგ შეფუთოს ის ახალ ფრეიმში, რომლის წყაროს ფიზიკური მისამართი იქნება მარშრუტიზატორის გამომავალი პორტის მისამართი, ხოლო დანიშნულების ადგილის მისამართი იქნება, ან შემდგომი მარშრუტიზატორის ან თვითონ დანიშნულების კვანძის ფიზიკური მისამართი.



ნახაზი 46. ფრეიმის გადაცემა Point-to-point ტოპოლოგიაში

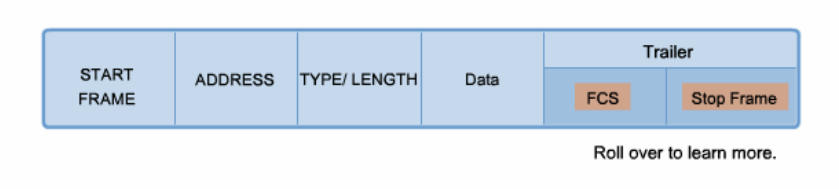
Point-to-point ტოპოლოგიაში არ არის საჭირო მისამართები, რადგანაც ინფორმაციის გაცვლში მონაწილეობს მხოლოდ ორი მხარე. ხოლო წრიულ და მრავალი-წვდომის ტოპოლოგიებში, რადგანაც დაკავშირებულია მრავალი კვანძი საერთო გამტარზე, საჭირო არის დამისამართება. როდესაც ფრეიმი აღწევს დანიშნულების ადგილს (კომპიუტერს), ის შეამოწმებს დანიშნულების ადგილის ველის შიგთავსს და თუ მისამართი დაემთხვევა ამ

ჰოსტის მისამართს, ის დაადგენს რომ ფრეიმი იყო მისთვის განკუთვნილი. წინააღმდეგ შემთხვევაში ფრეიმი იქნება გადაგდებული.

ფრეიმის ბოლოსართი შეიცავს ორ ძირითად ველს:

FCS (Frame Check Sequence) – გამოიყენება შეცდომების შემოწმებისათვის.

იმისთვის რომ არ მოხდეს ქსელში დაზიანებული კადრების გადაცემა ან დავადგინოთ დაზიანებულია თუ არა ფრეიმი მისი მიღებისას, არხის დონე იყენებს გარკვეულ მათემატიკურ ალგორითმებს რათა მიიღოს მოცემული ინფორმაციის წარმოსახვისათვის მოკლე მნიშვნელობა, ხოლო მიღებისას მიმღები იმეორებს იმავე ტიპის პროცესს და ადარებს შედეგებს. თუ შედეგები დაემთხვევა ფრეიმი არ არის დაზიანებული, ხოლო წინააღმდეგ შემთხვევაში მოხდება ფრეიმის გადაგდება.



ნახაზი 47. შეცდომების შემოწმება

Ethernet პროტოკოლი ლოკალური ქსელებისთვის

Ethernet არის ქსელური ტექნოლოგიების ნაკრები, რომელებიც არიან აღწერილნი IEEE 802.2 და 802.3 სტანდარტებში. Ehernet -ის სტანდარტები აღწერენ როგორც მეორე დონის პროტოკოლებს, ასევე პირველი დონის ტექნოლოგიებს. Ethernet არის ყველაზე ფართოდ გავრცელებული ლოკალური ქსელების ტექნოლოგია და

გააჩნია 10, 100, 1000 და 10,000 მეგაბიტ/წამი ინფორმაციის გამტარუნარიანობა. Ethernet -ში ფრეიმის ძირითადი ფორმატი და მისი პირველი და მეორე დონეები რჩება უცვლელი სხვადასხვა ტიპის ეზერნეტებში. მაგრამ იცვლება ფრეიმის გამტარზე განთავსებისა და აღმოჩენის მეთოდები. Ethernet ფრეიმს გააჩნია მრავალი ველი და ფრეიმის სტრუქტურა, რომელიც თითქმის იდენტურია სხვადასხვა სიჩქარის Ethernet -ში. თუმცა ფიზიკურ დონეზე სხვადასხვა ტიპის Ethernet სხვადასხვანაირად ანხორციელებს ამას. Ethernet II არის Ethernet ფრეიმის ფორმატი, რომელიც გამოიყენება TCP/IP ქსელში.

Field name	Preamble	Destination	Source	Type	Data	Frame Check Sequence
Size	8 bytes	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes

ნახაზი 48. Ethernet ფრეიმის ფორმატი

- პრეამბულა გამოიყენება სინქრონიზაციისათვის და ასევე შეიცავს გამყოფს რომელიც გვატყობინებს რომ სინქრო-ნიზაციის ველი ამოიწრა.
- დანიშნულების მისამართი - 48 ბიტიანი მნიშვნელობა (MAC მისამართი).
- წყაროს მისამართი - 48 ბიტიანი მნიშვნელობა (MAC მისამართი).
- ტიპი - გვატყობინებს ზედა დონის მომსახურეობის ტიპს.
- მონაცემები - მესამე დონის პაკეტი.

- ფრეიმის შესამოწმებელი თანმიმდევრობა.

Point-to-Point პროტოკოლი ფართო არის ქსელებში

PPP პროტოკოლი გამოიყნება ორ კვანძს შორის კადრების მიმოცვლისას. ის იქნა შემუშავებული როგორც ფართო არის ქსელის პროტოკოლი და ხშირად გამოიყენება სერიალური კავშირებისას, მაგრამ მისი გამოყენება სხვა ტიპის გამტარებზეც შეგვიძლია, მაგ. როგორიც არის გრეხილი წყვილი, ოპტიკურ-ბოჭკოვანი ხაზები, სატელიტური კავშირები და ასევე ვირტუალური კავშირები. ის იყენებს დონეებად დაყოფილ არქიტექტურას. იმისთვის რომ მრავალი სხვადასხვა ტიპის გამტარებისთვის უზრუნველყოს კავშირი, ის იყენებს ლოგიკურ კავშირებს ორ კვანძს შორის, რომლებსაც ეწოდებათ სესიები. ეს სესია მალავს იმ ფიზიკურ გამტარს ზედა პროტოკოლებისაგან. ასევე ის გვაძლევს საშუალებას მოხდეს რამდენიმე პროტოკოლის ენკაპსილაცია ერთ გამტარზე. თითოეულ პროტოკოლს თავისი სესია გააჩნია. ასევე სესიის შიგნით შეიძლება მოხდეს გარკვეული ტიპის აუტენტიფიკაცია, კომპრესია და Multilink (რამდენიმე ფიზიკური კავშირის გამოყენება).

Field name	Flag	Address	Control	Protocol	Data	FCS
Size (bytes)	1 byte	1 byte	1 byte	2 bytes	variable	2 or 4 bytes

ნახაზი 49. PPP ფრეიმი

- ალამი - ერთი ბაიტი, რომელიც გვაუწყებს ფრეიმის დასაწყის.

- მისამართი - ერთი ბაიტი, რომელიც შეიცავს სტანდარტულ PPP-ს ფართომაუწყებლობის მისამართს. PPP კვანძებს არ ანიჭებს ცალცალკე მისამართებს.

- კონტროლი - ერთი ბაიტი, რომელიც შეიცავს მნიშვნელობას 00000011, რომელიც გვაუწყებს რომ მონაცემები არ მოდის თანმიმდევრობით.

- პროტოკოლი - ორი ბაიტი, რომელიც განსაზღვრავს თუ რომელი პროტოკოლი არის ენკაპსულირებული მონაცემებში.

- მონაცემები - ზედა დონის პაკეტი.

- შეცდომების შემოწმების მნიშვნელობა.

უკაბელო ქსელის პროტოკოლები ლოკალური ქსელებისთვის

802.11 სტანდარტი არის 802 სტანდარტის გაგრძელება. ეს არის უკაბელო ქსელების სტანდარტი. უკაბელო ქსელებში ძალიან დიდ როლს თამაშობს გარემო, რადგანაც ასეთ გარემოში ფიქსირდება მნიშვნელოვანი ხარვეზები. ასევე უკაბელო ქსელებში ძალიან რთულია წვდომის კონტროლი. ამისათვის შეიმუშავეს დამატებითი ველები.

ეს სტანდარტი არის შეჯიბრებითობის მეთოდით მომუშავე სტანდარტი და იყენებს CSMA/CA გამტარზე წვდომის პროცესს, როდესაც მოწყობილობები შემთხვევითი დროით დაიხევენ უკან და დაიცდიან გადაცემის განახლებამდე. ეს ამცირებს კოლიზიების საშიროებას.

ამ სტანდარტში, როდესაც მოხდება ფრეიმის მიღება, შემდგომ აუცილებელია დადასტურების გაგზავნა. ეს გვეხმარება თავიდან ავიცილოთ ის პრობლემები, რომლებიც შეიძლება წარმოიშვას დიდი რაოდენობით ხარვეზებისაგან.

ასევე მას გააჩნია სხვა მომსახურეობების მხარდაჭერა, როგორებიც არის აუტენტიფიკაცია, დაშიფრვა.

- ტიპი და ქვეტიპის ველი - იდენტიფიცირებას უკეთებს სამი ფუნქციიდან ერთერთს : კონტროლი, მონაცემები, მართვა.

- ფრაგმენტირების ველი - თუ მისი მნიშვნელობა არის „1“, ეს ნიშნავს რომ ფრეიმი იქნა დაჭრილი გზაში და მას გააჩნია კიდევ ნაწილი.

- ხელახალი ცდის ველი - თუ მისი მნიშვნელობა არის „1“, ეს ფრემი ხელმეორედ არის გადაცემული

- ძაბვის ეკონომიის ველი - თუ მისი მნიშვნელობა „1“, მაშინ კვანძი არის ეკონომიურად მუშაობის რეჟიმში ჩართული.

- შიფრაციის ველი - თუ მისი მნიშვნელობა არის „1“, ე.ი. გამოიყენება შიფრაციის მეთოდი WEP (ეს მეთოდი არის სუსტი და არასაიმედო).

- Order field – რიგითობის ველი. თუ მისი მნიშვნელობაა „1“, მაშინ კადრებს არ სჭირდებად თანმიმდევრობის შეცვლა. ისინი მკაცრი თანრიგით იგზავნებიან.

- Destination Address (DA) - დანიშნულების ადგილის ფიზიკური მისამართი.

- Source Address (SA) - წყაროს ფიზიკური მისამართი.
- Receiver Address (RA) - მიმღები შუამავალი წვდომის წერტილის (Wireless Device) ფიზიკური MAC მისამართი.
- Transmitter Address (TA) - გადამცემი წვდომის წერტილის (Wireless Device) ფიზიკური MAC მისამართი.
- Fragment Number Field - ფრაგმენტირებული კადრების დალაგებისათვის საჭირო ველი. გვაუწყებს თუ რომელ რიგში უნდა იყოს ფრეიმი.
- Frame Body Field - თვით ინფორმაცია, რომელსაც ვაგზავნით, როგორც წესი არის IP პაკეტი.
- FCS Field - შეცდომების შესამოწმებელი ველი.

ტრანსპორტის დონე

მონაცემთა ქსელი და ინტერნეტი უზრუნველყოფს ადამიანებს შორის სხვადასხვა ტიპის კავშირს , როგორც ადგილობრივად ასევე მსოფლიო მასშტაბით. ერთი მოწყობილობით ადამიანს შეუძლია მრავალი სერვისის გამოყენება, როგორიც არის ელ-ფოსტა, ვები, ჩეთი და სხვა.

მონაცემები ყოველი პროგრამიდან იქცევა პაკეტებად,შემდგომ ტრანსპორტირდება და მიწოდებული იქნება ადრესატის შესაბამის პროგრამაზე ან სერვერულ დემონზე. ეს პროცესი აღწერილია OSI მოდელის ტრანსპორტის დონეზე. პროცესი მოიცავს გამოყენებითი დონიდან მიღებული ინფორმაციის მომზადებას

ქსელურ დონეზე მის გადასაცემად. ტრანსპორტის დონის მობალეობაა, ქსელურ პროცესებს შორის საბოლოო კომუნიკაციის დამყარება

ტრანსპორტის დონის დანიშნულება

ტრანსპორტის დონე გადაცემისას უზრუნველყოფს მონაცემთა სეგმენტაციას და მიღებისას სხვადასხვა კომუნიკაციისას სეგმენტირებული ნაწილების ხელმეორედ ასაწყობის კონტროლს.

სატრანსპორტო დონის ძირითადი პასუხისმგებლობაა:

- გამგზავნ და მიმღებ ჰოსტებს შორის ინდივიდუალური კომუნიკაციისთვის თვალყურის დევნება;
- მონაცემთა სეგმენტაცია და თითოეული პაკეტის მართვა;
- სეგმენტების ხელმეორედ აწყობა;
- განსხვავებული ქსელური პროცესების იდენტიფიცირება.

თითოეული ჰოსტს შესაძლებელია ქონდეს მრავალი პროგრამა, რომლებიც ანხორციელებენ კომუნუკაციას ქსელში. თითოეულ ამ პროგრამას შესაძლებელია ქონდეს ურთიერთობა ადრესატი კომპიუტერის ერთ ან მრავალ პროგრამასთან. სწორედ ტრანსპორტის დონე უზრუნველყოფს მრავალი კავშირის დამყარების შესაძლებლობას.

მონაცემთა სეგმენტაცია

რადგან თითოეული მოთხოვნა ქმნის მონაცემთა ნაკადს რომელიც იგზავნება დაშორებულ ქსელურ პროგრამასთან,აუცილებელია ეს მონაცემები იქნას მომზადებული ქსელში გადასაცემად.

ტრანსპორტის დონის პროტოკოლები აღწერენ იმ სერვისებს, რომლებიც ახდენენ გამოყენებითი დონის მონაცემების სეგმენტაციას. ეს მოიცავს თითოეული მონაცემთა ნაწილის ინკაპსულაციას. ყოველ მონაცემთა ნაწილს სჭირდება თავსართი რომელიც უნდა დაემატოს სატრანსპორტო დონეზე, რათა მითითებული იქნას, გამგზავნის რომელ ქსელურ პროგრამას, მიმღების რომელ ქსელურ პროგრამასთან სჭირდება შეერთება.

სეგმენტების აწყობა და იდენტიფიცირება

მიმღებ ჰოსტზე, მიღებული ინფორმაციული ნაწილები უნდა იქნას იდენტიფიცირებული. დამატებით ასევე საჭიროა იდენტიფიცირებული მონაცემთა ნაწილები აწყობილი იქნას მონაცემთა ნაკადის სახით და მიმართული იქნას გამოყენებით დონეზე მოქმედ შესაბამის პროგრამებზე. TCP/IP პროტოკოლი ამ იდენტიფიკატორს ეძახის პორტის ნომერს.ყოველ პროგრამულ პროცესს რომელსაც სჭირდება ქსელური კომუნიკაცია, საჭიროებს უნიკალურ პორტის მისამართს. პორტის მისამართი სჭირდება ტრანსპორტის დონეს, რათა განხორციელდეს პროგრამული პროცესების ,ანუ მათ მიერ წარმოქმნილი მონაცემთა ნაკადების იდენტიფიცირება.

ტრანსპორტის დონე - ეს არის კავშირი გამოყენებით და მასზე დაბალ დონეებთან, რომლებიც პასუხისმგებელნი არიან მონაცემთა გადაცემაზე. ეს დონე იღებს მონაცემებს სხვადასხვა პროგრამებიდან და გადასცემს ქვედა დონეს, როგორც მართვად ნაწილებს , რომლებიც ქვდა დონის პროტოკოლების საშუალებით, შესაძლებელია იქნას მარშუტიზირებული, მულტიპლექსირე-ბული და გადაცებული მედიაზე

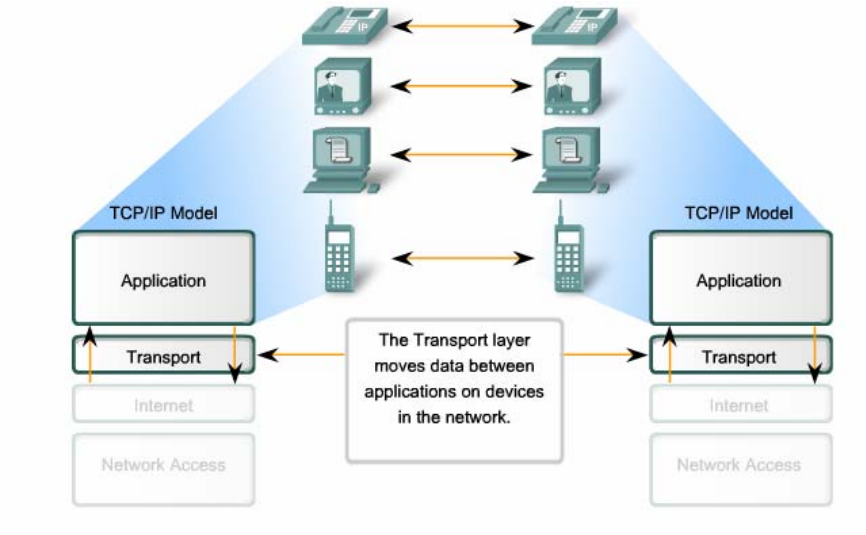
გამოყენებითი დონის პროგრამები აგენერირებენ მონაცემებს, რომელიც უნდა გაიგზავნოს ერთი პროგრამიდან მეორეში. ეს გადაცემა შესაძლებელია განხორციელდეს ისე რომ, არ არის საჭირო ვიცოდეთ: რა ტიპის არის მიმღები ჰოსტი, რა ტიპის მედიას გაივლის მონაცემი, რა გზას გაივლის, ან რა ტიპის ქსელს გაივლის.

ქვედა დონეების პასუხისმგებლობაა გადასცენ მონაცემი შესაბამის მოწყობილობას. ტრანსპორტის დონე კი-ახარისხებს მონაცემთა ნაწილებს და გადასაცემს მათ შესაფერის პროგრამებს .

მოთხოვნები მონაცემებზე განსხვავებულია, რადგანაც სხვადასხვა მონაცემებს გააჩნიათ სხვადასხვა მოთხოვნები, ამიტომ არსებობს ტრანსპორტის დონის მრავალი პროტოკოლი. ზოგ შემთხვევაში საჭიროა, რომ სეგმენტებმა მიაღწიონ დანიშნულების ადგილას გარკვეული თანმიმდევრობით, რათა მათი დამუშავება მოხდეს წარმატებით; სხვა შემთხვევაში შესაძლებელია იმის დაშვება რომ ზოიერთი მონაცემი შესაძლებელია დაიკარგოს ქსელში გადაცემისას.

თანამედროვე ქსელებში, სხვადსხვა პროგრამას სჭირდება სხვადასხვა ტრანსპორტის დონის პროტოკოლი. განსხვავებული ტრანსპორტის დონის პროტოკოლს აქვს განსხვავებული წესები.

ზოგიერთი პროტოკოლები უზრუნველყოფენ მხოლოდ ძირითად ფუნქციებს იმისათვის, რომ მათ ეფექტურად გადასცენ მონაცემები შესაბამის პროგრამებს შორის. ამ ტიპის პროტოკოლები გამოიყენება ისეთი მოთხოვნებისათვის რომლებიც მგრძნობიარეა (შეყოვნების) დაბრკოლების მომართ.



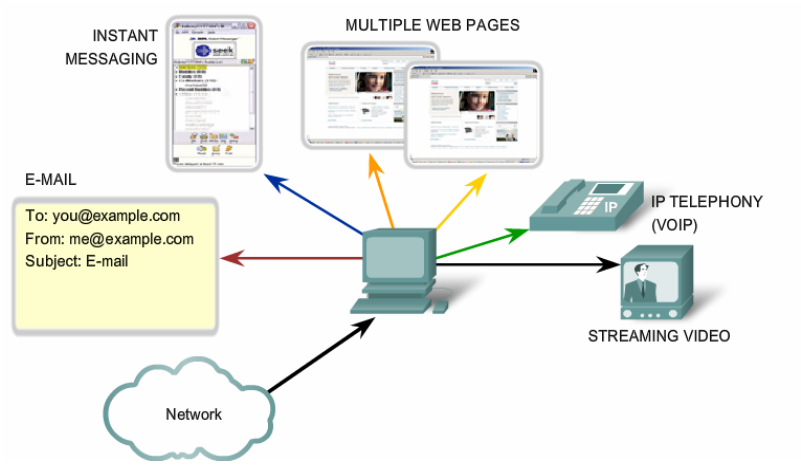
ნახაზი 50. ტრანსპორტის დონესა და ზედა დონეს შორის ურთიერთკავშირი

ზოგი (დანარჩენი) ტრანსპორტის დონის პროტოკოლები აღწერენ პროცესებს რომლებიც უზრუნველყოფენ დამატებით ფუნქციებს, როგორიცაა მონაცემთა გადაცემის საიმედოობა. იმ დროს როცა ეს დამატებითი ფუნქციები უზრუნველყოფენ გაცილებით საღ კომუნიკაციას ტრანსპორტის დონეზე, მათ გააჩნიათ დამატებითი მმართველი ინფორმაცია, რაც ზრდის ქსელური ტრაფიკის მოთხოვნას.

მრავალი კომუნიკაციის შექმნა

თუ კომპიუტერი ჩართულია ქსელში, მას შეუძლია ერთდროულად მიიღოს და გადასცეს ელ-ფოსტა, დაათვალიეროს საიტები, და ისარგებლოს VoIP ტელეფონით. თითოეული ეს

პროგრამა გადასცემს და იღებს მონაცემებს ქსელში ერთი და იგივე დროს.



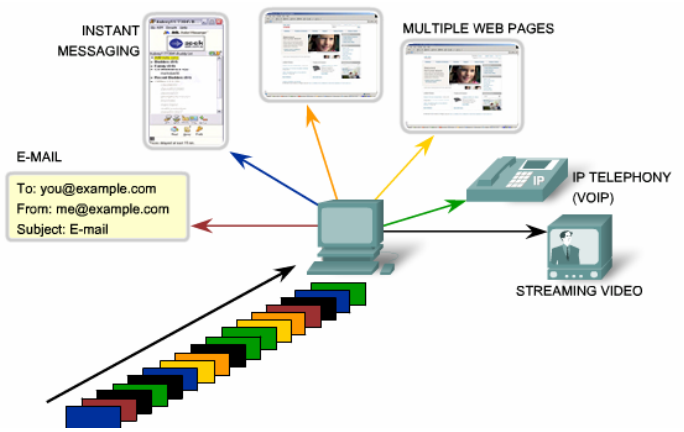
ნახაზი 51. რამოდენიმე კომუნიკაციის დამყარება

ზოგი (დანარჩენი) ტრანსპორტის დონის პროტოკოლები აღწერენ პროცესებს რომლებიც უზრუნველყოფენ დამატებით ფუნქციებს, როგორიცაა მონაცემთა გადაცემის საიმედოობა. იმ დროს როცა ეს დამატებითი ფუნქციები უზრუნველყოფენ გაცილებით საღ კომუნიკაციას ტრანსპორტის დონეზე, მათ გააჩნიათ დამატებითი მმართველი ინფორმაცია, რაც ზრდის ქსელური ტრაფიკის მოთხოვნას.

ზოგი (დანარჩენი) ტრანსპორტის დონის პროტოკოლები აღწერენ პროცესებს რომლებიც უზრუნველყოფენ დამატებით ფუნქციებს, როგორიცაა მონაცემთა გადაცემის საიმედოობა. იმ დროს როცა ეს დამატებითი ფუნქციები უზრუნველყოფენ გაცილებით საღ კომუნიკაციას ტრანსპორტის დონეზე, მათ გააჩნიათ დამატებითი

მმართველი ინფორმაცია, რაც ზრდის ქსელური ტრაფიკის მოთხოვნას.

მომხმარებლები ითხოვენ რომ ელექტრონული ფოსტა და ინფორმაციის დაყოფა მცირე ნაწილებად და მათი გადაცემა გამგზავნი ჰოსიდან ადრესატამდე საშუალებას აძლევს იარსებოს ბევრმა განსხვავებულმა კომუნიკაციამ ერთი და იმავე ქსელში



ნახაზი 52. სეგმენტაცია

ტრანსპორტის დონის თანახმად, მონაცდემების სეგმენტაცია უზრუნველყოფს მრავალი პროგრამის მიერ, როგორც მონაცემთა გაგზავნის ასევე მიღების საშუალებებს ერთდაიგივე კომპიუტე-რიდან. სეგმენტაციის გარეშე მხოლოდ ერთ პროგრამას შეუძლია ინფორმაციის გადაცემა ან მიღება (მაგ. ვიდეო ინფორმაცია), მაგრამ ამ დროის განმავლობაში ვერ მიიღებდით წერილებს, ვერ მოიხმარდით ჩატს, ვერ დაათვალიერებდით საიტებს და სხვა, სანამ არ დაამთვრებდით ვიდეო ინფორმაციის მიღებას.

ტრანსპორტის დონეზე გამგზავნიდან ადრესატამდე გადაცემული თითოეული ინფორმაციის ნაწილი ცნობილია როგორც ”ლაპარაკი - conversation ”.

რათა იდენტიფიცირებულ იქნას მონაცემის თითოეული სეგმენტი, ტრანსპორტის დონე მონაცემის ნაწილს ამატებს თავსართს რომელიც შეიცავს ორობით მონაცემს. ეს თავსართი შეიცავს ბიტების ველს. ეს არის მნიშვნელობები, რომელიც საშუალებას აძლევს ტრანსპორტის დონის სხვადასხვა პროტოკოლებს შეასრულონ სხვადასხვა ფუნქცია.

ურთიერთობის (Conversation) კონტროლი

ყველა ტრანსტორტის დონის პროტოკოლების პირველადი ფუნქციებია:

მონაცემთა სეგმენტაცია და შემდგომ აწყობა - ქსელების უმეტესობას გააჩნია შეზღუდვა მონაცემთა რაოდენობაზე, რომელსაც შეიძლება შეიცავდეს ერთი მონაცემთა პაკეტის ერთეული PDU. ტრანსპორტის დონე გამოყენებით მონაცემებს ყოფს ცალკეულ სათანადო ზომის მონაცემებად. საბოლოოდ ტრანსპორტის დონე კრებს მონაცემებს ხელმეორედ და აგზავნის შესაბამის პროგრამაზე ან სერვისზე.

ის ინფორმაცა რომელსაც შეიცავს თავსართი გამოიყენება სეგმე-ნტაციისა და მისი ხელახლა აწყობისთვის, სატრანსპრტო დონის ზოგიერთი პროტოკოლი უზრუნველყოფს:

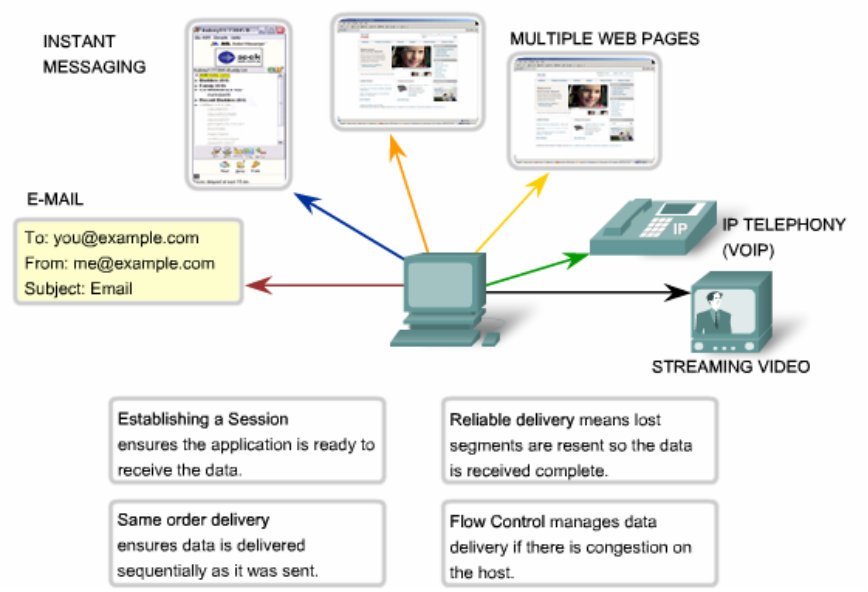
- კავშირზე ორიენტირებული ურთიერთობას
- საიმედო მიწოდებას
- მონაცეების დაშლას და აწყობას

- ნაკადის მართვას

სესიის დმყარება

ტრანსპორტის დონეს სესიების შექმნით შეუძლია განახორციელოს კავშირზე ორიენტირებული ურთიერთობა. კვშირს ამზადებს გამოყენებითი პროგრამები მანამ, სანამ მონაცემები იქნება გაგზავნილი. ამ სეანსით კომუნუკაცია ხდება მართული

ტრანსპორტის დონეზე არსებობს ორი ყველაზე გამოყენებადი პროტოკოლი Transmission Control Protocol (TCP) და User Datagram Protocol (UDP). ორივე ეს პროტოკოლი მართავს მრავალი ქსელური პროგრამის კომუნიკაციას. განსხვავება ამ ორ პროტოკოლს შორის არის სპეციფიური ფუნქციები, რომელიც დამახასიათებელია ორივე პროტოკოლისთვის.



ნახაზი 53. ტრანსპორტის დონის სერვისები

პორტების დამისამართება

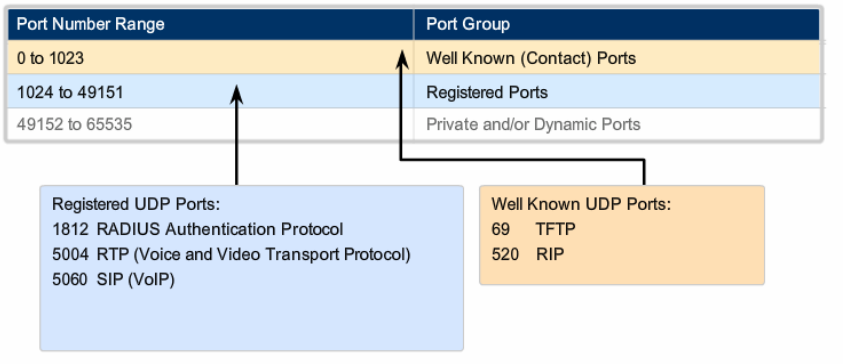
IANA (Internet Assigned Numbers Authority) - ეს არის სტანდარტიზაციის ორგანიზაცია, რომელიც პასუხისმგებელია სხვადასხვა დამისამართების სტანდარტების განსაზღვრაზე. ის ანიჭებს პროცესებს პორტის ნომრებს.

არსებობს სხვადასხვა ტიპის პორტის ნომრები:

Port Number Range	Port Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

ნახაზი 54. პორტის ნომრები

საყოველთაოდ ცნობილი პორტები (ნომრებით 0 - 1023) - ეს ნომრები რეზერვირებულია მომსახურებისა და გამოყენებისა-თვის. ისინი, როგორც წესი გამოიყენება ისეთი მოთხოვნებისთვის, როგორიცაა HTTP (ვებ სერვერი), POP3/SMTP (საფოსტო სერვერი) და Telnet (ტელნეტი).ცნობილი პორტები მინიჭებული აქვს სერვერულ პროგრამებს. კლიენტ პროგრამეები კი, შეიძლება ისე იყოს დაპროგრამებული, რომ ავტომატურად მოითხოვოს კავშირი სპეციალურ პორტთან და მასთან დაკავშირებულ მომსახურე-ბასთან.



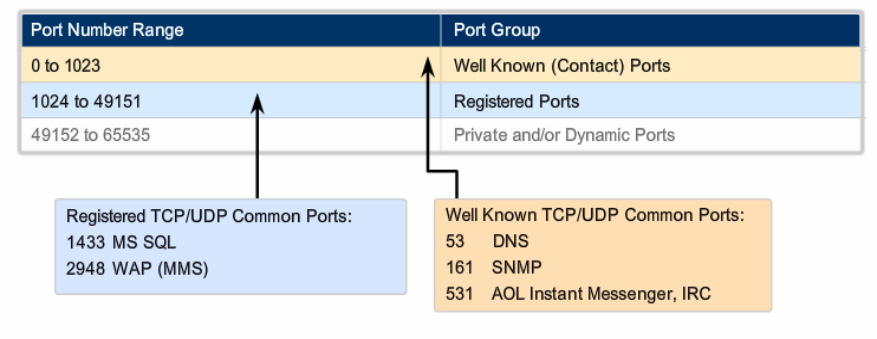
ნახაზი 55. პორტის ნომრები

რერეგისტრირებადი პორტები (1024-49151) - ეს პორტის ნომრები ენიჭებათ მომხმარებელთა პროცესებს ან პროგრამებს. ეს პროცესები უპირველეს ყოვლისა არის ცალკეული პროგრამები, რომლებსაც ირჩევს მომხმარებელი და აინსტალირებს საყოველთაო გამოყენებისთვის(მაგალითად MySQL-იყენებს პორტს 3306). ამ პროგრამებს ან პროცესებს შეუძლიათ გახდნენ საყოველთაოდ ცნობილი პორტების მისამართები. თუ ეს პორტები არ გამოიყენება მსგავსი პროგრამებისთვის, ის შეიძლება გამოყენებულ იქნას დინამიურად კლიენტების მიერ როგორც მათი წყარო პორტი.

დინამიური ანუ პირადული პორტები (49152-65535) - ცნობილია როგორც მოჩვენებითი (Ephemeral Ports) პორტები. ისინი როგორც წესი დინამიურად ენიჭებათ კლიენტ პროგრამებს როდესაც ისინი იწყებენ კავშირის განხორციელებას.

TCP და UDP ერთობლივად გამოყენება

ზოგიერთი მოთხოვნა იყენებს როგორც TCP ასევე UDP. მაგალითად, UDP მცირე მმართველი ინფორმაცია საშუალებას აძლევს DNS სერვერს მოემსახუროს ბევრი მომხმარებელის მოთხოვნას სწრაფად. ხანდახან, ინფორმაციის გაგზავნისას შესაძლებელია მოთხოვნილ იქნას TCP-ით საიმედო კავშირი. ორივე პროტოკოლის შემთხვევაში გამოიყენება ცნობილი პორტი - 53.

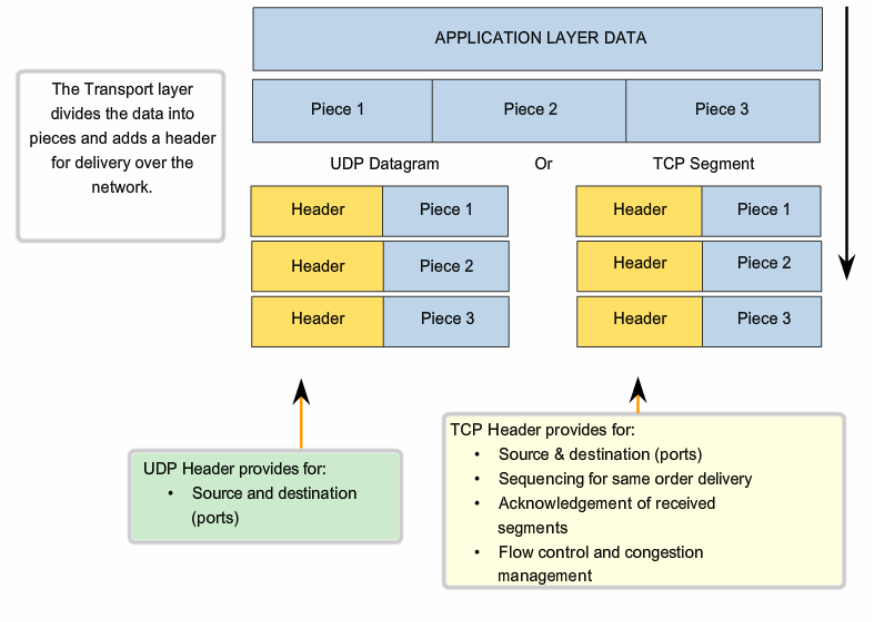


ნახაზი 56. პორტის ნომრები

ზოგიერთი პროგრამა გადასცემს დიდი რაოდენობის მონაცემებს - რამდენიმე გიგაბიტს. არაპრაქტიკული იქნებოდა რომ ეს მოთხოვნა გადაცემულიყო როგორც ერთი დიდი ნაწილი. თუ მსგავსი რამ განხორციელდება შეუძლებელი გახდება სხვა ქსელური ტრაფიკის გადაცემა. დიდი ზომის მონაცემის გადაიცემას შესაძლებელია დასჭირდეს რამდენიმე წუთის ან საათი. ამასთან თუ მოხდება რაიმე შეცდომა გადაცემისას, დაიკარგება მთლიანი მონაცემი და მის გადაცემა გახდება საჭიროა თავიდან. აგრეთვე ქსელურ მოწყობილობებს არ

გააჩნიათ მსგავსი ზომის მეხსიერების ბუფერები, რომ მათ მიიღონ ან გადასცენ ასეთი ზომის ინფორმაცია. მონაცემების დაყოფა ნაწილებად საშუალებას იძლევა სხვადასხვა მონაცემი იქნას გადაცემული ერთ მედიაში მონაცვლეობით.

ინფორმაცია ადრესატამდე შეიძლება მივიდეს განსხვავებული თანმიმდევრობით ვიდრე ის იქნა გაგზავნილი, რადგანაც სხვადასხვა პაკეტი ირჩევს სხვადასხვა გზას ქსელში. მოთხოვნა რომელიც იყენებს UDP-ს უნდა დაუშვას ის ფაქტი, რომ მონაცემი რომელიც გაიგზავნა შიძლება არ იქნეს მიღწეული დანიშნულების ადგილას.



ნახაზი 57. ტრანსპორტის დონის ფუნქციები

ძირითადი განსხვავება TCP და UDP შორის ეს არის საიმედოობა. TCP კავშირის საიმედოობა უზრუნველყოფილია კავშირზე ორიენტირებული სესიის გამოყენებით. მანამ, სანამ გამგზავნი, რომელიც იყენებს TCP გააგზავნის მონაცემებს ადრესატთან, ტრანსპორტის დონე იწყებს პროცესს რათა დაამყაროს კავშირი ადრესატთან. ეს პროცესი უზრუნველყოფს, რომ თითოეული ჰოსტმა იცის და მზადაა კომუნიკაციისათვის.

მას შემდეგ რაც დამყარდება სესია, ადრესატი უგზავნის გადამცემს დადასტურებას, რომ მზადაა სეგმენტების მისაღებად. ეს დასტური უზრუნველყოფს საიმედოობის საფუძველს TCP სესიაში. რადგან გამგზავნი იღებს დასტურს, მან იცის, რომ მონაცემები წარმატებით გადაიცემა. თუ იგი არ მიიღებს დასტურს, მაშინ გარკვეული დროის შემდეგ ხელმეორედ აგზავნის იგივე მონაცემებს.

UDP პროტოკოლი

UDP არის მარტივი პროტოკოლი, რომელიც არ არის კავშირზე ორიენტირებული და ვერ უზრუნველყოფს ამ დონეზე სეგმენტების საიმედო გადაცემას. მას გააჩნია მცირე მმართველი ინფორმაცია, რაც საშუალებას იძლევა ნაკელბი ტრაფიკის გამოყენებით გადაცემული იქნას უფრო მეტი ინფორმაცია ვიდრე TCP შემთხვევაში. UDP პროტოკოლი გამოიყურება შემდეგნაირად

ნახაზი 5მ. UDP პროტოკოლი

UDP პროტოკოლს იყენებს შემდეგი პროგრამები:

- Domain Name System (DNS)
- Video Streaming
- Voice over IP (VoIP)

UDP პროტოკოლი გამოიყენება ისეთი კომინიკაციის დროს, რომელიც უშვებს ინფორმაციის დანაკარგს, მაგ. პირდაპირ ეთერში გადაცემული ინტერნეტ ტელევიზია, ამ შემთხვევაში ინფორმაციის დაკარგვამ შეიძლება გამოიწვიოს კადრის შენელება ან მცირე დროით ხმის დაკარგვა, რაც არ არის კატასტროფული. ამ დროს წარმოუდგენელია დაკარგული ინფორმაციის აღდგენა, რადგანაც გადამცემი პერიოდულად აგზავნის ახალ ინფორმაციულ ნაკადს. ინფორმაციის აღდგენა კი შესაძლებელია მხოლოდ ისეთი გადაცემისას, რომელიც არის ფაილის სახით შენახული და რომლის ხელეხალი გაგზავანაც აბსოლუტტურად შესაძლებელია.

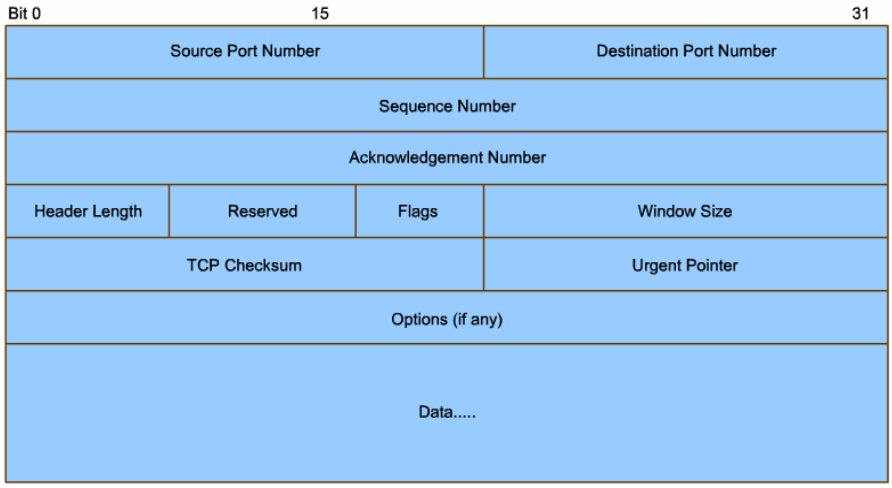
TCP პროტოკოლი

TCP ინტერნეტ პროტოკოლის იერარქიაში ერთერთი უმთავრესი და უმნიშვნელოვანესი პროტოკოლია, რომელსაც იყენებს მრავალი სხვადასხვა პროტოკოლი კავშირის დასამყარებლად და ინფორმაციის საიმედოდ გადასაცემად.

მონაცემის სეგმენტებად დაყოფის შემდეგ TCP პროტოკოლი თითოეულ სეგმენტს ამატებს ინფორმაციას:

- გამგზავნისა და მიმღების პორტის ნომრები

- მიმდევრობის რიცხვი
- დამადასტურებელი რიცხვი
- შემაჯამებელი რიცხვი
- ფანჯრის ზომა
- თავსართის სიგრძე
- კოდი



ნახაზი 59. TCP პროტოკოლის სეგმენტი

როგორც ზემოთ ავღნიშნეთ, TCP პროტოკოლი ცნობილია როგორც კავშირზე ორიენტირებული პროტოკოლი. დასაწყისში გამგზავნი მოწყობილობა გზავნის TCP სინქრონიზაციის შეტყობინებას და ელოდება TCP დამადასტურებელ შეტყობინებას, რის მიღების შემთხვევაში ისევ გზავნის უკვე კავშირის დამყარების დამადასტურებელ შეტყობინებას და სწორედ ამის შემდეგ ითვლება ორ მოწყობილობას შორის TCP კავშირი დამყარებულად.

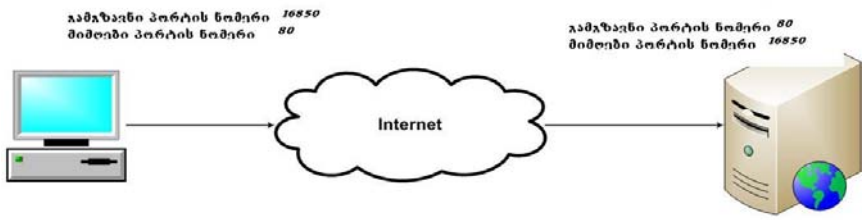
თუ ყველაფერმა ზემოთ ჩამოთვლილმა წარმატებით ჩაიარა, მოწყობილობები იწყებენ ინფორმაციის გაცვლას. ინფორმაციის სეგმენტებად დაყოფისას საჭიროა სეგმენტების დანომვრა, რადგანაც მიმღებმა მოწყობილობამ ინფორმაცია უნდა ააგოს, რათა ის გახდეს წაკითხვადი მომხმარებლის მიერ. ამისათვის TCP სეგმენტის თავსართში, მიმდევრობის რიცხვის ველში იწერება ნომერი რომელიც შეესაბამება გაგზავნილი სეგმენტის რიგითობას.

TCP თავსართი შეიცავს პორტის ნომრის ველებს. ამ ველების დანიშნულების ასაღწერად მოვიყვანოთ მარტივი მაგალითი, როდესაც კლიენტის კომპიუტერი გზავნის მოთხოვნას ვებ-სერვერთან: თავდაპირველად, კომპიუტერი გამგზავნი პორტის ველში წერს შემთხვევით შერჩეულ ნომერს 1024-დან 65535-მდე. (1-1023 ცნობილი პორტები), ხოლო მიმღები პორტის ველში ამ შემთხვევაში 80–ს, რადგანაც HTTP პროტოკოლი სწორედ ამ პორტს იყენებს. მიმღები სერვერი ამუშავებს მიღებულ ინფორმაციას და პორტის ნომრის მიხედვით ადგენს რომ ინფორმაცია ეკუთვნის სერვერზე გაშვებულ http სერვისს. პასუხის დაბრუნებისას სერვერი ადგილებს უცვლის პორტის ნომრებს, რათა მიმღებმა მოწყობილობამ განასხვავოვოს მიღებული სხვადასხვა პასუხები ერთმანეთისაგან.

TCP პროტოკოლში მონაცემთა ნაკადის კონტროლი

TCP პროტოკოლის ერთერთი მნიშვნელოვანი ფუნქციაა მონაცემთა ნაკადების კონტროლი. მონაცემთა ნაკადების კონტროლი კი თავის მხრივ არის მეთოდი, რომლითაც მოწყობილობები ერთმანეთს ატყობინებენ თავიანთი სტატუსის შესახებ(შეუძლიათ თუ არა მოცემულ მომენტში მიიღონ ინფორმაცია და რა რაოდენობის).

ზოგჯერ ინფორმაციის გაცვლა ხდება ორი არათანაბარი შესაძლებლობის მქონე მოწყობილობას შორის, ამიტომ შესაძლებელია ერთერთ მათგანს დროის მოცემულ შუალედში უფრო დიდი მოცულობის ინფორმაციის გაგზავნა ან მიღება, შეეძლოს ვიდრე მეორეს, ან პირიქით. ეს პრობლემა სწორედ მონაცემთა ნაკადების კონტროლით იჭრება, რაც იმას ნიშნავს, რომ მოწყობილობები თანხმდებიან ერთმანეთში ინფორმაციის მოცულობაზე დროის მოცემულ შუალედში და ამყარებენ ზომას (Window size), რომელიც წარმოადგენს სეგმენტების რაოდენობას, რომელთა გაგზავნის შემდეგ მიმღები მოწყობილობა გამოაგზავნის დასტურს.

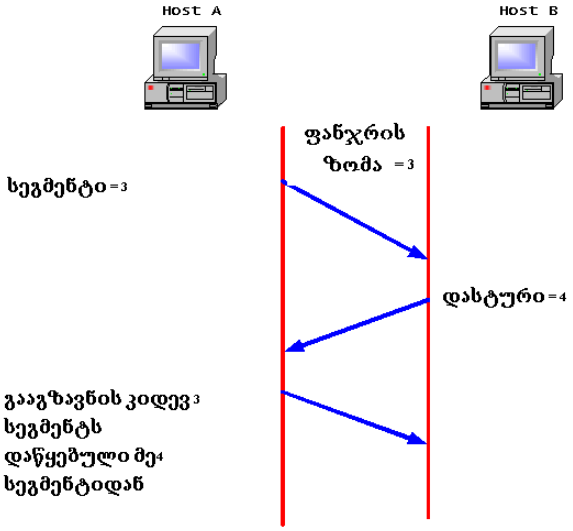


ნახაზი 60. ინფორმაციის გაცვლა

ისეთ მოწყობილობებს, როგორიცაა ქსელის ადაპტერი, გააჩნიათ ბუფერული მეხსიერება, სადაც მიღებულ ინფორმაციას ათავსებს რაღაც გარკვეული დროის განმავლობაში, სანამ მოახერხებს გადამუშავებას და მომხმარებლისთვის საჭირო დონეზე წარმოდგენას. თუ "ფანჯრის ზომა" 1-ის ტოლია, ეს იმას ნიშნავს, რომ ყოველი გაგზავნილი სეგმენტის შემდეგ მიმღებმა მოწყობილობამ დასტური უნდა გამოუგზავნოს მგზავნელს, მაგრამ ამგვარი კომუნიკაცია დაახლოებით ქსელის გამტარუნარიანობის 50% მოიხმარს, ამის გამო მოწყობილობები თანხმდებიან ისეთ ზომაზე,

რომლის რაოდენობის სეგმენტების გადამუშავებას შეძლებს დროის გარკვეულ მონაკვეთში. ამ ზომის სიდიდე შესაძლებელია დინამიურად შეიცვალოს, რაც დამოკიდებულია მოწყობილობის დატვირთვაზე.

სურათზე ჩანს, რომ კომპიუტერი A უგზავნის კომპიუტერ B-ს რაღაც ინფორმაციას.



ნახაზი 61. კომპიუტერი A უგზავნის კომპიუტერ B-ს ინფორმაციას

როგორც ზემოთ აღვნიშნეთ, კომპიუტერი A დაყოფს ამ ინფორმაციას სეგმენტებად, რის შემდეგაც მოწყობილობები შეთანხმდებიან ფანჯრის ზომაზე. მაგალითზე ფანჯრის ზომა არის 3 ერთეული. მას შემდეგ რაც კომპიუტერი A გზავნის 3 სეგმენტს, ის ელოდება კომპიუტერ B-სგან დასტურს

(acknowledgement =Seq+1), რის მიღების შემთხვევაშიც გააგზავნის მომდევნო 3 სეგმენტს.

მონაცემთა ნაკადების კონტროლი ხელს უწყობს ქსელში ინფორმაციის მაქსიმალურად ეფექტურად გაგზავნას, მოწყობილობების ბუფერული მეხსიერებების გადავსების და ამით ინფორმაციის დაკარგვის თავიდან აცილებას და ამასთანავე გამტარუნარიანობის ხელსაყრელად გამოყენებას.

TCP პროტოკოლის საიმედოობა

TCP პროტოკოლი, როგორც ზემოთ აღვნიშნეთ, კავშირზე ორიენტირებული პროტოკოლია, რაც იმას ნიშნავს, რომ ის ინფორმაციის გაგზავნამდე ამყარებს საბოლოო მოწყობილობებს შორის კავშირს. ზოგჯერ ინფორმაციის გაგზავნისას გაუთვალისწინებელი მიზეზების გამო ხდება სეგმენტების დაკარგვა, რაც საბოლოოდ მონაცემების დამახინჯებას იწვევს. ეს სიტუაცია წინასწარ განსაზღვრულია TCP პროტოკოლის ფუნქციონირებისას. გამგზავნი მოწყობილობა სეგმენტების გარკვეული რაოდენობის გაგზავნის შემდეგ (window size) ელოდება დასტურს (acknowledgement) განსაზღვრული დროის განმავლობაში, რომლის მიღების შემდეგ თვლის, რომ მონაცემი გაგზავნილია წარმატებით. თუ დასტური ამ დროის შუალედში არ მოუვიდა, ამ შემთხვევაში ხდება დაკარგული სეგმენტების (გაგზავნილი სეგმენტები, რომლებზედაც არ მოვიდა დასტური) თავიდან გაგზავნა. ინფორმაციის ხელახლა გაგზავნა მეორდება16 ჯერ, თუ ვერ მიიღო დასტური.

Ethernet ტექნოლოგია

Ethernet – არის დღევანდელ დღეს ყველაზე გავრცელებული ლოკალური ქსელის სტანდარტი. ამ სტანდარტით აგებულია ათეულობით მილიონი ლოკალური ქსელი. მსოფლიოში პრიველი ლოკალური ქსელი იყო **Ethernet**-ის ორიგინალური ვერსია.

ისტორია

30-ზე მეტი წლის წინ რობერტ მეტკალფმა და მისმა კოლეგებმა **Ethernet** ქსელი ფირმა "ქსეროქსში" დააპროექტეს. პირველი Ethernet ტექნოლოგიის სტანდარტი იქნა გამოქვეყნებული 1980 წელს კონსორციუმის მიერ, რომელიც შედგებოდა Intel-ისაგან, Xerox-ისაგან და Digital Equipment Corporation-ისგან (DIX). მეტკალფს უნდოდა რომ Ethernet ყოფილიყო განაწილებული სტანდარტი, ამიტომ ის იქნა გამოშვებული როგორც ღია სტანდარტი. პირველი პროდუქტები რომლებიც შეიქმნა Ethernet სტანდარტიდან გაყიდვაში გამოჩნდა XX საუკუნის 80-იან წლებში. 1985 წელს, ელექტრონიკისა და ელექტროობის ინსტიტუტის (IEEE) სტანდარტების კომიტეტმა გამოაქვეყნა ლოკალური და ქალაქის ზომის ქსელების სტანდარტები, ციფრებით 802.

Ethernet-ის სტანდარტია 802.3. ინსტიტუტს უნდოდა, რომ მათი სტანდარტი შეთავსებულიყო საერთაშორისო სტანდარტების ორგანიზაციასთან (ISO) და OSI მოდელთან. იმისათვის, რომ ეს მომხდარიყო IEEE802.3 სტანდარტებს უნდა დაეკმაყოფილებინა OSI მოდელის პირველი დონისა და მეორე დონის ქვედა ნაწილის მოდელის მოთხოვნები. ამის შედეგად პატარა ცვლილებები განიცადა ორიგინალურმა Ethernet სტანდარტმა (802.3).

Ethernet მოქმედებს OSI მოდელის ორ ქვედა: არხის და ფიზიკურ დონეზე. რადგანაც OSI მოდელი გამოიყენება მხოლოდ წარმოსახვისთვის (ახსნისათვის), ამიტომ ის ყოველთვის ზუსტად ვერ აღწერს ყველა ტექნოლოგიას და პროტოკოლს რომელიც გამოიყენება კომპიუტერულ ქსელებში. არხის დონე გაყოფილია ორ ქვედონედ. პირველი ქვედონე (ზედა - Logical Link Control (LLC) ,ხოლო მეორე ქვედონე ე.წ. Media Access Control (MAC - მედიაზე წვდომის კონტროლი. რეალურად Ethernet მოქმედებს არხის დონის მეორე (ქვედა - MAC) ქვედონეზე და ფიზიკურ დონეზე., რადგანაც (LLC) საერთოა ბევრი ტექნოლოგიისათვის

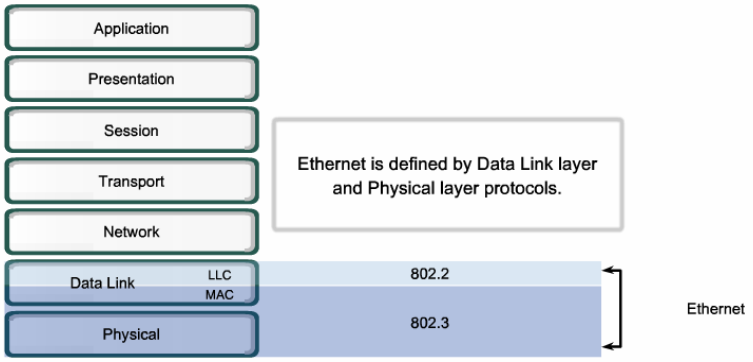
Ethernet პირველ (ფიზიკურ) დონეზე შეიცავს:

- სიგნალებს;
- ბიტთა ნაკადებს, რომლებიც მოგზაურობენ მედიაში;
- ფიზიკურ კომპონენტებს, რომლებიც ათავსებენ სიგნალებს მედიაზე;
- სხვადასხვა ტოპოლოგიებს.

Ethernet-ის პრიველ დონეს გადამწყვეტი როლი უკავია მოწყობილობებს შორის კავშირის განხორციელებაში, თუმცა მის ყოველ ფუნქციას აქვს შეზღუდვები.

Ethernet-ის მეორე (არხის) ქვედონეები, მნიშვნელოვან როლს ასრულებენ ტექნოლოგიურ თავსებადობაში და კომპიუტერულ კომუნიკაციაში. MAC ქვედონე დაკავშორებულია ფიზიკური კომპონენტებითან, რომლებიც გამოყენება ინფორმაციის დასა-კავშირებლად და ის ამზადებს მონაცემებს მედიაზე გადასაცემად.

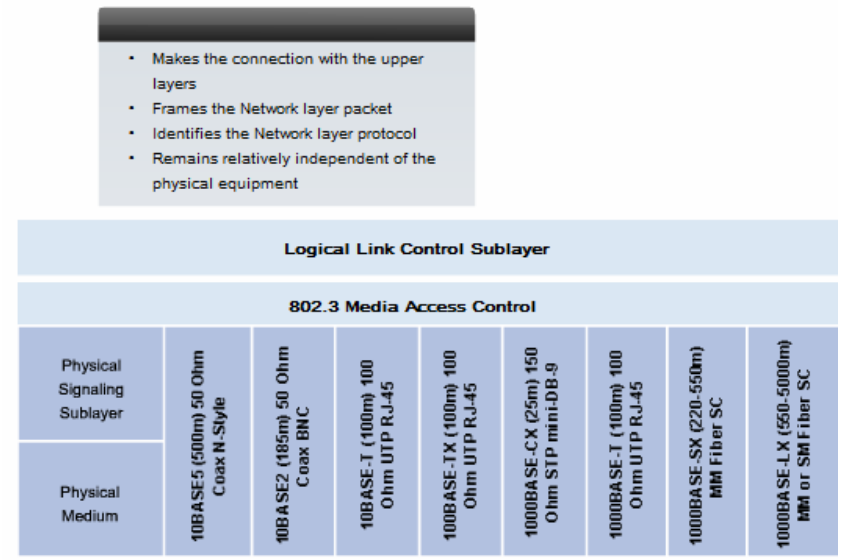
Logical Link Control (LLC) - ლოგიკური არხის კონტროლის ქვედონე, შედარებით დამოუკიდებელი რჩება ფიზიკურ მოწყობილობებისაგან, რომლებსაც იყენებენ კომპიუტერულ ქსელებში.



ნახაზი 62. Ethernet

როგორც ზემოთ ავნიშნეთ Ethernet ყოფს მონაცემთა არხის დონის ფუნქციებს ორ განსხვავებულ ქვედონედ: LLC და MAC ქვედონეები. ფუნქციები რომლებიც იყო აღწერილი OSI მოდელში მონაცემთა არხის დონისთვის მოიცავს ამ ორ ქვედონეს. ამ ორი ქვედონის გამოყენება ხელს უწყობს თავსებადობას სხვადასხვა მოწყობილობებს შორის. Ethernet-ისთვის IEEE 802.2 სტანდარტმა აღწერა LLC ქვედონის ფუნქციები და 802.3 სტანდარტმა MAC ქვედონის და ფიზიკური დონის ფუნქციები. LLC ქვედონის ფუნქცია არის კავშრის უზრუნველყოფა ზედა დონეებთან და ქსელურ პროგრამებთან, ხოლო ქვედა ქვედონის ფუნქცია არის კავშრის უზრუნველყოფა (MAC) - აპარატურასთან. LLC ქვედონე იღებს ქსელური პროტოკოლის მონაცემებს, რომელიც ჩვეულებრივ არის IPv4 პაკეტი და ამატებს მმართველ ინფორმა-

ციას იმისათვის, რომ დაეხმაროს პაკეტს დანიშნულების ადგილის მისაღწევად. მეორე დონე უკავშირდება ზედა დონეებს LLC-ის გამოყენებით. LLC წარმოდგენილია პროგრამულ უზრუნველყოფის სახით და ის დამოუკიდებელია ფიზიკურ მოწყობილობებზე. კომპიუტერში LLC შეგვიძლია წარმოვიდგინოთ როგორც ქსელური ადაპტერის დრაივერი. ეს არის პროგრამა, რომელიც შუამავლების გარეშე ურთიერთქმედებს აპარატურასთან ქსელურ ადაპტერში, რათა გადასცეს მონაცემი მედიასა და MAC ქვედონეს შორის.



ნახაზი 63. LLC - ლოგიკური არხის კონტროლის ქვედონე

MAC - არის არხის დონის (Ethernet) ქვედა ქვედონე. მას აქვს ორი ძირითადი სამუშაო:

- მონაცემთა ენკაპსულაცია - Data Encapsulation;

- მედიაზე წვდომის კონტროლი - Media Access Control.

მონაცემთა ენკაპსულაცია გვაძლევს სამ ძირითად ფუნქციას:

- შეცდომების აღმოჩენა;
- დამისამართება;
- კადრების განსაზღვრა.

მონაცემთა ენკაპსულაციის პროცესი შეიცავს ფრეიმების აწყობას მონაცემთა გადაცემამდე და ფრეიმების გარჩევას მონაცემთა მიღების შემდეგ. ფრეიმის ჩამოყალიბებაში, MAC ქვედონე ამატებს თავსართს და ბოლოსართს, მესამე დონის "პაკეტის მონაცემთა ერთეულზე" (PDU). ფრეიმების გამოყენება გვეხმარება ბიტების გადაცემაში როცა ისინი გადაიცემინ მედიაზე და მათ აწყობაში როცა ხდება მათი მიმღება.

ფრეიმის შექმნის პროცესი გვაწვდის მნიშვნელოვან მსაზღვრელებს, რომლებიც გამოიყენებიან ბიტების ჯგუფის იდენტიფიცირებისთვის რომლისგანაც შედგება ფრეიმი. ეს პროცესი ახდენს სინქრონიზაციას გადამცემ და მიმღებ მხარეებს შორის.

ენკაპსულაციის პროცესი ასევე გვაძლევს მონაცემთა არხის დონის დამისამართებას. თითოეული Ethernet თავსართი, რომელიც ემატება ფრეიმს, შეიცავს ფიზიკურ მისამართს (MAC Address), რომელიც მას აძლევს საშუალებას მიაღწიოს დანიშნულების ადგილამდე. ენკაპსულაციის დამატებითი ფუნქცია არის შეცდომების აღმოჩენა. თითოეული Ethernet ფრეიმი შეიცავს ბოლოსართს, რომელიც შედგება ციკლური ნამატის შემოწმების სისტემისაგან (CRC). სანამ ფრეიმი გაიგზავნება ქსელში, ფრეიმის ფორმირებისას ხდება გარკვეული მათემატიკური ოპერაცია,

შედეგი კი მიეწერება ფრეიმს ბოლოში ციკლური ნამატის სახით. ფრეიმის მიღების შემდეგ, მიმღები მხარე ქმნის იგივე პრინციპით CRC-ს და შემდგომ მას ადარებს მიღებულ კადრში განთავსებულ CRC-თან. თუ ეს ორი CRC ერთმანეთს ემთხვევა, შეგვიძლია ჩავთვალოთ რომ ფრეიმი მიღებულია უშეცდომოდ.

MAC ქვედონე აკონტროლებს მედიაზე კადრების განთავსებას და აგრეთვე მათ მოშორებას. როგორც მისი სახელიდან ჩანს ის მართავს მედიაზე დაშვებას, ეს შეიცავს ფრეიმის გადაცემის დაწყებას და კოლიზიის აღმოჩენის შემთხვევაში მის ხელახალ გადაცემას.

Ethernet-ის საფუძველს წარმოადგენს ლოგიკური ტოპოლოგია “მრავალი-დაშვების პრინციპი მედიაზე” (Multi-Access Bus). ეს ნიშნავს რომ ყველა მხარე (მოწყობილობა) ქსელში ინაწილებს “მედიას (გამტარს)”. ეს კი თავისმხრივ ნიშნავს, რომ ყველა მხარე იღებს ყველა ფრეიმს იმისდა მიუხედავათ არის ის განკუთვნილი მისთვის . ამის გამო თითოეულმა მიმღებმა უნდა გაარკვიოს არის ეს ფრეიმი მისთვის გამოგზავნილი თუ არა. ამისათვის ხდება მისამართების შემოწმება კადრში, რომელიც წარმოდგენილია MAC მისამართის სახით. Ethernet გვაწვდის მეთოდს რათა დავადგინოთ თუ როგორ ხდება მედიაზე წვდომის განაწილება მხარეთა შორის. კლასიკურ Ethernet-ში ამას ანხორციელებს პროტოკოლი(CSMA/CD) „ინფორმაციის გადაცემის აღმოჩენა მრავალჯერადი შეღწევა და კოლიზიის აღმოჩენა“ (Carrier Sense Multiple Access with Collision Detection).

ინტერნეტში ტრაფიკის უდიდესი ნაწილი იწყება და მთავრდება Ethernet კავშირებით. მისი დასაბამიდან 70-წლებში, Ethernet-მა განიცადა ცვლილებები, რათა ეპასუხა გაზრდილ მოთხოვნილე-

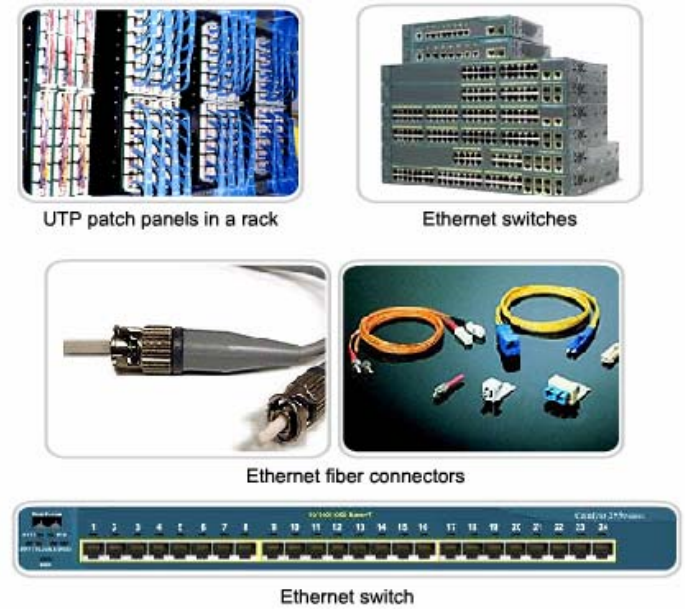
ბაზე, შექმნილიყო სწრაფი ლოკალური ქსელები. როდესაც ოპტიკურ ბოჭკოვანი კაბელი შემოვიდა ხმარებაში, Ethernet-მა გაიარა ამ ახალ ტექნოლოგიასთან ადაპტაცია და გამოიყენა მისი უპირატესობები, როგორიც არხის მაღალი გამტარობა და შეცდომების მცირე რაოდენობა. დღესდღეობით იგივე პროტოკოლს, რომელსაც გადაჰქონდა ინფორმაცია 3მბ/წმ სიჩქარით, შეუძლია გადაიტანოს ის 10გბ/წმ სიჩქარით.

Ethernet წარმატება შემდეგმა პირობებმა გამოიწვია:

- სიმარტივე და ადვილი მომსახურეობა;
- საშუალება შთანთქას ახალი ტექნოლოგიები;
- საიმედოობა;
- ინსტალაციის და გაუმჯობესების დაბალი ფასი.

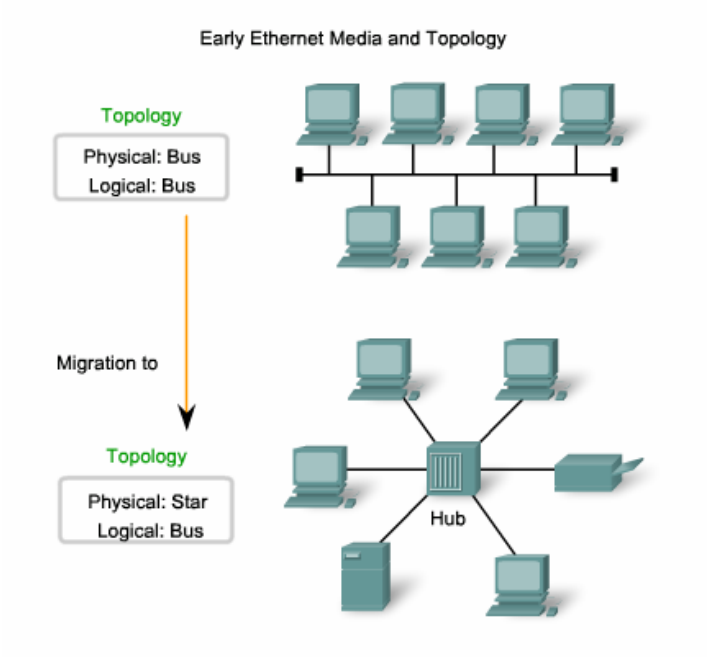
Ethernet ტექნოლოგიისთვის საფუძველი პირველად 1970 წელს შეიქმნა და პროგრამას ერქვა Alohanet. ეს იყო ციფრული რადიო ქსელი, შემუშავებული ისე რომ გადაეცა ინფორმაცია განაწილებულ რადიო სიხშირეზე ჰავაის კუნძულებს შორის. ამ ქსელისთვის საჭირო იყო ყველა მონაწილე მხარე დამორჩილებოდა პროტოკოლს, რომელშიც არადადასტურებული (Unacknowledged) გადაცემა უნდა განმეორებულიყო დროის პატარა მონაკვეთის შემდეგ. განაწილებული მედიის გამოყენების გზები იქნა შემდგომში გამოყენებული კაბელურ გამტარებში Ethernet ფორმით. Ethernet დიზაინი შექმნილი იყო ისე, რომ განეთავსებინათ რამდენიმე ურთიერთდაკავშირებული კომპიუტერი განაწილებულ სალტურ ტოპოლოგიაზე. Ethernet-ის პირველ ვერსიაში დაშვების მეთოდი იყო ცნობილი როგორც

Carrier Sense Multiple Access with Collision Detection (CSMA/CD). ის მართავდა პრობლემებს რომლებიც წარმოიქმნებოდნენ მაშინ, როდესაც რამდენიმე მოწყობილობა ერთდროულად შეეცდებოდა კავშირს განაწილებულ ფიზიკურ მედიაზე.



ნახაზი 64. Ethernet ტექნოლოგიის ფიზიკური მოწყობილობები

Ethernet-ის პირველი ვერსიები სალტურ ტოპოლოგიასთან დასაკავშირებლად იყენებდნენ კოაქსიალურ კაბელს. თითოეული კომპიუტერი პირდაპირ იყო შეერთებული “მაგისტრალურ არხთან” (Backbone). ეს ვერსიები იყო ცნობილი როგორც Thicknet (10BASE5) და Thinnet (10BASE2).



ნახაზი 65. Ethernet ტექნოლოგიის პირველი ვერსიები

10BASE5 იყენებდა სქელ კოაქსიალურ კაბელს, რომელიც იძლეოდა საშუალებას 500 მეტრამდე კაბელის გაყვანას, სანამ დასჭირდებოდა განმეორებელი (Repeater). 10BASE2 კი იყენებდა თხელ კოაქსიალურ კაბელს, თუმცა ის უფრო ელასტიური იყო და მისი გაყვანა შეიძლებოდა 185 მეტრამდე.

ორიგინალური Ethernet-ის მოღწევამ დღევანდელ დღემდე გამოიწვია შემდეგმა ფაქტორმა, მეორე დონის ფრეიმის სტრუქტურა პრაქტიკულად შეუცვლელი რჩება. ფიზიკური მედია, მედიაზე დაშვება და მედია კონტროლი განვითარდა და აგრძელებენ განვითარებას. თუმცა Ethernet-ის თავსართი და ბოლოსართი შეუცვლელი დარჩა. Ethernet ადრინდელ

ვარიანტებში იყო გამოყენებული დაბალი გამტარობის ლოკალური ქსელების გარემოში, სადაც დაშვებას განაწილებულ მედიაზე მართავდა CSMA, ხოლო შემდგომ CSMA/CD. იმასთან ერთად რომ ის იყო ლოგიკური სალტური ტოპოლოგია მონაცემთა არხის დონეზე, ის ასევე იყო სალტური ტოპოლოგია ფიზიკურ დონეზეც. ეს ტოპოლოგია გახდა უფრო პრობლემატური, როდესაც ლოკალური ქსელები გაიზარდნენ და მათი მომსახურეობებიც მომრავლდა. კოაქსიალური კაბელები ჩაანაცვლეს UTP კაბელების ადრეულმა ვარიანტებმა. კოაქსიალურთან შედარებით ეს კაბელები მსუბუქი და იაფია. მათთან მუშაობა ბევრად უფრო მარტივი იყო. ფიზიკური ტოპოლოგიაც შეიცვალა ვარსკვალურ ტოპოლოგიად კონცენტრატორების (Hub) გამოყენებით. ისინი კავშირებს აკონცენტრირებდნენ, სხვა სიტყვებით რომ ვთქვათ, მას ინდივიდუალური კაბელებით უკავშირდება ყველა ქსელში ჩართული მოწყობილობა და ეს საშუალებას იძლევა ქსელი აღქმულ იქნას როგორც ერთი განაწილებული მედია. როდესაც ფრეიმი შემოვა ერთ პორტზე, მისი გადაკოპირება ხდება ყველა დანარჩენ პორტზე გარდა იმ პორტისა საიდანაც შემოვიდა ფრემი, შესაბამისად ქსელის ყველა სეგმენტი იღებს ფრეიმს. კონცენტრატორის გამოყენებამ სალტურ ტოპოლოგიაში მას შემატა საიმედოობა და ერთი კონკრეტული კაბელის მწყობრიდან გამოსვლის შემთხვევაში არ ითიშება მთელი ქსელი. თუმცა ყველა დანარჩენი პორტისთვის ფრეიმის გამეორებამ არ გადაწყვიტა კოლიზიების პრობლემა.

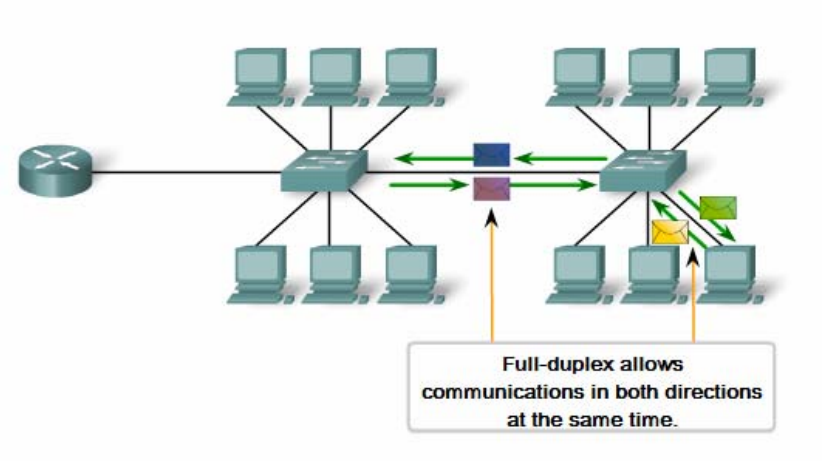
კლასიკური Ethernet

ტიპიურად 10BASE-T ქსელებში, ცენტრალური წერტილი ქსელის სეგმენტისა იყო კონცენტრატორი. ამან წარმოშვა განაწილებული მედია. იმის გამო, რომ მედია არის განაწილებული, მხოლოდ ერთ

მხარეს შეეძლო წარმატებით ინფორმაციის გადაცემა ნებისმიერ მოცემულ დროის მონაკვეთში. ამ კავშირს ეწოდება ნახევარ-დუპლექსური კომუნიკაცია. მეტი მოწყობილობების დამატებასთან ერთად, ქსელში კადრების კოლიზიების რიცხვი მატულობდა. მაშინ, როდესაც კოლიზიების რიცხვი დაბალი იყო CSMA/CD მართვის შედეგად მომხმარებლისთვის არ იგრძნობოდა დისკომფორტი. თუმცა მათი რიცხვის გაზრდასთან ერთად შეიქმნა დისკომფორტიც. მსგავსი სიტუაციია იქნება როდესაც დიღით ადრე მივემგზავრებით სადმე, გზა თავისუფალია და მასზე ცოტა მანქანები მოზრაობენ, თუმცა საღამოთი როდესაც გზებზე ბევრი მანქანა იწყებს მოძრაობას, იქმნება საცობები და მოძრაობა შენელებულია.

დღევანდელი Ethernet

ლოკალური ქსელების განვითარების ერთერთი უმნიშვნელოვანესი ეტაპი იყო სვიჩების (კომუტატორების) გამოჩენა, რომლებმაც ჩაანაცვლეს კონცენტრატორები. ეს დროში ახლოს მოხდა 100BASE-TX Ethernet-ის შექმნასთან. სვიჩებს შეუძლიათ აკონტროლონ მონაცემთა ნაკადი და გააგზავნონ ფრეიმი მხოლოდ იმ პორტზე, რომლისთვისაც არის ის განკუთვნილი. სვიჩი ამცირებს იმ მოწყობილობების რაოდენობას, რომლებიც იღებენ კონკრეტულ ფრეიმს, რადგანაც სვიჩი ანხორციელებს მიზანმიმართულ გადაცემას პორტიდან პორტზე და ამით ამცირებს კოლიზიების რაოდენობას. ზემოთანიშნული ფუნქციის და შემდგომ სრული-დუპლექსის კომუნიკაციის გამოჩენამ (ერთდროულად გადაცემის და მიღების საშუალება) გამოიწვია 1გბიტ/წამში და უფრო სწრაფის Ethernet შექმნა .



ნახაზი 66. სვიჩის გამოყენებით აგებული ლოკალური ქსელი

თანამედროვე მულტიმედიური პროგრამები, რომლებიც იყენებენ კომპიუტერულ ქსელს, ყოველდღიურად ტვირთავენ ყველაზე სწრაფ ქსელებსაც კი. მაგალითად, VoIP ტექნოლოგიის და მულტიმედიური გამოყენების ზრდამ, საჭირო გახადა უფრო სწრაფ კავშირები, ვიდრე არის 100მბიტ/წამში Ethernet.

გიგაბიტ Ethernet გამტარობა შეადგენს 1000 მბიტ/წმ. ეს მიიღება სრული-დუპლექსის და UTP ან ოპტიკურ ბოჭკოვანი ტექნოლოგიების გამოყენებით.

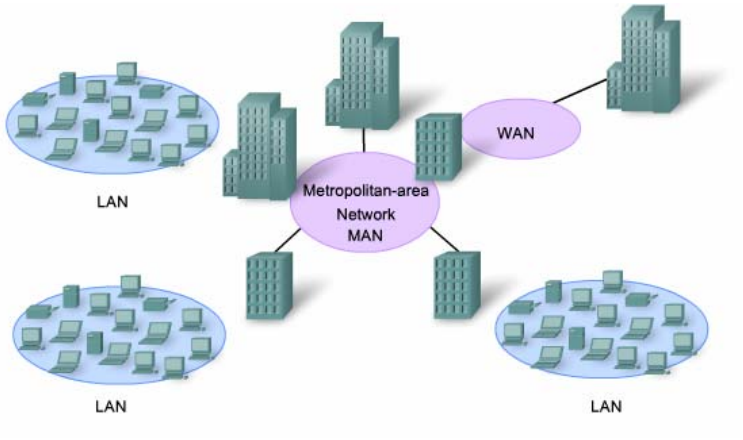
როდესაც ხდება ქსელის განახლება 100მბიტ/წამის გამტარობიდან 1გბიტ/წამამდე ან მეტი, განსხვავება საგრძნობია.

ქსელის განახლება 1გბ/წმ-მდე ყოველთვის არ ნიშნავს მთელი ქსელის ინფრასტრუქტურის გამოცვლას. ზოგიერთი მოწყო-

ბილობა თანამედროვე ქსელებში შეიძლება ძალიან პატარა დანახარჯებით ამუშავდეს უფრო მაღალ სიჩქარეებზე.

ნახაზი 67. ახალი მოწყობილობები და სერვისები, რომლებიც ითხოვენ სწრაფ კომუნიკაციას

ოპტიკურ-ბოჭკოვანი კაბელის შემოსვლასთან ერთად ზღვარი ლოკალურ ქსელსა და ფართო არის ქსელთან წაიშალა. Ethernet თავდაპირველად შემოისაზღვრებოდა ერთი შენობით და შემდეგ გავრცელდა შენობათა შორის. დღეს ის შეიძლება მთელს ქალაქს ფარავდეს და მას ეწოდებოდეს საქალაქო ქსელი (Metropolitan Area Network (MAN)).



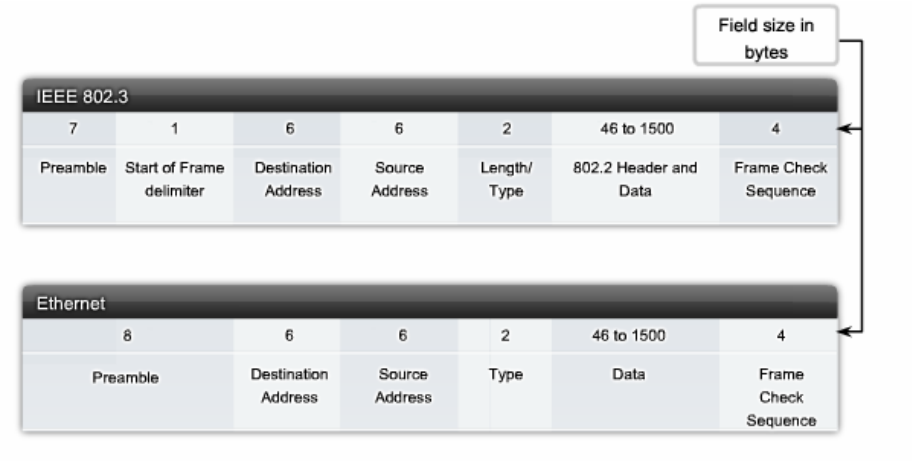
ნახაზი 68. გიგაბიტ Ethernet

ფრეიმის ფორმატი Ethernet ტექნოლოგიაში

Ethernet ფრეიმის სტრუქტურა ამატებს თავსართებს და ბოლოსართებს მესამე დონის მონაცემთა პაკეტის ერთეულზე, რათა მოახდინოს გასაგზავნი ინფორმაციის ენკაპსულაცია და მისი გადაცემა ფიზიკურ მედიაში.

ორივეს, Ethernet თავსართსაც და ბოლოსართსაც აქვს ინფორმაციის რამდენიმე სექცია, რომელიც გამოიყენება Ethernet პროტოკოლის მიერ. ფრეიმის თითოეულ სექციას ეწოდება ველი. Ethernet ფრეიმირების ორი სტილი არსებობს: DIX Ethernet სტანდარტი რომელიც ეხლა არის ცნობილი როგორც Ethernet II და IEEE 802.3 რომლის განახლებაც მოხდა რამდენჯერმე, ახალი ტექნოლოგიების გასათვალისწინების მიზნით. მათ შორის სხვაობა მინიმალურია. ყველაზე დიდი სხვაობა არის საწყისი ფრეიმის მსაზღვრელის დამატება (Start Frame Delimiter (SFD)) და ტიპის

ველისა მცირე შეცვლა, ტიპის ველს დაემატა სიგრძის პარამეტრი 802.3-ში.



ნახაზი 69. 802.3 და Ethernet ფრეიმის ფორმატი

ორივე სტანდარტი აღწერს ფრეიმის მინიმალურ ზომას როგორც 64 ბაიტს და მაქსიმალურს როგორ 1518 ბაიტს. ეს შეიცავს ყველა ბაიტს, დანიშნულების ადგილის მისამართიდან ფრეიმის შემმოწმებლამდე. პრეამბულა და საწყისი ფრეიმის მსაზღვრელი (SFD)არ არის ჩათვლილი როდესაც ვსაზღრავთ ფრეიმის ზომას.

IEEE 802.3ac სტანდარტში, რომელიც გამოვიდა 1998 წელს, ფრეიმის ზომა გაზრდილია 1522 ბაიტამდე. ეს მოხდა ახალი ტექნოლოგიისთვის, რომელსაც ეწოდება ვირტუალური ლოკალურ ქსელი. თუ კი ფრეიმი არის უფრო პატარა ვიდრე მინიმალური ზომა ან უფრო დიდი ვიდრე მაქსიმალური ზომა მიმღები მოწყობილობა აგდებს ფრეიმს.

პრეამბულა და ფრეიმის საწყისი მსაზღვრელი ველი

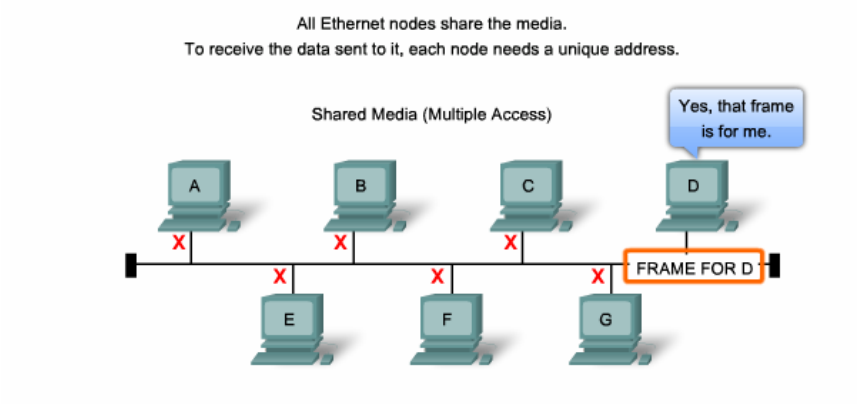
პრეამბულა (7 ბაიტი) და ფრეიმის საწყისი მსაზღვრელი (1 ბაიტი) გამოიყენება გამგზავნ და მიმღებ მოწყობილობებს შორის სინქრონიზაციისათვის. პირველი რვა ბაიტი გამოიყენება მიმღები ჰოსტის ყურადღების მოსაპოვებლად. პრაქტიკულად პირველი რამდენიმე ბაიტი ეუბნება მიმღებს რომ მოემზადოს ახალი ფრეიმის მისაღებად.

დანიშნულების ადგილის (ადრესატის) MAC მისამართის ველი

დანიშნულების ადგილის MAC მისამართის ველი (6 ბაიტი) არის მიმღების იდენტიფიკატორი. ასეთი მისამართი გამოიყენება მეორე დონეზე, რათა მოწყობილობებმა გაარკვიონ არის თუ არა ფრეიმი მათთვის განკუთვნილი. მისამართი მიღებულ კადრში შედარდება მოწყობილობის მისამართთან და თუ დაემთხვა მოწყობილობა მიიღებს ფრეიმს.

წყაროს (გამგზავნის) MAC მისამართის ველი

წყაროს MAC მისამართის ველი (6 ბაიტი) ფრეიმის გამგზავნი ქსელური ადაპტერის ან ინტერფეისის იდენტიფიკატორია. ამ მისამართებს სვიჩებიც იყენებენ და ამატებენ მათ თავიანთ ცხრილებში.



ნახაზი 70. ფრეიმის გაგზავნა კონკრეტულ მისამართზე

სიგრძის/ტიპის ველი

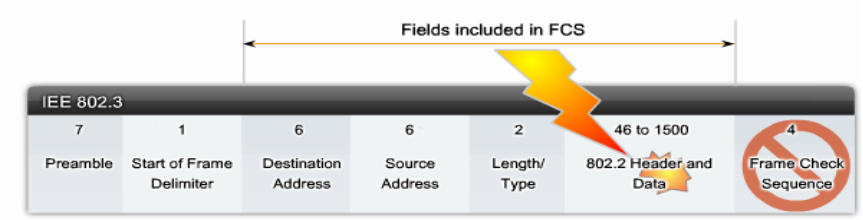
1997 წლამდე IEEE 802.3 სტანდარტისათვის სიგრძის ველი წარმოადგენდა ფრეიმის მონაცემთა ველის ზუსტ ზომას. მოგვიანებით ეს გამოიყენეს როგორც ფრეიმის შემმოწმებლის ნაწილი, რათა შემოწმდეს რომ ფრეიმი მიღებულია სრულად და დაზიანებების გარეშე. თუ ველის დნიშნულება არის ისე როგორც Ethernet II ტიპის აღწერაშია მოცემული, ტიპის ველი აღწერს თუ რომელი პროტოკოლი გამოიყენება. ეს ორივე გამოყენება შეჯამებულია 1997 წლის IEEE 802.3x სტანდარტში, რადგანაც ორივე ხშირად გამოიყენებოდა. Ethernet II ტიპის ველი არის ჩაშენებული დღევანდელ 802.3 ფრეიმის აღწერაში. როდესაც მხარე იღებს ფრეიმს, ის ამოწმებს ტიპის ველს რათა დაადგინოს თუ რომელი ზედა დონის პროტოკოლი არის გამოყენებული. თუ ამ ველის შიგთავსი მეტია თექვსმეტობით 0x0600 ან ათობით 1536 რიცხვზე, მაშინ მისი შიგთავსი არის ტიპი, ხოლო თუ ის ნაკლებია თექვსმეტობით 0x05DC და ათობით 1500 რიცხვზე მაშინ ის სიგრძის ველია. ასე განასხვავებენ Ethernet II-ს და 802.3 ფრეიმს.

მონაცემთა და Pad ველები

მონაცემთა და Pad ველები (46 - 1500ბაიტი) შეიცავენ ენკაპსულირებულ მონაცემებს ზედა დონიდან, რომელიც არის 3 დონის პაკეტი, როგორც წესი ხშირად IPv4 –ს პაკეტი. ყველა ფრეიმი უნდა იყოს მინიმუმ 64 ბაიტი. თუ გადასაცემი პაკეტი არის პატარა, ენკაპსულირებული Pad გამოიყენება რათა მოხდეს ზომის გაზრდა მინიმუმამდე.

ფრეიმის შემოწმების ველი

ეს ველი არის 4 ბაიტი და გამოიყენება შეცდომების შესამოწმებლად.



ნახაზი 71. ფრეიმის შემოწმების ველი

ის იყენებს ციკლური ნამატის შემოწმების ხერხს (cyclic redundancy check (CRC)). გამგზავნი მოწყობილობა აგზავნის ამ რეზულტატს ფრეიმის შემოწმების ველით (Check Sequence (FCS)), ხოლო მიმღები მოწყობილობა, ფრეიმის მიღების შემდეგ, ანხორციელებს იგივე პროცესს და ადარებს თავის მიერ მიღებულ გამოთვლებს გამოგზავნილი ფრეიმის (CRC). დამთხვევის შემთხვევაში შეცდომა არ არის, თუ არა და ჩაითვლება რომ მონაცემები დაზიანებულია და მოხდება ფრეიმის გადაგდება. მონაცემის

დაზიანების მიზეზი შეიძლება იყოს ელექტრული სიგნალების განადგურება, რომლებიც წარმოადგენენ ბიტებს.

ფიზიკური მისამართი

თავდაპირველად Ethernet იყო განხორციელებული სალტური ტოპოლოგიით განაწილებულ მედიაზე. ეს დაბალი ტრაფიკის ან პატარა ქსელებში იყო მისაღები. თუმცა პრობლემა რომელიც იყო გადასაწყვეტი მდგომარეობდა იმაში, რომ ფრეიმის გაგზავნის შემდეგ ყველა მოწყობილობასთან უნდა მომხდარიყო მოწყობილობების იდენტიფიცირება და მოწყობილობას უნდა გაეგო არის თუ არა მისთვის ეს ფრეიმი გამოგზავნილი. ამიტომ მოხდა უნიკალური იდენტიფიკატორის შემოღება, რომელსაც ეწოდება მედიაზე დაშვების კონტროლის მისამართი (MAC) ან უბრალოდ ფიზიკური მისამართი. ის იქნა გამოყენებული გამგზავნის და მიმღების დადგენაში და იმისდა მიუხედავად, თუ რა ტიპის Ethernet იყო გამოყენებული ქსელში, ეს დამისამართება წარმოადგენდა იდენტიფიცირებისის მეთოდს OSI მოდელის ქვედა დონეზე. ფიზიკური მისამართი ემატება მეორე დონეზე. ის არის 48 ბიტიანი ორობითი მნიშვნელობა, გამოხატული 12 თექვსმეტობითი ციფრით.

ფიზიკური მისამართის სტრუქტურა

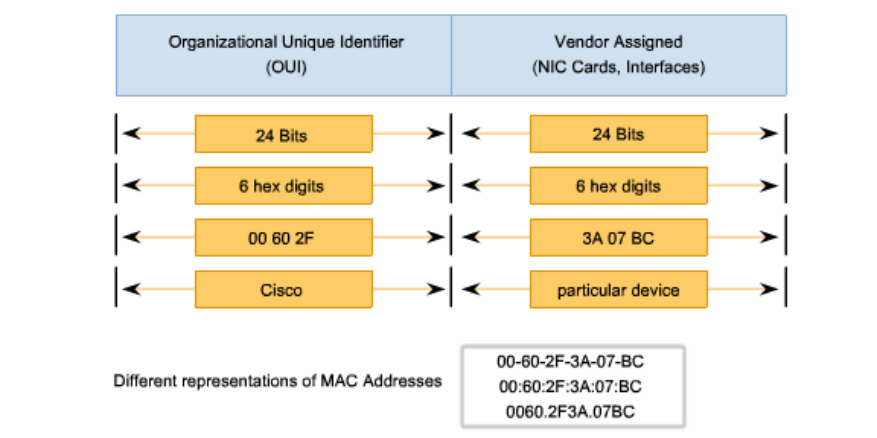
ფიზიკური მისამართის მნიშვნელობა არის IEEE-ს მიერ მწარმოებლებისათვის შემოღებული წესების პირდაპირი შედეგი, რათა გლობალურად უნიკალური მნიშვნელობა მიგვეღო თითოეული Ethernet მოწყობილობისათვის. წესები თხოვენ თითოეულ მწარმოებელს, რომელიც ყიდის Ethernet

მოწყობილობებს, დარეგისტრირდეს IEEE-სთან და ის მიანიჭებს 3 ბაიტიან კოდს, რომელსაც ჰქვია ორგანიზაციის უნიკალური იდენტიფიკატორი (OUI).

IEEE ითხოვს მწარმოებლისგან მხოლოდ ორი მარტივ წესს:

1. ყოველი MAC მისამართი რომელიც უნდა მიენიჭის ქსელურ ადაპტერს, საჭიროა პირველი 3 ბაიტში იყოს ორგანიზაციის იდენტიფიკატორი.

2. ყოველი MAC მისამართი მწარმოებლის ერთნაირი პირველი 3 ბაიტით უნდა ფლობდეს უნიკალურ მნიშვნელობას, ბოლო 3 ბაიტში.



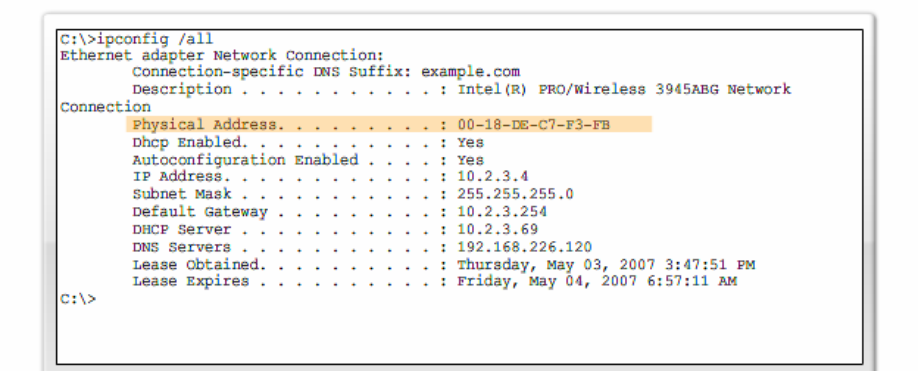
ნახაზი 72. MAC მისამართის სტრუქტურა

ფიზიკურ მისამართს ხშირად უწოდებენ “ჩამწვარ მისამართს” რადგანაც ის არის ჩაწერილი ქსელური ადაპტერის წასაკითხ ROM მეხსიერებაში. ეს ნიშნავს, რომ მისამართი არის შეუცვლელი და ჩაწერილია სამუდამოდ. თუმცა კომპიუტერის ჩატვირთვის

შემდეგ, ხდება ფიზიკური მისამართის ოპერატიულ მეხსიერებაში ჩაწერა და კადრების შემოწმებისას ოპერატიულ მეხსიერებაში მყოფ MAC მისამართთან ხდება შედარება.

ქსელური მოწყობილობები

როდესაც წყარო აგზავნის მონაცემებს Ethernet ქსელში, თავსართში ხდება ადრესატის და წყაროს ანუ გამომგზავნის ფიზიკური მისამართის ჩაწერა. წყარო აგზავნის ფრეიმს ქსელში, თითოეული ქსელში ჩართული ადაპტერი ხედავს ინფორმაციას და ამოწმებს ფიზიკურ მისამართს, თუ მიღებული ფრეიმის ადრესატის მისამართი არ ემთხვევა მის საკუთარ მისამართს, მოწყობილობა აგდებს ფრეიმს. როდესაც ფრეიმი აღწევს დანიშნულების მისამართს და ფიზიკური მისამართი ემთხვევა, ქსელური ადაპტერი გადასცემს ფრეიმს OSI-ს ზედა დონეებზე, სადაც ის გაივლის დეკაპსულაციის პროცესს.



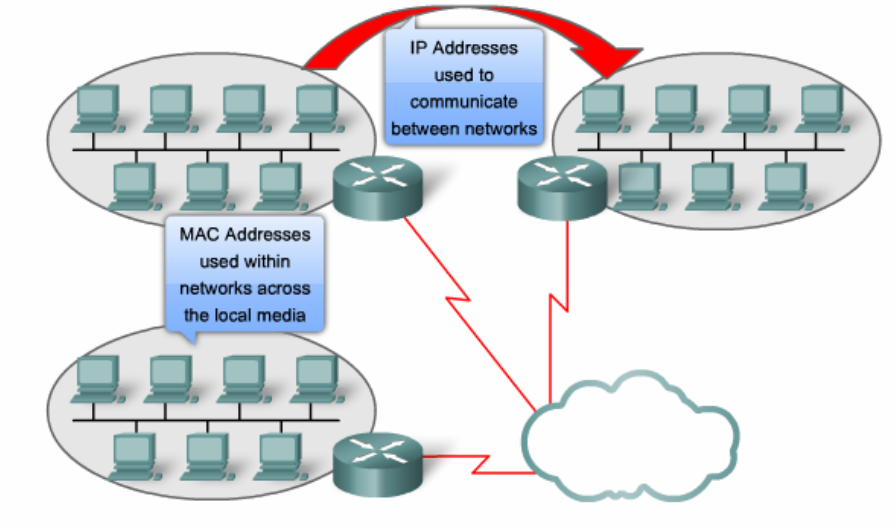
ნახაზი 73. MAC მისამართის ნახვა

ყველა მოწყობილობა დაკავშირებული Ethernet ლოკალურ ქსელთან ფლობს ფიზიკურ მისამართს. სხვადასხვა მწარმოებლებმა შესაძლოა წარმოსახონ ეს მისამართი სხვადასხვა 16-ობით ფორმატებში. მაგ. 00-05-9A-3C-78-00, 00:05:9A:3C:78:00, ან 0005.9A3C.7800. ფიზიკური მისამართების მინიჭება ხდება: კომპიუტერებისთვის, პრინტერებისთვის, სვიჩებისთვის, მარშრუტიზატორებისთვის და ნებისმიერი მოწყობილობისთვის, რომელმაც უნდა მიიღოს ან გააგზავნოს ინფორმაცია ქსელში.

დამისამართება სხვადასხვა დონეებზე

მონაცემთა არხის დონე

როგორც ზემოთ ავღნიშნეთ, OSI მოდელის მეორე დონეზე ხდება ფიზიკური დამისამართება. ეს მისამართი გამოიყენება კადრების გადასაცემად ლოკალურ მედიაზე და გვაძლევენ ჰოსტებისთვის უნიკალურ მისამართებს. ფიზიკური დამისამართება არ არის იერარქიული. ისინი ასოცირებული არიან კონკრეტულ მოწყობილობასთან და არა რომელიმე ადგილმდებარეობასთან ან რომელიმე ქსელთან, სადაც ისინი არიან მიერთებული. ამ მეორე დონის მისამართებს არ აქვთ მნიშვნელობა ლოკალური ქსელის გარეთ. პაკეტს შეიძლება მოუწიოს რამდენიმე მონაცემთა არხის ტექნოლოგიაში გავლა, ლოკალურ ან გლობალურ ქსელში სანამ ის მიაღწევს დანიშნულების ადგილს. შესაბამისად წყაროს მოწყობილობას არ აქვს ინფორმაცია(ცოდნა) თუ რა ტექნოლოგია იქნება გამოიყენებული საშუამავლო მოწყობილობებში და დანიშნულების ადგილის ქსელში. აგრეთვე არ აქვს ინფორმაცია მათი მეორე დონის მისამართის და ფრეიმის სტრუქტურაზე.



ნახაზი 74. დამისამართება სხვადასხვა დონეზე

ქსელური დონე

მესამე დონის მისამართი, ისეთი როგორიც არის IPv4 მისამართი, გვაძლევს ლოგიკურ დამისამართებას, რომელიც გასაგებია წყაროშიც და დანიშნულების ადგილშიც.

იმისთვის რომ პაკეტმა მიაღწიოს თავის საბოლოო დანიშნულების ადგილს, მას წყაროდანვე თან მიაქვს დანიშნულების ადგილის-მესამე დონის მისამართი. თუმცა გზადაგზა, მისი ფრეიმირებისას (მეორე დონეზე ფრეიმის შექმნა) სხვადასხვა მონაცემთა არხის დონის პროტოკოლების მიერ, გამოყენებული იქნება სხვადასხვა მეორე დონის მისამართი, რომელიც საჭიროა მხოლოდ იმ ლოკალურ ნაწილში მისი მოგზაურობისას.

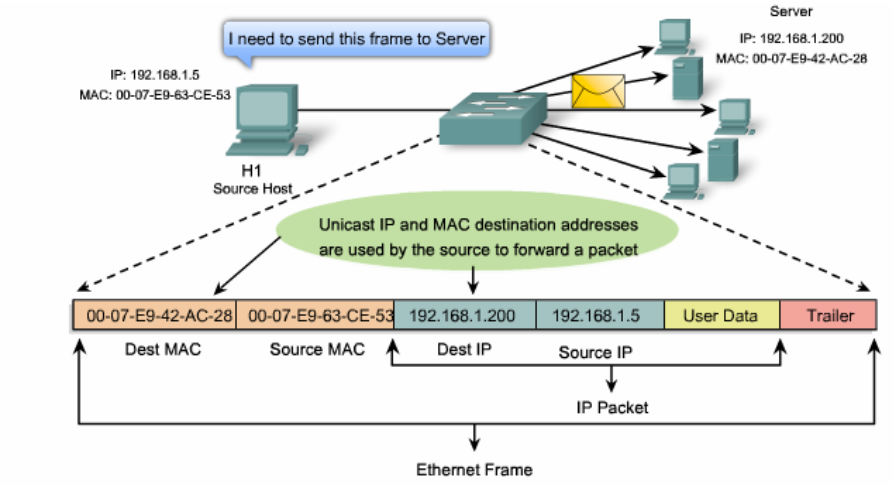
მოკლედ:

ქსელური დონის მისამართი პაკეტს აძლევს საშუალებას გადაცემულ იქნას ის დანიშნულების ადგილისაკენ.

მონაცემთა არხის დონის მისამართი პაკეტს აძლევს საშუალებას გადაცემულ იქნას სეგმენტებს შორის.

უნივერსალური მაუწყებლობა (Unicast)

Ethernetში გამოიყენება სხვადასხვა ფიზიკური მისამართები, მეორე დონის Unicast, Multicast და Broadcast კომუნიკაციისთვის.



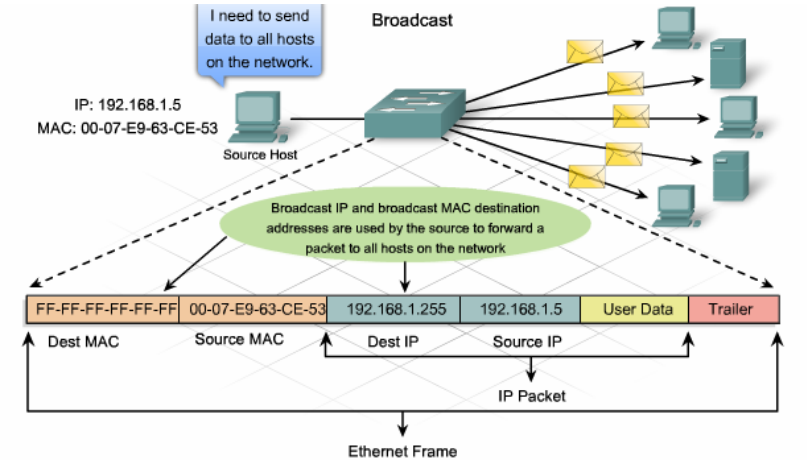
ნახაზი 75. Unicast IP და MAC მისამართი გამოყენებული გამგზავნი ჰოსტის მიერ

Unicast მისამართი არის უნიკალური მისამართი, რომელიც გამოიყენება ფრეიმის გაგზავნისას ერთი წყარო მოწყობილობიდან ერთ დანიშნულების ადგილის მოწყობილობამდე.

მაგ. ჰოსტი IP მისამართით 192.168.1.5(წყარო) აგზავნის ვებ გვერდის მოთხოვნას სერვერთან რომლის მისამართია 92.168.1.200. Unicast პაკეტის გასაგზავნად და მისაღებად, დანიშნულების ადგილის IP მისამართი უნდა იყოს პაკეტის თავსართში, ხოლო შესაბამისი დანიშნულების ადგილის ფიზიკური მისამართი უნდა იყოს Ethernet ფრეიმის თავსართში. IP მისამართი და ფიზიკური მისამართი ერთობლივად უზრუნველყოფენ მონაცემების დანიშნულების ადგილამდე მიიტანას.

ფართო-მაუწყებლობა (Broadcast)

Broadcast-ის შემთხვევაში პაკეტი შეიცავს დანიშნულების ადგილის IP მისამართს, რომელსაც აქვს სულ ორობითი 1-იანები ჰოსტის ნაწილში. ამითი ნაგულისხმებია, რომ ყველა ჰოსტი ლოკალურ ქსელში მიიღებს ამ პაკეტს, ანუ ეს არის პაკეტი რომელიც განკუთვნილია ყველა ჰოსტისთვის ლოკალურ ქსელში. ბევრი პროტოკოლი იყენებს ფართო-მაუწყებლობას, მათ შორის არის ჰოსტების კონფიგურირების დინამიური პროტოკოლი და მისამართის დადგენის პროტოკოლი (ARP).

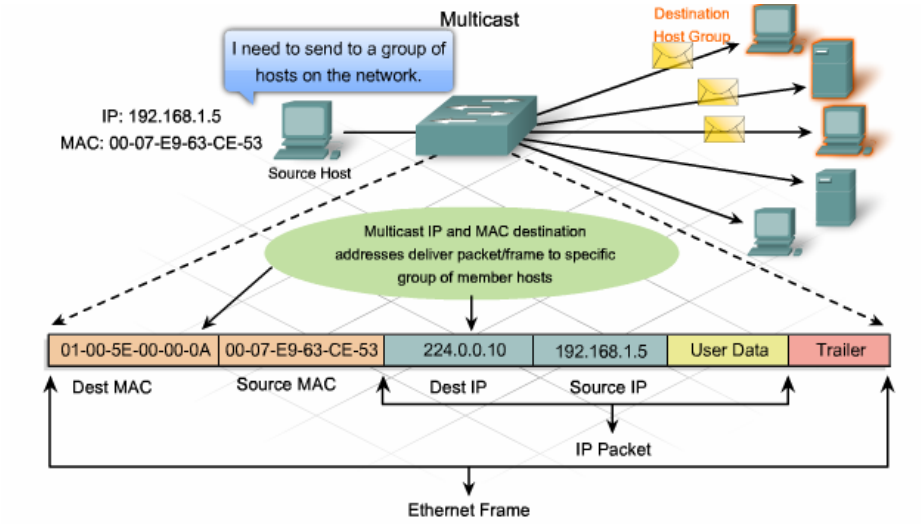


ნახაზი 76. ფართო-მაუწყებლობა (Broadcast)

როგორც მოცემულია ნახაზში, Broadcast IP მისამართს რომელიც განკუთვნილია მთელი ქსელისთვის ,უცილებელია მოყვებოდს Broadcast MAC მისამართი, რომელიც წარმოადგენს ყველა ქსელში ჩართულ მოწყობილობას. ეს მისამართი არის თექვსმეტობითი FF-FF-FF-FF-FF-FF.

მრავალობითი მაუწყებლობა (Multicast)

ეს მისამართები წყაროს მოწყობილობას აძლევს საშუალებას გაუგზავნოს პაკეტი მოწყობილობების ჯგუფს. მოწყობილობები რომლებიც შედიან Multicast ჯგუფში, მათ ენიჭებათ მისამართები 224.0.0.0-დან 239.255.255.255-მდე. იმის გამო, რომ ეს მისამართები წარმოადგენენ მოწყობილობების ჯგუფს , ისინი შეიძლება იყვნენ მხოლოდ დანიშნულების ადგილი, ხოლო წყარო ყოველთვის იქნება Unicast მისამართი.



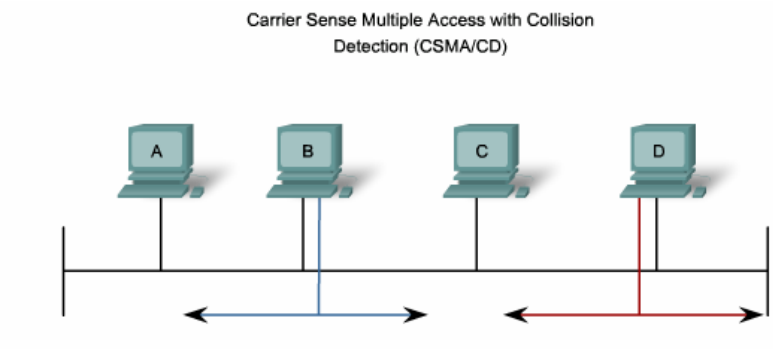
ნახაზი 77. მრავალობითი მაუწყებლობა (Multicast)

მაგალითი იმისა თუ სად შეიძლება გამოვიყენოთ Multicast მისამართები, არის თამაშები, სადაც მრავალი მოთამაშე არის დაკავშირებული სერვერთან და ერთიდაიგივე თამშს თამაშობს. მეორე მაგალითი - დისტანციური სწავლება ვიდეო კონფერენციის გამოყენებით, სადაც ბევრი სტუდენტია დაკავშირებული ერთ კლასთან, ისინი იღებენ იდენტურ ინფორმაციას.

ისევე როგორც Unicast და Broadcast მისამართებში Multicast IP მისამართს უცილებელია მოყვებოდს Multicast MAC მისამართი. Multicast MAC მისამართს გააჩნია სპეციალური მისამართი და ის იწყება 01-00-5E და გრძელდება ჯგუფის IP მისამართის ბოლო 23 ბიტის კონვერტაციით თექვსმეტობითში, დარჩენილი ბიტი ფიზიკურ მისამართში ყოველთვის არის “0”.

მედიაში შეღწევის კონტროლი CSMA/CD

განაწილებულ მედია სივრცეში ყველა მოწყობილობას აქვს გარანტირებული წვდომა გამტარზე, თუმცა მათ არ აქვთ პრიორიტეტი დაშვებაზე. თუ კი ერთზე მეტი მოწყობილობა ერთდროულად აგზავნის სიგნალს, ხდება კოლიზია და უნდა მოხდეს ქსელის "აღდგენა" იმისათვის, რომ გაგრძელდეს კომუნიკაცია.



ნახაზი 78. მედიაში შეღწევის კონტროლი

კოლიზია არის საფასური იმისა რომ Ethernet-ში არის დაბალი ლოდინის დრო თითეულ გადაცემაში. ეს ნიშნავს იმას რომ, მოწყობილობა სწრაფად იღებს გადაწყვეტილებას

Ethernet იყენებს (CSMA/CD Carrier Sense Multiple Access with Collision Detection), რათა მოახდინოს კოლიზიის აღმოჩენა და მართოს კომუნიკაციის აღდგენის პროცესი.

იმის გამო, რომ ყველა კომპიუტერი Ethernet-ში იყენებს ერთი და იგივე მედიას, გავრცელებული კოორდინაციის სქემა (CSMA) გამოიყენება ელექტრული აქტივობის აღმოსაჩენად კაბელში.

მოწყობილობას შემდგომ შეუძლია დაადგინოს როდის დაიწყოს გადაცემა. როდესაც მოწყობილობა აღმოაჩენს რომ სხვა არცერთი მოწყობილობა არ აგზავნის ფრეიმს ან მატარებელ სიგნალს, მოწყობილობა დაიწყებს გადაცემას.

მატარებელი სიგნალის აღმოჩენა (Carrier Sense)

CSMA/CD დაშვების მეთოდში ყველა ქსელური მოწყობილობამ რომელსაც აქვს გაზაგზავნი ინფორმაცია, გაგზავნამდე უნდა მოისმინოს ქსელს.

თუ მოწყობილობა აღმოაჩენს სხვა მოწყობილობის მიერ გადაცემულ სიგნალს, ის იცდის გარკვეული დროის განმავლობაში, ამ დროის გასვლის შემდეგ მოწყობილობა ხელმეორედ ცდილობს მედიაზე შეღწევას.

როდესაც არ ხდება ტრაფიკის აღმოჩენა, მოწყობილობა იწყებს მონაცემის გადაცემას. სანამ ეს გადაცემა გრძელდება მოწყობილობა განაგრძობს უსმინოს ტრაფიკის ან კოლიზიებს ლოკალურ ქსელში. როდესაც მონაცემი გაიგზავნება, მოწყობილობა ბრუნდება საწყისი სმენის მდგომარეობაში.

მრავალი-დაშვება (Multi-access)

თუ მანძილი მოწყობილობებს შორის იმდენად დიდია, რომ როდესაც ერთი მოწყობილობა იწეყებს გადაცემას, ხოლო მეორეს პირველის მიერ გადაცემული სიგნალი არ მისვლია(სიგნალის გადაცემას ჭირდება გარკვეული დრო), შეიძლება მოხდეს ისე რომ მეორემაც დაიწყოს გადაცემა. მაშინ ეს სიგნალები სადმე გზაში ერთმანეთს დაეჯახება და მონაცემი გაფუჭდება, თუმცა სიგნალი

მთლიანად არ გაქრება და დამახინჯებული ფორმით განაგრძობს მოგზაურობას.

კოლიზიის აღმოჩენა (Collision Detection)

როდესაც მოწყობილობა სმენის რეჟიმშია, მას შეუძლია აღმოაჩინოს მოხდება თუ არა კოლიზია. კოლიზიის აღმოჩენა არის შესაძლებელი იმიტომ რომ ყველა მოწყობილობას შეუძლია აღმოაჩინოს სიგნალის ამპლიტუდის მომატება ჩვეულებრივთან შედარებით.

მას შემდეგ რაც მოხდება კოლიზია, ყველა მოწყობილობა ისევე როგორც გადაცემაში მონაწილე მოწყობილობები აღმოაჩენს ამას, იმიტომ რომ კოლიზიური სიგნალი განსხვავებლია ჩვეულებრივი სიგნალისგან, რომელიც ფორმირდება მონაცემების გადაცემისას. აღმოჩენის შემდეგ, ყველა მოწყობილობა რომელიც აგზავნიდა ინფორმაციას, აგრძელებენ გაგზავნას რათა დარწმუნდნენ იმაში, რომ ყველა ქსელში ჩართული მოწყობილობებიც აღმოაჩენენ ამ კოლიზიას.

დახშობის სიგნალი და შემთხვევითი უკან დახევა

მას შემდეგ რაც კოლიზიას აღმოაჩენენ გადამცემი მოწყობილობები, ისინი გააგზავნიან დამხშობ სიგნალს. ის გამოიყენება იმისთვის, რომ შეატყობინონ სხვა მოწყობილობებს კოლიზიის შესახებ რათა მათ გააქტიურონ უკან დახევის ალგორითმი. ეს ალგორითმი გამოიწვევს ყველა მოწყობილობის გაგზავნის შეჩერებას შემთხვევითი დროით, რაც კოლიზიურ სიგნალებს ჩაცხრომის საშუალებას მისცემს. დროის გავლის შემდეგომ მოწყობილობა გადავა „მოსმენა გაგზავნამდე“ მდგომარეობაში. შემთხვევითი დრო გვეხმარება იმაში, რომ გამოვრიცხოთ

განმეორებითი კოლიზია იმ მოწყობილობების მერ, რომლებიც იყვნენ ჩართულნი კოლიზიაში. თუმცა ეს ასევე ნიშნავს რომ გადაცემა შეიძლება დაიწყოს სხვა მოწყობილობამ უფრო ადრე ვიდრე ამას შეძლებენ კოლიზიაში ჩართული მოწყობილობები.

კონცენტრატორები და კოლიზიური დომეინები

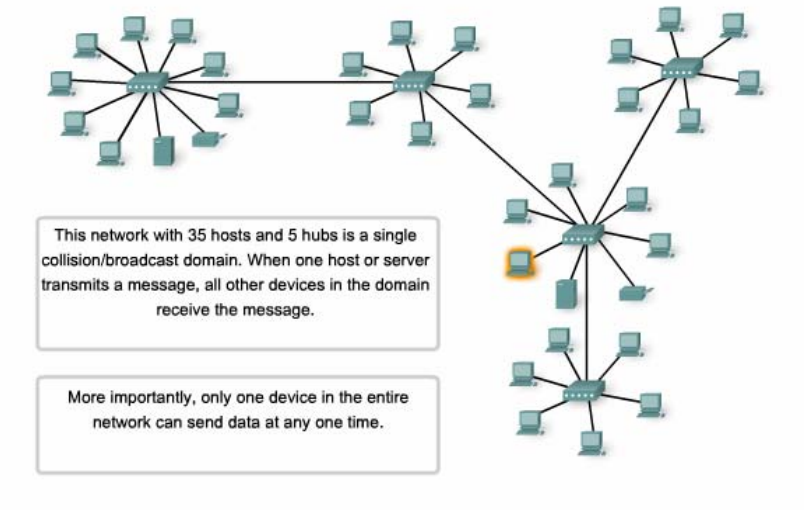
იმის გამო რომ კოლიზიები, როგორც წესი ხდება ნებისმიერ საერთო გამტარულ ტოპოლოგიაზე, ისევე როდესაც გამოიყენება CSMA/CD მეთოდი, ამიტომ ჩვენ უნდა დავაკვირდეთ პირობებს რომელთა დროსაც შესაძლებელია მოიმატოს კოლიზიების რაოდენობამ. ინტერნეტის სწრაფი გაზრდის გამო:

1. ქსელში უფრო მეტი მოწყობილობა ერთვება;
2. მოწყობილობები უფრო ხშირად უკავშირდებიან მოწყობილობებს;
3. მოწყობილობათა შორის მანძილი იზრდება;

კონცენტრატორები იყო შექმნილი როგორც საშუამავლო მოწყობილობები, რომლებიც უფრო მეტ მოწყობილობას აძლევდნენ საშუალებას ჩართულიყვნენ ქსელში. ისინი ასევე ცნობილი არიან როგორც მრავალპროტიანი გამმეორებლები. კონცენტრატორები აგზავნიან მოსულ სიგნალს ყველა პორტში გარდა იმ პორტისა რომლიდანაც სიგნალი მოვიდა. კონცენტრატორები არ ასრულებენ ქსელურ ფუნქციებს, ისეთებს როგორიც არის მონაცემების გადამისამართება.

კონცენტრატორები და გამმეორებლები არიან მოწყობილობები რომლებიც აგრძელებენ დისტანციას, რომელზეც შესაძლებელია

Ethernet კაბელების გაყვანა. იმის გამო რომ კონცენტრატორები მოქმედებენ პირველ დონეზე და მუშაობენ მხოლოდ ელექტრულ სიგნალებთან, კოლიზიები შეიძლება მოხდეს მოწყობილობების შიგნით ან მატ შორის რომლებსაც ისინი აერთებენ .



ნახაზი 79. ჰაბის გამოყენება გაფართოებული ვარსკვლავური ტოპოლოგიის შემთხვევაში

კონცენტრატორების გამოყენება იმისთვის რომ გავზარდოთ მომხმარებლების რაოდენობა ქსელში, აუარესებს მომსახურეობას არსებული მომხმარებლებისთვის, იმიტომ რომ საერთო მედია რჩება უცვლელი.

მოწყობილობები, რომლებიც არიან დაკავშირებული კონცენტრატორების მეშვეობით საერთო გამტარზე, წარმოადგენენ კოლიზიურ დომეინს. მას ასევე ეძახიან ქსელის სეგმენტს. კონცენტრატორები და გამმეორებლები ზრდიან კოლიზიური

დომეინების ზომას. თუ გამოვიყენებთ გაფართოებული ვარსკვლავის ფიზიკურ ტოპოლოგიას კონცენტრატორების გამოყენებით, ჩვენ შევქმნით ძალიან დიდ კოლიზიურ დომეინს. კოლიზიების გაზრდილი რაოდენობა ძლიერ ამცირებს ქსელის ეფექტურობას.

იმის და მიუხედავათ, რომ CSMA/CD არის კადრების კოლიზიის მართვისთვის შექმნილი, ის იყო მცირე რაოდენობით მოწყობილობისთვის და დაბალი დატვირთვის ქსელებისთვის შექმნილი. ამიტომ ხდება საჭირო მოინახოს სხვა გზა, რათა მოხდეს დიდი რაოდენობით მოწყობილობის ჩართვა ქსელში და უფრო დიდი დატვირთვის ქსელის ოპერირება.

Ethernet-ის დროითი პარამეტრები

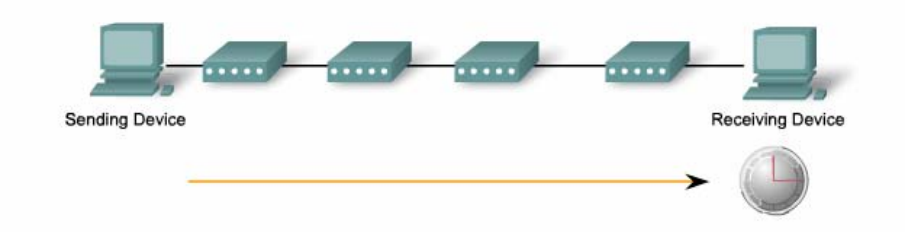
დაყოვნება (Latency)

კოლიზიების მართვაში უფრო სწრაფი ფიზიკური დონის გამოყენებას შემოაქვს უფრო მეტი სირთულე.

როგორც ვთქვით, თითოეული მოწყობილობა რომელსაც სურს მონაცემის გადაცემა, უნდა ჩაირთოს სმენის რეჟიმში, რათა შეამოწმოს ტრაფიკი ქსელში. თუ ტრაფიკი არ არსებობს, მაშინ მოწყობილობა იწყებს გადაცემას. ელექტრული სიგნალის გადაცემას მიაქვს გარკვეული დრო (დაყოვნება). თითოეული კონცენტრატორი ან გამმეორებელი სიგნალის გზაზე ზრდის ამ დაყოვნებას და ეს ზრდის კოლიზიების რაოდენობას.

ეს დაყოვნენები იწვევს კოლიზიების მოხდენის შესაძლებლობას რადგანაც, თუ სიგნალი რომელიც გადაცემული იყო ერთი მოწყობილობის მიერ და მუშავდებოდა კონცენტრატორში ან

გამმეორებელში, იმ მომენტში მეორე მოწყობილობას რომელსაც ასევე უნდა ინფორმაციის გადაცემა, მოუსმენს ქსელს. რადგანაც სიგნალს ამ მოწყობილობამდე ჯერაც არ მოუღწევია ის ჩათვლის რომ ქსელი თავისუფალია და დაიწყებს გადაცემას. შედეგად მივიღებთ კოლიზიას.



ნახაზი 80. სიგნალის დაყოვნება Ethernet-ში

დრო და სინქრონიზაცია (Timing and Synchronization)

თუ ნახევარ-დუპლექსურ რეჟიმში არ მოხდა კოლიზია, მოწყობილობა აგზავნის დროის სინქრონიზაციითვის 64 ბიტ ინფორმაციას, რომელსაც ეწოდება პრეამბულა და შემდგომ გააგზავნის მთლიან ფრეიმს.

Ethernet 10მბ/წმ სიჩქარით და უფრო ნელი არის ასინქრონული. ასინქრონული კომუნიკაცია ნიშნავს, რომ თითოეული მიმღები მოწყობილობა იყენებს 8 ბაიტიან დროით ინფორმაციას სინქრონიზაციისათვის, რომელიც გამოიყენება მიმღები მოწყობილობის მიერ ახის და ადაპტერის სინქრონიზაციისთვის, შემდგომ აგდებს ამ 8 ბაიტს.

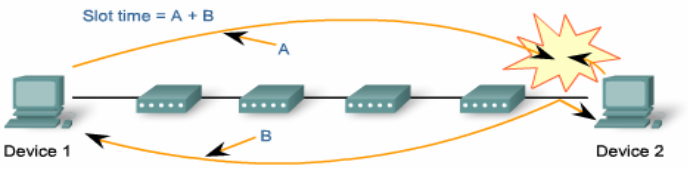
Ethernet იმპლემენტაცია სიჩქარით 100მბ/წმ და უფრო სწრაფი არის სინქრონული. ამ დროს დროითი ინფორმაცია არ არის

საჭირო, თუმცა თავსებადობის მიზნით პრეამბულა და ფრეიმის საწყისი მსაზღვრელი მაინც არის კადრში.

ბიტ დრო (Bit Time)

ყველა სხვადასხვა მედია სიჩქარისთვის, დროის მონაკვეთი საჭიროა იმისათვის, რომ მოხდეს ბიტის დასმა გამტარზე. ამ პერიოდს ეწოდება ბიტ დრო. 10მბ/წმ. Ethernet-ში ერთი ბიტ დრო წარმოადგენს 100 ნანოწამს, ხოლო 100მბიტ/წამზე Ethernet-ში 10 ნანოწამს, 1გიგაბიტ/წმ. Ethernet 1 ნანოწამს. მიახლოებით 20.3 სანტიმეტრის მანძილის გასავლელად UTP კაბელზე საჭიროა 1 ნანოწამი, ამის შედეგად 100 მეტრის კაბელზე მანძილის გასავლელად დაგვჭირდება 5 ბიტ დრო 10BASE-T სიგნალისთვის.

CSMA/CD რომ იმუშაოს Ethernet-ში, გამგზავნმა მოწყობილობამ, უნდა შეძლოს შეიტყოს კოლიზიის შესახებ ინფორმაცია, სანამ დაამთავრებს მინიმალური ზომის ფრეიმის გადაცემას. 100მბიტ/წამის სიჩქარის დროს ძლივს ხერხდება ეს 100 მეტრიან კაბელზე, ხოლო 1გბ Ethernet, განსაკუთრებული მორგება არის საჭირო იმიტომ, რომ თითქმის მთლიანი მინიმალური ფრეიმი იქნება გადაცემული უფრო ადრე ვიდრე პირველი ბიტი მიაღწევდა 100 მეტრის ბოლოს UTP კაბელში, ამ მიზეზის გამო 10გბ Ethernet-ში ნახევარ-დუპლექსური რეჟიმი არ არის დაშვებული.



Speed	Slot Time	Time Interval
10 Mbps	512 bit time	51.2 µs
100 Mbps	512 bit time	5.12 µs
1 Gbps	4096 bit time	4.096 µs
10 Gbps	not applicable	not applicable

Ethernet Speed	Bit time
10 Mbps	100 ns
100 Mbps	10 ns
1000 Mbps = 1 Gbps	1 ns
10,000 Mbps = 10 Gbps	.1 ns

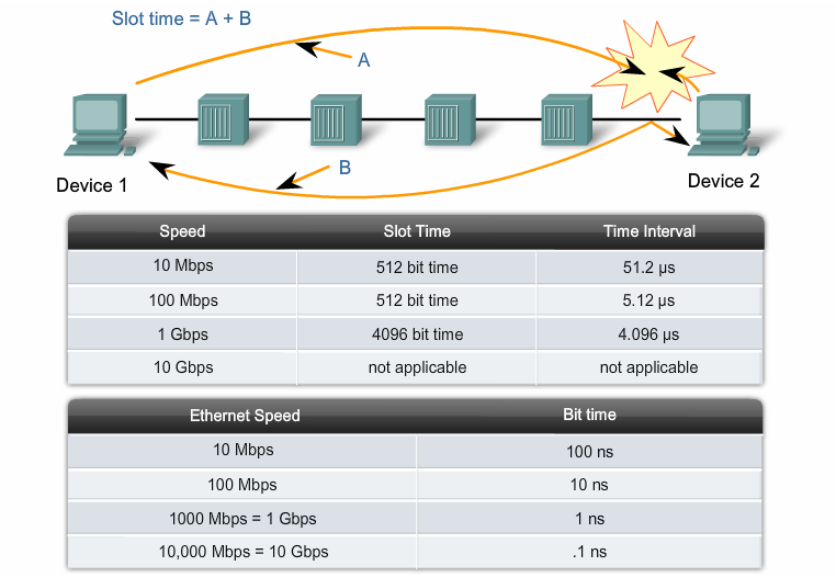
ნახაზი 81. Ethernet-ის ბიტ და სლოტის დრო

სწორედ ეს ბიტ დრო არის გამოყენებული კადრთაშორის დაშორებაში და უკანდახევის ალგორითმის დროს, იმისთვის რომ მინიმუმამდე დავიყვანოთ განმეორებითი კოლიზიის რისკი, როდესაც მოწყობილობა გადასცემს ფერიმს თავიდან.

სლოტის დრო

ნახევარ-დუპლექსურ Ethernet-ში, სადაც მონაცემებს დროის ერთ მომენტში შეუძლიათ მოგზაურობა მხოლოდ ერთ მიმართულებით, სლოტის დრო ხდება მნიშვნელოვანი პარამეტრი იმის დასადგენად თუ რამდენ მოწყობილობას შეუძლია გაინაწილოს ქსელი. ყველა სიჩქარის Ethernet-ისთვის არაუმეტეს 1გიგაბიტ/წამისა. სტანდარტი აღწერს რომ ინდივიდუალური გადაცემა არ შეიძლება იყოს უფრო დაბალი, ვიდრე სლოტის დრო.

სლოტის დროის განსაზღვრა, არის არჩევანი კოლიზიების შედეგების შემცირების საჭიროებისა და საშუალო ქსელის ზომის დასაკმაყოფილებლად, მანძილის გაზრდის საჭიროებას შორის. კომპრომისის შედეგად მიღწეულ იქნა შეთანხმება და მაქსიმალური ქსელის დიამეტრი გახდა 2500 მეტრი. ამის შემდეგ დადგინდა ფრეიმის მინიმალური ზომა რათა მოხდეს კოლიზიების აღმოჩენა ყველაზე უშორეს მანძილზეც.



Speed	Slot Time	Time Interval
10 Mbps	512 bit time	51.2 µs
100 Mbps	512 bit time	5.12 µs
1 Gbps	4096 bit time	4.096 µs
10 Gbps	not applicable	not applicable

Ethernet Speed	Bit time
10 Mbps	100 ns
100 Mbps	10 ns
1000 Mbps = 1 Gbps	1 ns
10,000 Mbps = 10 Gbps	.1 ns

ნახაზი 82. Ethernet-ის სლოტის და ბიტ დრო

სლოტის დრო 10 და 100 მბიტ/წამი Ethernet-ში არის 512ბიტი/დრო ან 64 ოქტეტი. სლოტ ტაიმი 1გიგაბიტიანი Ethernet-ისთვის არის 4096 ბიტ/დრო ან 512 ოქტეტი. სლოტის დრო არის მნიშვნელოვანი პარამეტრი შემდგომი მიზეზების გამო:

- 512 ბიტი სლოტის დრო უზრუნველყოფს მინიმალური Ethernet ფრეიმის, რომლის ზომაც არის 64 ბაიტი სარწმუნო გადაცემას უშორეს წერთილში. 64 ბაიტზე ნაკლები ნებისმიერი ფრეიმი ჩაითვლება როგორც კოლიზიის ფრაგმენტი და ავტომატიურად გადაგდებული იქნება მიმღების მიერ.

- სლოტის დრომ წარმოქმნა ქსელის სეგმენტის ზომის მაქსიმალური ზღვარი. თუ ქსელი დიამეტრი ძალიან გაიზრდება, შეიძლება წარმოიქმნას დაგვიანებული კოლიზიები და ისინი წარმოქმნიან მტყუნებას, რადგანაც მოწყობილობა რომელიც გადასცემს მინიმალური ზომის ფრეიმს, 512 ბიტი სლოტის დროის გავლის შემთხვევაში ამთავრებს ფრეიმის გადაცემას, ხოლო გადაცემულ ფრეიმს თვლის წარმატებულად. თუ ქსელის დიამეტრი უფრო დიდია ვიიდრე სლოტის დრო და ამ სლოტის დროის შემდგომ აღმოჩნდა კოლიზია, CSMA/CD ვერ მართავს ავტომატიურად ამ პროცეს, რაც საბოლოო ჯამში იწვევს მტქუნებას ანუ შეცდომებს .

სლოტის დრო გამოითვლება ქსელის დიამეტრის მაქსიმალური შესაძლო ზომით, რომელიც დაშვებულია ქსელური არქიტექტურიდან გამომდინარე.

იმისათვის, რომ სისტემამ სწორად იმუშაოს, როგორც ზემოთ ავღნიშნეთ, პირველმა მოწყობილობამ უნდა შეიტყოს კოლიზიის შესახებ მანამ, სანამ ის დაამთავრებს თავისი უმცირესი სტანდარტული ფრეიმის გაგზავნას.

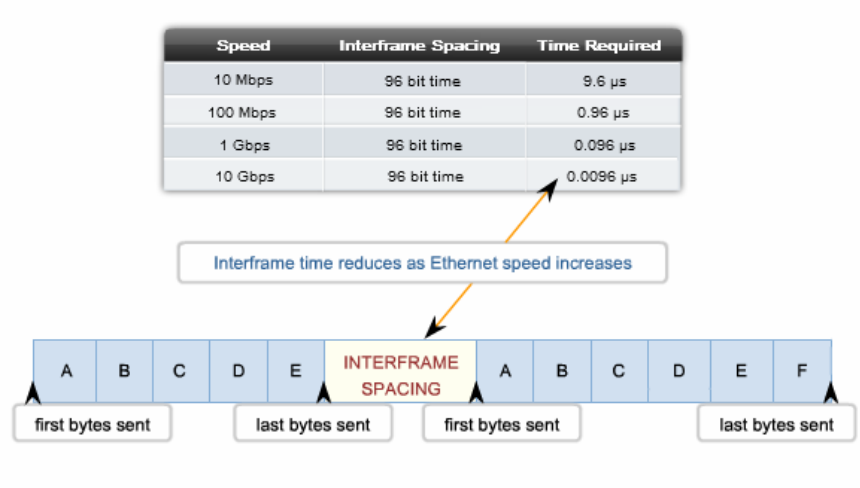
იმისათვის რომ 1გბ Ethernet-ს მიეცეს საშუალება იმუშაოს ნახევარ-დუპლექსურ რეჟიმში, გამოყენებულ იქნა

დამაგრძელებელი ველი და ის დამატებული იქნა კადრში. როდესაც იგზავნება მინიმალური ზომის ფრეიმი, ბიტები გადაცემა მანამდე არ უნდა შეწყდეს , სანამ უშორეს წერტილში მომხდარი კოლიზიის შესახებ არ გაიგებს გადამცემი. ეს ველი არის მხოლოდ ნახევარ-დეუპლქსურ 1გბ Ethernet-ში და ნებას რთავს მინიმალური ზომის კადრებს იმდენხანს "იცოცხლონ" რომ დაექვემდებარონ სლოტის დროს. დამამმაგრძელებელი ბიტები გადაგდებულნი იქნება მიმღები მხრის მიერ.

<u>კადრთაშორისი დაცილება (Interframe Spacing)</u>

Ethernet სტანდარტებს ესაჭიროებათ მინიმალური დაცილება ორ არაკოლიზიურ ფრეიმს შორის. ეს გამტარს აძლევს დროს, რათა დასტაბილურდეს გადაცემის შემდეგ, მიღებს- დროს, ფრეიმების დასამუშავებლად. ამას ეწოდება კადრთაშორისი დაცილება. ის იზომება შესამოწმებელი (FCS) ველის ბოლო ბიტიდან ახალი ფრეიმის პრეამბულის პირველ ბიტამდე.

ფრეიმის გაგზავნის შემდგომ, 10მბტ/წმ Ethernet-ში, ყველა მოწყობილობა ვალდებულია დაიცადოს 96ბიტ/დრო, ეს საშუალებას აძლევს სხვა მოწყობილობა დაიწყოს ან განაახლოს გადაცემა. Ethernet-ის უფრო სწრაფ ვერსიებში, ეს დაყოვნება რჩება იგივე 96ბიტ/დრო, თუმცა დრო მცირდება. (რაც უფრო სწრაფია Ethernet მით უფრო მოკლეა ბიტ/დრო ნელთან შედარებით).



ნახაზი 83. კადრთაშორისი დაცილება

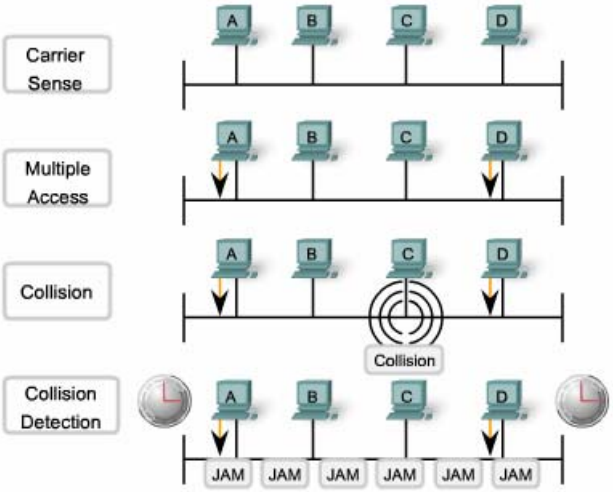
სინქრონიზაციის შეყოვნება მოწყობილობებს შორის შეიძლება გამოიწვეული იყოს ფრეიმის პრეამბულის რამდენიმე ბიტის დაკარგვით, ეს იწვევს პატარა ცვლილებას კადრთაშორის დაცილებაში, როდესაც კონცენტრატორები და გამმეორებლები რეგენერაციას უკეთებენ თითოეული ფრეიმის დასაწყისში დროით ინფორმაციას (პრეამბულას, ფრეიმის მსაზღვრელს) სრულ 64 ბიტს. სწრაფ Ethernet-ში ზოგიერთმა დროზე დამოკიდებულმა მოწყობილობამ შეიძლება უარი განაცხადოს ფრეიმის მიღებაზე, რაც გამოიწვევს შეფერხებას კავშირგაბმულობაში.

ჩამხშობი სიგნალი (Jam Signal)

Ethernet ნებას რთავს მოწყობილობებს ერთმანეთს შეეჯიბრონ გადაცემის დაწყებაზე, თუ დროს ერთ მომენტში ერთდროულად მოხდება ორი მოწყობილობის მიერ გადაცემა, ქსელის CSMA/CD შეეცდება გამოასწოროს პრობლემა. თუმცა გახსოვთ ალბათ, რომ

მოწყობილობების რაოდენობის ზრდასთან ერთად წარმოქმნილი კოლიზიები შესაძლებელია გახდეს ძალიან რთულად გასასწორებელი.

კოლიზიის აღმოჩენისთანავე გადამცემი მოწყობილოა გადასცემს 32 ბიტიან ჩამხშობ სიგნალს, რათა უზრუნველყოს ყველა მოწყობილობისთვის შეტყობინება კოლიზიის შესახებ. მნიშვნელოვანია, რომ ჩახშობის სიგნალი არ ჩაითვალოს როგორც მუშა ფრეიმი, თორემ ვერ მოხდება კოლიზიის აღმოჩენა. ყველაზე გავრცელებული ჩამხშობი სიგნალი არის უბრალოდ 1,0,1,0... როგორც პრეამბულა. დამახინჯებულ მონაცემებს ხშირად უწოდებენ კოლიზიის ფრაგმენტებს. ნორმალური კოლიზიები 64 ოქტეტზე მოკლეა, რის შედეგადაც ადვილია მათი ამოცნობა, რადგან ისინი არ აკმაყოფილებენ მინიმალურ ზომას და შესამოწმებელ (FCS) ტესტს.

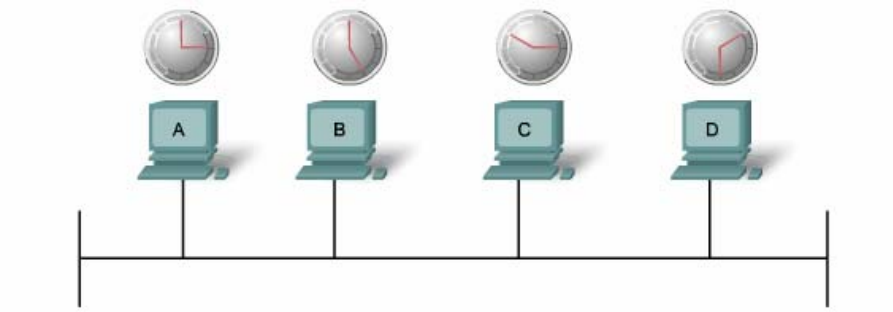


ნახაზი 84. კოლიზია და ჩამხშობი სიგნალი

უკან დახევის დრო (Backoff Timing)

მას შემდეგ, რაც მოხდება კოლიზია, ყველა მოწყობილობა იცდის სრული კადრთაშორისი დაცილების დროით(96 ბიტ/დრო), ხოლო ის მოწყობილობები რომელთა გამოც მოხდა კოლიზია დამატებით იცდიან შემთხვევით დროის განმავლობაში. ეს დრო შემთხვევითია, იმიტომ რომ, მათ არ დაიწყონ გადაცემა ისევ ერთდროულად, რაც გამოიწვევდა კიდევ მეტ კოლიზიას. ეს მიიღწევა ნაწილობრივ იმით, რომ ხდება ინტერვალის გაზრდა, რომლიდანაც ხდება შემთხვევითი დროის ამორჩევა. ლოდინის დრო განისაზღვრება სლოტის დროის პარამეტრებით.

იმ შემთხვევაში, როდესაც ვერ გაიგზავნება ფრეიმი ზედიზედ 16-ჯერ, მოხდება შეცდომის შეტყობინება ქსელური დონისთვის. ასეთი რამ იშვიათობაა სწორად გამართულ ქსელში, და უფრო ხშირია, როდესაც არის ფიზიკურ დონეზე დაზიანება. ამ მეთოდმა დართო ნება Ethernet-ს უკეთესი მომსახურება გაეწია განაწილებული მედიის ტოპოლოგიაში რომლებიც დამყარებული იყო კონცენტრატორებზე. სვიჩების შემოსვლასთან ერთად CSMA/CD-სადმი მოთხოვნილებამ იკლო და ზოგიერთ ვარიანტში, საერთოდაც ამოღებულ იქნა.



ნახაზი 85. უკან დახევის დრო

განსხვავებები Ethernet სტანდარტებს შორის, არის ფიზიკურ დონეზე. Ethernet არის აღწერილი IEEE 802.3 სტანდარტებში. ამჟამად აღწერილია 4 მონაცემთა გამტაროობა ოპტიკურ-ბოჭკოვანი და ხვეული წყვილის კაბელებში:

- 10 მბ/წმ -10Base-T Ethernet;
- 100 მბ/წმ - ჩქარი Ethernet;
- 1000 მბ/წმ – გიგაბიტ Ethernet;
- 10 გბ/წმ – 10 გიგაბიტ Ethernet.

Ethernet Type	Bandwidth	Cable Type	Duplex	Maximum Distance
10Base-5	10 Mbps	Thicknet Coaxial	Half	500 m
10Base-2	10 Mbps	Thinnet Coaxial	Half	185 m
100Base-TX	10 Mbps	Cat3/Cat5 UTP	Half	100 m
100Base-TX	100 Mbps	Cat5 UTP	Half	100 m
100Base-FX	200 Mbps	Cat5 UTP	Full	100 m
100Base-FX	100 Mbps	Multimode Fiber	Half	400 m
1000Base-T	200 Mbps	Multimode Fiber	Full	2 km
1000Base-TX	1 Gbps	Cat5e UTP	Full	100 m
1000Base-SX	1 Gbps	Cat6 UTP	Full	100 m
1000Base-LX	1 Gbps	Multimode Fiber	Full	550 m
10GBase-CX4	1 Gbps	Single-Mode Fiber	Full	2 km
10GBase-T	10 Gbps	Twin-axial	Full	100 m
10GBase-LX4	10 Gbps	Cat6a/Cat7 UTP	Full	100 m
10GBase-LX4	10 Gbps	Multimode Fiber	Full	300 m
10 Mbps	10 Gbps	Single-Mode Fiber	Full	10 km

ნახაზი 86. Ethernet-ის ტიპები

<u>10 მბ/წმ Ethernet ოჯახებს:</u>

10BASE5 Thicknet - კოაქსიალური კაბელს.

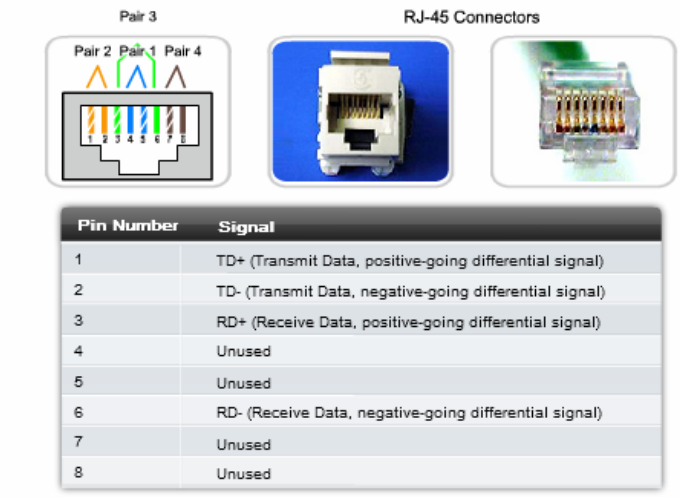
10BASE2 Thinnet - კოაქსიალური კაბელს.

10BASE-T Cat3/Cat5 - არაეკრანირებული ხვეული წყვილის კაბელს.

Ethernet ადრინდელ ვარიანტებში ფიზიკური სალტის შესაქმნელად 10BASE5 და 10BASE2-ში გამოიყენებოდა კოაქსიალური კაბელი, თუმცა ეს ვარიანტები აღარ გამოიყენება და არ არის მხარდაჭერილი ახალ 802.3 სტანდარტში.

10 მბ/წმ Ethernet - 10BASE-T

10BASE-T იყენებს მანჩესტერის კოდირებას ორ არაეკრანირებულ გრეხილ წყვილზე. ადრინდელ ვარიანტებში 10BASE-T-ში გამოიყენებოდა Cat3 კაბელი, თუმცა დღესდღეობით გამოიყენება მხოლოდ Cat5 ან უფრო ახალი ტიპის კაბელები. 10მბ/წმ Ethernet ითვლება კლასიკურ Ethernet-ად და გამოიყენებს ვარსკვლავის ფიზიკურ ტოპოლოგიას. Ethernet 10BASE-T კაბელები შეიძლება იყვნენ 100 მეტრამდე სიგრძეში სანამ მათ დასჭირდებათ კონცენტრატორი ან გამმეორებელი. 10BASE-T იყენებს ოთხწყვილიანი კაბელის ორ წყვილს და ბოლოვდება 8 გასართიანი RG-45 კონექტორით. წყვილები შეერთებულები პირველ და მეორე გასართთან გამოიყენება ინფორმაციის გასაგზავნად, ხოლო 3 და 6 გამოიყენება ინფორმაციის მისაღებად.



Pin Number	Signal
1	TD+ (Transmit Data, positive-going differential signal)
2	TD- (Transmit Data, negative-going differential signal)
3	RD+ (Receive Data, positive-going differential signal)
4	Unused
5	Unused
6	RD- (Receive Data, negative-going differential signal)
7	Unused
8	Unused

ნახაზი 87. RG-45 კონექტორი და კაბელის კონექტორზე მიერთების სქემა

ახალი ქსელის შექმნისას 10BASE-T-ს აღარავინ ირჩევს, თუმცა ჯერჯერობით არსებობს ბევრი ქსელი აგებული მის მეშვეობით. კონცენტრატორების სვიჩებით გამოცვლამ ძალიან გაზარდა ამ ქსელებისა გამტარობა და გაუხანგძლივა მას სიცოცხლე. სვიჩთან შეერთებულ კაბელებს აქვთ მხარდაჭერა, როგორც ნახევარ-დუპლექსის ასევე სრული-დუპლექსისაც.

Fast Ethernet-100 მბიტ/წამში

20 საუკუნის შუა 90-იან წლებში რამდენიმე ახალი 802.3 სტანდარტი იქნა ჩამოყალიბებული 100მბიტ/წამში სიჩქარით ინფორმაციის გადასაცემად. ეს სტანდარტები იყენებენ განსხვავებულ კოდირებას, რათა მიაღწიონ გაზრდილ გამტარუნარიანობას. ამ Ethernet გამართვა შეგვიძლია გრეხილი

წყვილის კაბელის მეშვეობით ან ოპტიკურ-ბოჭკოვანი გამტარით. ყველაზე გავრცელებული ვარიანტებია:

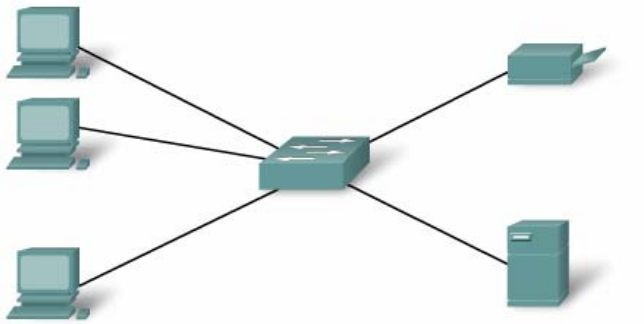
100BASE-TX - Cat5 კაბელის გამოყენებით;

100BASE-FX - ოპტიკურ ბოჭკოვან კაბელის გამოყენებით.

იმის გამო რომ უფრო მაღალი სიხშირის სიგნალები გამოიყენება Fast Ethernet -ში, ის უფრო მეტად ზიანდება ხარვეზებისგან, სიგნალის სრულფასოვნების გასამუჯობესებლად გამოიყენება ორი განცალკევებული კოდირების სისტემა.

100BASE-TX

იგი შემუშავებული იქნა მეხუთე კატეგორიის UTP კაბელზე გადაცემის მხარდასაჭერად. ის იმავე ორ წყვილის იყენებს და ისეთივე გასართი აქვს როგორც 10BASE-T-ს, თუმცა მას ესაჭიროება მე-5 კატეგორიის ან უფრო ახალი UTP კაბელი. 100BASE-TX Ethernet-სთვის გამოიყენება 4B/5B კოდირება. ის ისევე როგორც 10BASE-TX მოწყობილობებს აკავშირებს ფიზიკური ვარსკვლავის ტოპოლოგიით, თუმცა 10BASE-T-გან განსხვავებით ჩვეულებრივ აქ კონცენტრატორის მაგივრად გამოიყენება სვიჩი. 100BASE-TX ტექნოლოგია და სვიჩები ერთდროულად გახდნენ გავრცელებულნი, და ამან გამოიწვია მათი ბუნებრივი შერწყმა 100BASE-TX ქსელებში.



ნახაზი 88. ვარსკვლავის ტოპოლოგია 10BASE-TX Ethernet გამოყენებით

100BASE-FX

ეს ტექნოლოგია იყენებს სიგნალების გადაცემის იგივე ხერხს როგორსაც 100BASE-TX, თუმცა მისგან განსხვავებით აქ გამოიყენება ოპტიკურ-ბოჭკოვანი გამტარი. კოდირებაის და დეკოდირების პროცედურები ერთნაირია ორივე ტექნოლოგიაში, თუმცა სიგნალის გადაცემა 100BASE-TX-ში ხდება ელექტრული იმპულსების გამოყენებით, ხოლო 100BASE-FX სინათლის იმპულსებით. 100BASE-FX იყენებს ეგრეთ წოდებულ დუპლექსურ SC კონექტორებს.

Gigabit Ethernet -1000მბ/წმ

გიგაბიტ Ethernet შექმნა გარკვეულ წილად განაპირობა, ერთმოდიანი და მრავალმოდიანი ოპტიკური სადენის, UTP სადენის შესაძლებლობებმა. გიგაბიტ Ethernet ქსელებში, ბიტები წარმოიქმნება გაცილებით სწრაფად, ვიდრე რომელიც საჭიროა 100 მბ/წ და 10მბ/წ Ethernet-ში. სიგნალების უფრო მოკლე დროში

გაჩენის გამო, ბიტები უფრო მგრძნობიარე ხდებიან ხარვეზების მიმართ. შესაბამისად, სინქრონულობა კრიტიკულია. შესრულება დამოკიდებულია იმაზე, თუ რამდენად სწრაფად შეუძლია ქსელის ადაპტერს შეცვალოს ვოლტაჟის დონეები და რამდენად კარგად შეიძლება ამ ვოლტაჟის ცვლილების აღმოჩენა მიმღებ ქსელის ადაპტერზე ან ინტერფეისზე 100 მეტრის მანძილზე.

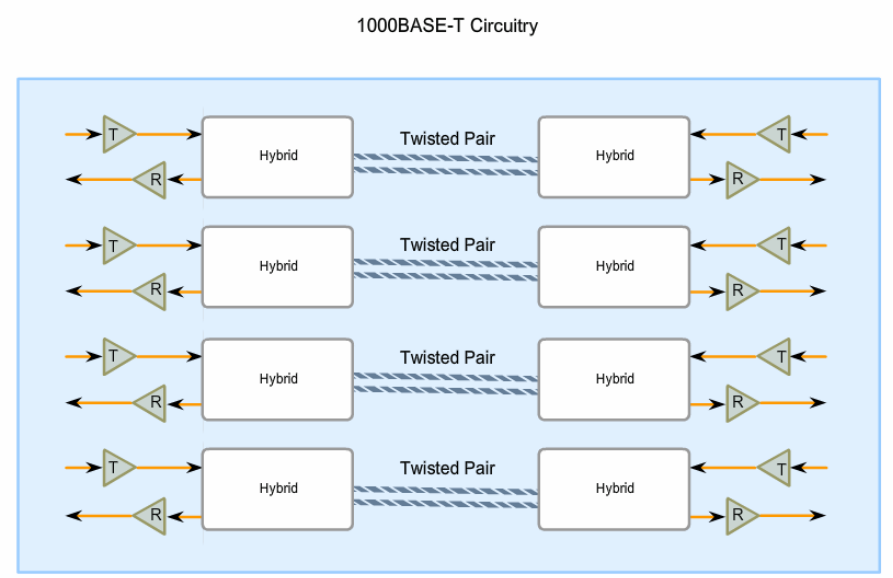
ასეთ მაღალ სიჩქარეებზე, მონაცემების კოდირება და დეკოდირება უფრო კომპლექსურია. გიგაბიტ Ethernet-ში გამოიყნება ორი განცალკევებული კოდირების საფეხური. მონაცემთა გადაცემა უფრო ეფექტურია, როდესაც კოდები გამოიყენება ორობითი ნაკადის აღნიშვნისთვის. კოდირებული მონაცემები იძლევა სინქრონიზაციის უფლებას და გამტარუნარიანობის უფრო ეფექტურად გამოყენების საშუალებას და გაუმჯობესებულ მოთმინების უნარს ხარვეზებისადმი.

1000BASE-T Ethernet

იგი უზრუნველყოფს კატეგორია 5 ან უფრო ახალი კაბელით და ოთხივე წყვილის გამოყენებით სრულ-დუპლექსურ გადაცემას. გიგაბიტ Ethernet თითოეული წყვილზე იძლევა 125მბიტ/წამამდე სიჩქარეს, ოთხივე წყვილზე 500მბიტ/წამამდე სიჩქარეს.. თითოეული წყვილი მუშაობს სრულ-დუპლექსურ რეჟიმში და

აორმაგებს 500მბიტ/წამს 1000მბიტ/წამამდე. 1000BASE-T იყენებს 4D-PAM5 კოდირებას, რათა მიიღოს 1გიგაბიტ/წამში გამტარუნარიანობა. ეს კოდირების სქემა იძლევა სიგნალის ოთხივე წყვილზე ერთდროულად გადაცემის საშუალებას. ის 8-ბიტიან ბაიტს გარდაქმნის ოთხივე წყვილში ერთდროულად გადაცემად კოდურ სიმბოლოდ(4D), რომლებიც იგზავნებიან გამტარის თითოეულ წყვილზე, ისევე როგორც PAM5-ის (5-level

Pulse Amplitude Modulated PAM5)შემთხვევაში.ეს იმას ნიშნავს, რომ თითოეული სიმბოლო აღნიშნავს ორ ბიტ ინფორმაციას. იმის გამო რომ ინფორმაცია მოგზაურობს ერთდროულად 4 განსხვავებულ გზაზე(წყვილზე), უნდა მოხდეს კადრების დაყოფა გადამცემთან და შეერთება მიმღებთან. დაავირდით სურათს



ნახაზი 89. 1000BASE-T Ethernet

საშუალებას გვაძლევს გავაგზავნოთ და მივიღოთ ინფორმაცია ერთი და იგივე კაბელზე ერთდროულად. ეს ტრაფიკი მუდმივად იწვევს კოლიზიებს. კოლიზიების მიზეზი არის კომპლექსური ვოლტაჟის მიმდევრობები(ექო) რომელიც მოყვება გადაცემულ სიგნალს. მიმღები იყენებს გამოცდილ ხერხებს როგორიც არის ექოს გაუქმება, პირველი დონის გადაგზავნიის შეცდომის გამოსწორებას (FEC) და წინდახედულად ვოლტაჟის დონნების

არჩევას, ამ ხერხების გამოყენებით სისტემა აღწევს 1გიგაბიტ გამტარუნარიანობას.

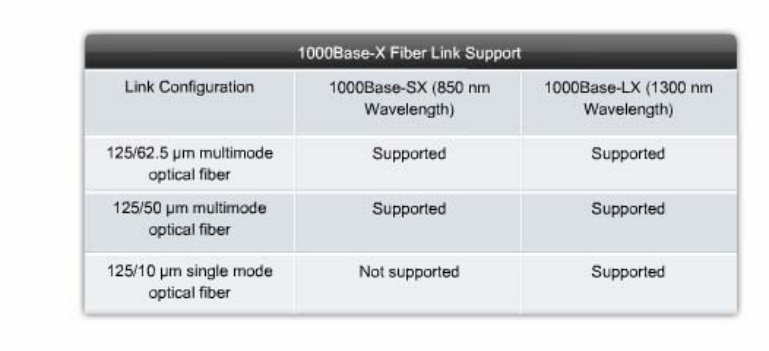
სინქრონიზაციის დასახმარებლად, ფიზიკური დონე ენკაპსულაციას უკეთებს თითოეულ ფრეიმს ნაკადის დამწყები და დამმამთავრებელი მსაზღვრელით.

განსხვავებით სხვა ციფრული აპარატურისგან, სადაც წყვილი როგორც წესი იყენებს დისკრეტულ ვოლტაჟს, 1000 BASE-T იყენებს მრავალ ვოლტაჟის დონეს, უმოქმედობის დროს კაბელში შესაძლებელია 9-მდე დონის ვოლტაჟის აღმოჩენა. მონაცემების გადაცემისას კი 17-მდე ვოლტაჟის დონის. ამდენი განსხვავებული მდგომარეობის გათვალისწინებით და ხარვეზებთან ერთად, სიგნალი უფრო გავს ანალოგურს ვიდრე ციფრულს და როგორც ანალოგური ის უფრო მგრძნობიარეა ხარვეზებზე.

1000BASE-SX და 1000BASE-LX

1000BASE-SX და 1000BASE-LX არის Ethernet-ის ოპტიკური ვერსია ამ გამტარს UTP-სგან განსხვავებით, აქვს შემდეგი უპირატესობები: იმუნიტეტი ხარვეზებზე, პატარა ფიზიკური ზომა, გადიდებული დისტანცია(რომელიც არ საჭიროებს გამმეორებლებს) და გამტარუნარიანობა. 1000BASE-SX და 1000BASE-LX ორივეს აქვს მხარდაჭერა სრულ-დუპლექსური ორობითი გადაცემის 1250 მბ/წმ, ერთ წყვილზე. კოდირება დაფუძნებულია 8B/10B კოდირების სქემაზე. თუმცა ამ კოდირების ზედნადებისგან სიჩქარე მაინც 1000მბიტ/წამია. თითოეული მონაცემთა ფრეიმი ენკაპსულირებულია ფიზიკურ დონეზე გადაცემამდე, არხის სინქრონიზაცია მიიღწევა კადრთაშორის დაცილების პერიოდში, უმოქმედობის კოდის ჯგუფების უწყვეტი

1000BASE-SX და 1000BASE-LX შორის პრინციპული განსხვავებები არის შემდეგ კომპონენტებში: არხის გამტარი, კონეკტორები, ოპტიკური სიგნალის ტალღის სიგრძე.



1000Base-X Fiber Link Support		
Link Configuration	1000Base-SX (850 nm Wavelength)	1000Base-LX (1300 nm Wavelength)
125/62.5 µm multimode optical fiber	Supported	Supported
125/50 µm multimode optical fiber	Supported	Supported
125/10 µm single mode optical fiber	Not supported	Supported

ნახაზი 90. 1000BASE-SX და 1000BASE-LX გამოყენებული ოპტიკური სადენები და ტალღის სიგრძეები

მომავალი Ethernet სიჩქარეები

IEEE 802.3ae სტანდარტი იყო ადაპტირებული 10გბიტ/წამში, სრულ-დუპლექსიანი გადაცემისთვის ოპტიკურ კაბელში. ეს სტანდარტი ძალიან გავს 802.3 სტანდარტს (Ethernet ორიგინალური სტანდარტი). 10გბიტიანი Ethernet ვითარდება არა მხოლოდ ლოკალურ ქსელებში გამოსაყენებლად, არამედ გლობალურ ქსელებშიც. იმის გამო რომ ფრეიმის ფორმატი და 10გბ Ethernet-ის მეორე დონის სპეციფიკაციები თავსებადია Ethernet-ის წინა სტანდარტებთან, მას შეუძლია უზრუნველყოს მეტი გამტარუნარიანობა უკვე არსებულ ქსელურ ინფრა-სტრუქტურაში.

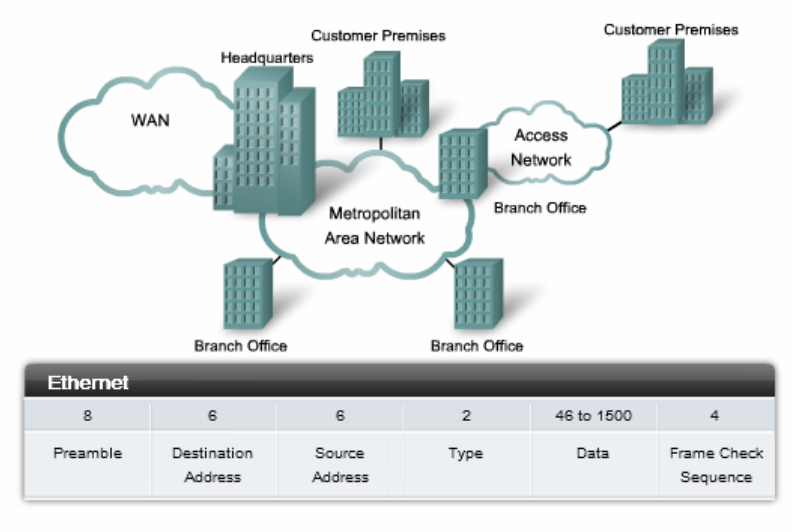
მისი შედარება სხვა Ethernet შეიძლება ესე:

- ფრეიმის ფორმატი იგივეა, კლასიკურ Ethernet-ში, Fast Ethernet-ში, გიგაბიტ Ethernet-ში და 10გიგაბიტიან Ethernet-ში. თავსებადობა შესაძლებელია, ფრეიმების და პროტოკოლების კონვერტაციის გარეშე.

- ბიტ დრო არის 0.1ნანოწამი.

- იმის გამო რომ მხოლოდ ოპტიკური გამტარი გამოიყენება, არ არის CSMA/CD გამოყენების საჭიროება

- პირველ და მეორე დონეებში 802.3 -ის ქვედონეები უმეტესად დაცულია, მხოლოდ რამდენიმე დანამატია გამოყენებული, 40 კილომეტრიანი ოპტიკური არხის მხარდაჭერისათვის და სხვა ოპტიკურ ტექნოლოგიებთან თავსებადობისათვის



ნახაზი 91. გბტ Ethernet ფრეიმის ფორმატი

1 გიგაბიტიანი Ethernet უკვე ფართოდა გავრცელებული და 10 გიგაბიტიანი Ethernet პროდუქციის აჩევანიც არის. მიმდინარეობს მუშაობა 40, 100 და 160გიგაბიტიან სტანდარტებზე. ტექნოლოგიების დანეგრვა დამოკიდებულია რამდენიმე ფაქტორზე, მათ შორის ტექნოლოგიის და სტანდარტების "დაღვინებაზე", ბაზარში მისი გავცელებაზე და პროდუქციის ფასზე.

Hub-ების გამოყენება

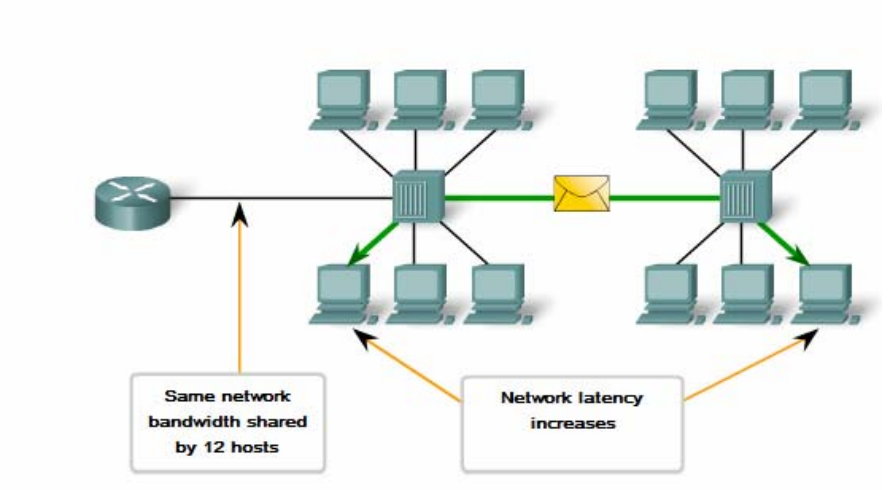
კონცენტრატორს იყენებს კლასიკური Ethernet, მოწყობილობების დასაკავშირებლად. ის არ ახდენს მონაცემების ფილტრაციას, ის უბრალოდ აგზავნის მიღებულ ბიტებს ყველა მოწყობილობაზე. ამის გამო ყველა მოწყობილობა ქსელში ინაწილებს გამტარუნარიანობას. დამატებით კლასიკური Ethernet გამოირჩევა მაღალი კოლიზიების რაოდენობით. ამ პრობლემებიდან გამომდინარე, მას შეზღუდული გამოყენება აქვს დღევანდელ ქსელებში. კონცენტრატორები გამოიყენებიან ან მარტო პატარა ქსელებში არამედ იმ ქსელებშიც, რომლებსაც დაბალი გამტარუნარიანობის მოთხოვნა აქვთ. ქსელის გაზრდასთან ერთად გამტარის განაწილება იწვევს დიდ პრობლემებს.

გაფართოებითობა

კონცენტრატორით აგებულ ქსელში არსებობს გარკვეული გამტარუნარიანობის ზღვარი, რომელის გამოიყენებაც შეუძლიათ ქსელში ჩართულ მოწყობილობებს. თითოეული ახალი მოწყობილობის დამატებასთან ერთად, საშუალო გამტარუნარიანობა რომელიც არის ხელმისაწვდომი თითოეული მოწყობილობისათვის მცირდება. თითოეული მოწყობილობის დამატებით ქსელში, მწარმოებლურობის ხარისხი მცირდება.

დაყოვნება

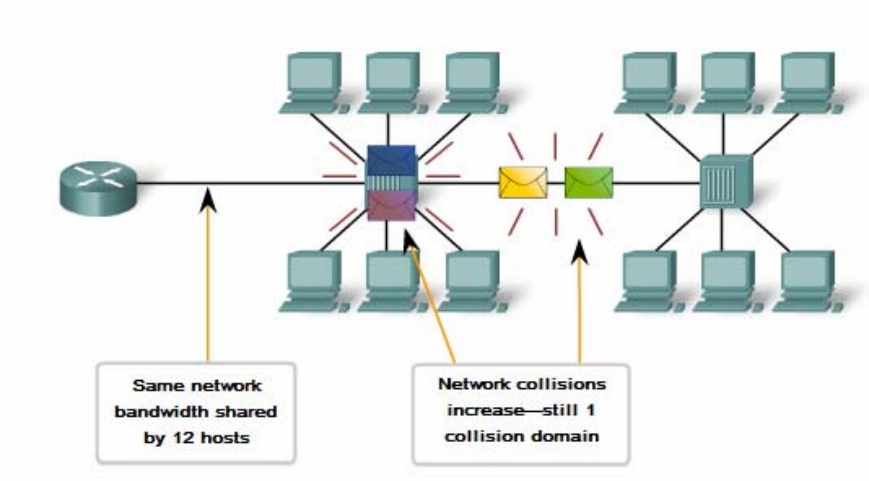
ქსელური დაყოვნება - ეს არის დრო, რომელიც სჭირდება სიგნალს, რომ გამტარით მიაღწიოს ყველა დანიშნულების ადგილას. თითოეულ მოწყობილობას უწევს ლოდინი . დაყოვნება შეიძლება ძლიერ გაიზარდოს, როცა მანძილი მოწყობილობებს შორის იზრდება. დაყოვნებაზე ასევე მოქმედებს გამტარზე სიგნალის დაყოვნება და დაყოვნება კონცენტრატორის ან გამმეორებლის გავლის დროს დამატებული გამოთვლითი ოპერაციებით. გამტარის სიგრძის მომატება, კონცენტრატორების ან გამმეორებლების რაოდენობის მომატება, იწვევს დაყოვნების მომატებას. რაც დიდია დაყოვნება მით დიდია კოლიზიის მოხდენის შანსი.



ნახაზი 92. ჰაბზე აგებული ლოკალური ქსელი ზრდის ქსელის დაყოვნებას

კოლიზიები

CSMA/CD-ს შესაბამისად, მოწყობილობამ არ უნდა გაგზავნოს პაკეტი თუ ქსელი თავისუფალი არ არის. თუ ორი მოწყობილობა ერთდროულად გააგზავნის პაკეტებს მოხდება კოლიზია და პაკეტები ზიანდება. შემდგომ ორივე მათგანი გააგზავნის ჩამხშობ სიგნალს, დაიცდის შემთხვევით დროის განმავლობაში და შემდგომ დაბრუნდებიან გაგზავნამდე მოსმენის რეჟიმში. ქსელის ნებისმიერი ნაწილი სადაც პაკეტებს შეუძლიათ ერთმანეთში შეჯახება კოლიზიური დომეინი ეწოდება. ქსელი რომელსაც ბევრი მოწყობილობა აქვს ერთ სეგმენტში, წარმოადგენს დიდ კოლიზიურ დომეინს და როგორც წესი გააჩნია მეტი ტრაფიკი. ტრაფიკის რაოდენობის გაზრდასთან ერთად იმატებს კოლიზიების რაოდენობაც. სვიჩები წარმოადგენენ Ethernet -ის კლასიკურ შეჯიბრზე დაფუძნებულ ალტერნატივას.

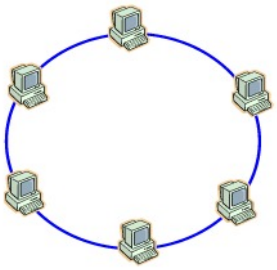


ნახაზი 93. ჰაბზე აგებული ლოკალური ქსელი ზრდის ქსელიში კოლიზიებს

ტექნოლოგია Token Ring

Token Ring-ის ქსელს, ისევე როგორც Etherne-ს, გააჩნია საერთო გარემო ინფორმაციის გადასაცემად, რომელიც შედგება სადენების მონაკვეთებისაგან, რომლებიც აერთიანებს ჰოსტებს წრიულ ქსელში.

წრე განიხილება როგორც საერთო გაყოფადი რესურსი და ამ რესურსში შესაღწევად გამოიყენება განსაზღვრული ალგორითმი, რომელიც განსხვავდება Ethernet-ში გამოყენებული ალგორითმისგან. ეს არის დეტერმინირებული წესი, და მის მიხედვით ხდება გარემოში შეღწევა. ეს უფლება გადაიცემა სპეციალური ფრეიმის მიერ, რომელსაც მარკერს უწოდებენ.

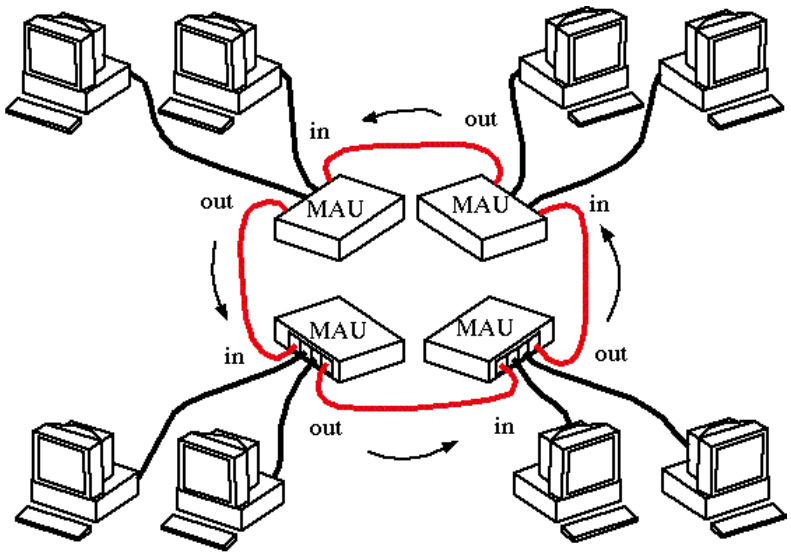


ნახაზი 94. ტოპოლოგია წრე

მარკერი დარბის წრეში განსაზღვრული მიმართულებით. ის მიდის წრეში ჩართულ ჰოსტებთან თანმიმდევრობით. თუ რომელიმე ჰოსტს აქვს ინფორმაცია გადასაცემი ის ჩაიბამს ამ ინფორმაციას და გადააქვს წრეში.

ტექნოლოგია Token Ring შეიქმნა კომპანია IBM-ის მიერ. ეს კომპანია იყენებს ამ ტექნოლოგიას ძირითადად ლოკალური ქსელების ასაგებად.

Token Ring-ის ქსელი მუშაობს ორ ბიტურ სიჩქარეზე - 4 და 16მბ/წმ. ერთ წრეში სხვადასხვა სიჩქარით ჰოსტების მუშაობა დაუშვებელია.



ნახაზი 95. Token Ring-ით აგებული ლოკალური ქსელი

ტექნოლოგია Token Ring წარმოადგენს უფრო რთულ ტექნოლოგიას Ethernet-თან შედარებით. ის ხასიათდება საიმედოობით. ქსელის კონტროლისათვის ერთი ჰოსტი ასრულებს *აქტიური მონიტორის* როლს.

აქტიური მონიტორი ირჩევა ქსელის ინიციალიზაიის დროს. ის ჰოსტი, რომელსაც გააჩნია ყველაზე დიდი MAC მისამართი ხდება

აქტიური მონიტორი. თუ აქტიური მონიტორი გამოდის წყობიდან, ქსელის ინიციალიზაციის პროცედურა იწყება თავდიან და ირჩევა აქტიური მონიტორი. აქტიური მონიტორის მთავარი ფუნქციაა აკონტროლოს მარკერის მუშაობა. თუ მარკერი დაზიანდა ან დაიკარგა მან უნდა უზრუნველყოს ახალი მარკერის გამომუშავება.

მარკეული მეთოდი ქსლეში შესაღწევად

როგორც ზემოთ ავღნიშნეთ Token Ring ქსელი შედგება სადენების მონაკვეთებისაგან, რომლებიც ჰოსტებს აერთიანებენ წრეში, აქედან გამომდინარე ყოველი ჰოსტი დაკავშირებულია თავის უკან და წინ მდგომ ჰოსტებთან და მონაცემების გაცვლა უშუალოდ მხოლოდ ამ ჰოსტებთან შეუძლია. ფიზიკურ გარემოში შესაღწევად წრეში მუდმივად ცირკულირებს სპეციალური ფრეიმი - მარკერი. Token Ring ქსელში ნებისმიერი ჰოსტი ინფორმაციას ღებულობს მხოლოდ უკან მდგომი ჰოსტიდან. ასეთ ჰოსტს უწოდებენ *უახლოეს აქტიურ მეზობელს.* გადაცემისას კი ის გადასცემს ინფორმაციას მხოლოდ მის წინ მდგომ ჰოსტს.

მარკერის მიღების შემდეგ ჰოსტი აანალიზებს მას და მონაცემების არარსებობის შემთხვევაში ის უზრუნველყოფს მარკერის გადაცემას მის წინ მდგომ ჰოსტზე. ჰოსტს, რომელსაც გააჩნია მონაცემი გადასაცემად, მარკერის მიღებისას ის ხსნის ამ მარკერს წრიდან,რაც მას საშუალებას აძლევს შეაღწიოს ფიზიკურ გარემოში. ამის შემდეგ ეს ჰოსტი უშვებს მონაცემთა ფრეიმს წრეში. გადაცემული მონაცემები გადიან წრეში ყოველთვის ერთი მიმართულებით ერთი ჰოსტიდან მეორეში. ფრეიმი აღიჭურვება ადრესატის და გამომგზავნის მისამართებით. ყველა ჰოსტი რეტრანსილირებას უკეთებ ამ ფრეიმს როგორც კონცენტრატორი.

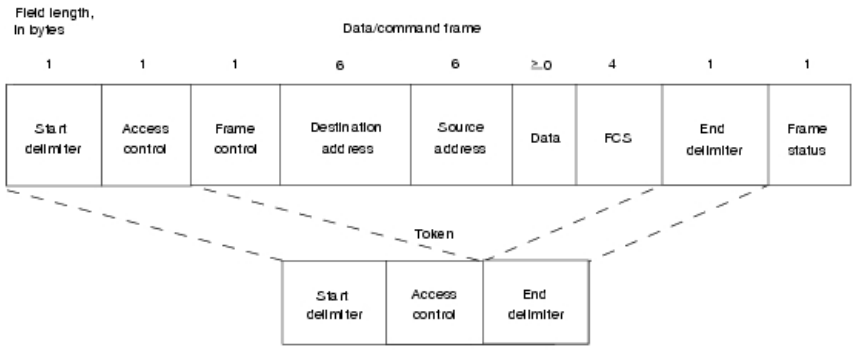
თუ ფრეიმი გადის ადრესატის ჰოსტს, მაშინ ეს ჰოსტი ამოიცნობს საკუთარ მისამართს. ამოცნობის შემდეგ ეს ფრეიმი კოპირდება შიდა ბუფერში, შემდეგ ადრესატი გამომგზავნს უდასტურებს რომ მან მიიღო ფრეიმი. ჰოსტი, რომელმაც გააგზავნა ფრეიმი, დასტურის მიღების შემდეგ ხსნის ამ ფრეიმს წრიდან და აგზავნის ახალ მარკერს.

Token Ring ფრეიმის ფორმატი

Token Ring-ში არსებობს 3 განსხვავებული ფორმატი:

- მარკერი;
- მონაცემთა ფრეიმი;
- წყვეტის თანმიმდევრობა;
- მარკერი.

ფრეიმი - მარკერი შედგება სამი ველისაგან, თითოეული ერთი ბაიტია.



ნახაზი 96. Token Ring ფრეიმის ფორმატი

- საწყისი გამყოფი (Start delimiter) - ჩნდება მარკერის და ყველა ფრეიმის დასაწყისში. ეს ველი წარმოადგენს უნიკალური მათემატიკური კოდის თანმიმდევრობას. ამიტომ საწყისი მსაზღვრელი არ უნდა შეგვეშალოს სხვა ბიტურ თანმიმდევრობაში ფრეიმის შიგნით.

- გარემოში შეღწევის კონტროლი (Access Control) - შედგება 4 ქვეველისაგან: PPP,T,M, RRR. სადაც: PPP-არის პრიორიტეტის ბიტები, T-მარკერის ბიტი, M - მონიტორის ბიტი, RRR-სპრირეზერვო პრიორტეტის ბიტები. ბიტ T–ში თუ მითითებულია 1, ეს მიანიშნებს, რომ ეს მინიჭებულია აქტიური მონიტორის მიერ, დანარჩენ ყველას უთითებს 0. თუ აქტიური მონიტორი ხედავს ფრეიმს ან მარკერს, რომელიც შეიცავს მნიშვნელობას 1, მაშინ აქტურმა მონიტორმა იცის, რომ მარკერმა ან ფრეიმმა უკვე შემოიარა ერთი წრე ისე რომ არცერთი ჰოსტის მიერ არ იქნა დამუშავებული. თუ ეს ფრეიმია, მაშინ ის მოშორებული იქნება წრიდან და თუ ეს მარკერია მაშინ ის გადაცემული იქნება წრეში ხელმეორედ.

- საბოლოო გამყოფი (End delimiter) - საბოლოო ველი მარკერში. ისევე როგორც საწყისი გამყოფი შეიცავს უნიკალურ თანმიმდევრობას მათემატიკური კოდისა. იგი ასევე შეიცავს ორ ერთბიტიან მაჩვენებელს: I და E. I მიუთითებს იმაზე არის თუ არა ფრეიმი საბოოლოო (I=0), ან შუალედური (I=1). ნიშანი E-ეს არის შეცდომის მანიშნებელი. მასში ეთითება 0 გამომგზავნი ჰოსტის მიერ და ნებისმიერი ჰოსტი, რომლის გავლითაც გადის ფრეიმი, თუ ის საკონტროლო ჯამის მიხედვით აღმოაჩენს შეცდომას, ვალდებულია ნიშანი შეცვალოს 1-ით.

მონაცემთა ფრეიმი და წყვეტადი თანმიმდევრობა

მონაცემთა ფრეიმი ისევე როგორც მარკერი შეიცავს იმავე 3 ველს და დამატებით კიდევ რამოდენიმე ველს:

- საწყისი გამყოფი (Start delimiter);
- გარემოში შეეღწევის კონტროლი (Access Control);
- ადრესატის მისამართი;
- გამომგზავნის მისამართი;
- მონაცემები;
- საკონტროლო ჯამი;
- საბოლოო გამყოფი (End delimiter);
- ფრეიმის სტატუსი.

კომუტაცია

ლოკალური ქსელების ძირითადი ნაწილი იგება Ethernet ტექნოლოგიით, რომელიც როგორც ვიცით ტოპოლოგიურად, შეიძლება იყოს როგორც სალტე, ასევე ვარსკვლავი. თანამედროვე ლოკალური Ethernet ქსელები იგება მხოლოდ და მხოლოდ ვარსკვლავური ტოპოლოგიით.

ვარსკვლავური ტოპოლოგიის შესაქმნელად საჭიროა ქსელური აპარატურა, როგორიც არის ჰაბი და სვიჩი.

ჰაბი არის მოწყობილობა რომელიც მუშაობს ფიზიკურ დონეზე და ხშირად მას უწოდებენ Ethernet კონცენტრატორს. ჰაბი არის საუკეთესო მოწყობილობა ქსელში მომხმარებლების ჩასართველად. მისი მთავარი ფუნქციაა ერთ პორტზე შემოსული სიგნალი გაავრცელოს ყველა თავის არსებულ პორტებზე, გარდა იმ პორტისა საიდანაც შემოვიდა სიგნალი.

ის აგრეთვე უზრუნველყოფს სიგნალის რეგენერირებას, რათა გასწორდეს დამახინჯებული სიგნალი.

Ethernet ფუნდამენტურად არის საერთო არხის სისტემა. ამ ქსელში გაერთიანებული ყველა მომხმარებელი იყოფს საერთო არხს. ეს მსგავსია იმ სიტუაციის, როდესაც ცალმხრივ გზაზე თავს იყრის ერთდროულად რამოდენიმე მანქანა, მაგრამ გზა საშუალებას იძლევა დროის ერთ მომენტში მხოლოდ ერთი გაატაროს.

კოლიზია (ინფორმაციის შეჯახება) არის Ethernet ქსელის პროდუქტი.

როგორც წინა თავში ავღნიშნეთ, თუ ორი მოწყობილობა ცდილობს დროის ერთ მომენტში გააგზავნოს ინფორმაცია, ეს იწვევს კოლიზიას. ამიტომ ასეთ დროს ინფორმაცია უნდა იქნეს გადაცემული თავიდან. ხშირი კოლიზია შეიძლება გამოწვეული იქნას მომხმარებლების დიდი რაოდენობით არსებობის გამო, ან მათი ქსელში ერთდროულ შეღწევის სურვილის გამო.

Ethernet იდეალურად მუშაობს, თუ მოწყობილობები რომლებიც ქსელში ცდილობენ შეღწევას მცირე რაოდენობით არიან, კოლიზიების რიცხვი ამ შემთხვევაში მისაღებ ფარგლებში რჩება. მაგრამ, როდესაც მომხმარებლების რაოდენობა იზრდება ქსელში,

მაშინ შესაბამისად იზრდება კოლიზიებიის რაოდენობა, რაც მნიშვნელოვნად ამცირებს ქსელის მწარმოებლურობას.

კოლიზიები და ფართომაუწყებლობითი შეტყობინებები არის თანამედროვე ქსელებშიც.

ამ პრობლემის გადაწყვეტა შესაძლებელია მხოლოდ სეგმენტაციით ანუ ერთი კოლიზიური დომეინის გაყოფით რამოდენიმე ნაწილად. ამ ამოცანის შესასრულებლად გამოიყენება მოწყობილობა ხიდი, რომელიც არის არხის დონის მოწყობილობა. ხიდი ქმნის მისამართების ცხრილს და ამ ცხრილის საშუალებით ღებულობს გადაწყვეტილებას გადააგზავნოს თუ არა ფრეიმი.

სვიჩი არის მეორე დონის მოწყობილობა, რომელიც ინფორმაციის გადაცემისას გადაწყვეტილებას ღებულობს ფრეიმში მოთავსებული ფიზიკური მისამართის შესაბამისად.

ბოლო რამდენიმე წელიწადში სვიჩები გახდნენ უმეტესობა ქსელების ფუნდამენტალური ნაწილი. სვიჩები ახდენენ ლოკალური ქსელის სეგმენტაციას კოლიზიურ დომენებათ. სვიჩის თითოეული პორტი წარმოადგენს განცალკევებულ კოლიზიურ დომეინს და უზრუნველყოფს მოწყობილობას სრული გამტარუნარიანობით. რაც ნაკლებია მოწყობილობა თითოეულ კოლიზიეურ დომეინში, მით მეტია საშუალო გამტარუნარიანობის ზრდა თითოეული მოწყობილობისათვის და კოლიზიების რიცხვიც მცირდება.

ლოკალურ ქსელს შეიძლება ჰქონდეს ცენტრალური სვიჩი, რომელსაც უკავშირდებიან კონცენტრატორები და კონცენტრატორებს კი მომხმარებლები, ან ლოკალური ქსელში შეიძლება ყველა კოპმიუტერი იყოს შეერთებული სვიჩში. ქსელში

სადაც კონცენტრატორები უკავშირდებიან სვიჩს კოლიზიები მაინც მოხდება, თუმცა სვიჩი მათ იზოლაციას ახდენს.

თუ მოწყობილობები პირდაპირ არიან ჩართულნი ლოკალურ ქსელში სადაც ყველა მოწყობილობა პირდაპირ არის ჩართული სვიჩში, მაშინ ქსელის გამტარუინარიანობა ძლიერ იზრდება. სამი ძირითადი მიზეზი ამისა არის:

1. მიკუთვნებული გამტარუნარიანობა თითოეული პორტი-სათვის;

2. უკოლიზიო გარემო;

3. სრული-დუპლექსის რეჟიმი.

გამტარუნარიანობა

თითოეულ მოწყობილობას აქვს მედიის სრული გამტარუნა-რიანობა მოწყობილობასა და სვიჩს შორის. იმის გამო, რომ კონცენტრატორი უგზავნის ყველა მოწყობილობას მიღებულ სიგნალებს, ეს ნიშნავს რომ არხის მთლიანი გამტარუნარიანობა უნდა განაწილედეს ყველა მოწყობილობას შორის. სვიჩებში გამტარზე შეჯიბრის გარეშე თითოეულ მოწყობილობას აქვს მიკუთვნებული კავშირი

მაგალითად შევადაროთ ორი Fast Ethernet ლოკალური ქსელი **ა** და **ბ**, თითოეულზე 10 მოწყობილობით, ქსელის სეგმენტ **ა**-ში, 10 მოწყობილობა არის ჩართული კონცენტრატორით და თითოეული მოწყობილობა ინაწილებს ამ 100მბიტ/წამს. ეს იძლევა საშუალო 10მბიტ/წამს. **ბ** ქსელის სეგმენტში ასევე 10 მოწყობილობა

ჩართულია ოღონდ სვიჩში, ამ სეგმენტში ათივე მოწრობილობას აქვს სრული 100მბიტ/წმ გამტარუნარიანობა.

ამ პატარა ქსელის მაგალითშიც კი, განსხვავება დიდია და მოწყობილობების რაოდენობის გაზრდასთან ერთად განსხვაბაც მნიშვნელოვნად იზრდება.

უკოლიზიო გარემო

მიკუთვნებული კავშირი (წეტილიდან-წერტილამდე) სვიჩთან ასევე აუქმებს ნებისმიერი სახის შეჯიბრს მოწყობილობათა შორის. და ნებას რთავს მოწყობილობას იმუშაოს ნაკლებ ან საერთოდ უკოლიზიო გარემოში. საშუალო ზომის კლასიკური Ethernet ქსელებში კონცენტრატორების გამოყენებით გამტარუნარიანობის 40%-დან 50%-მდე იხარჯება კოლიზიებიდან გამოსვლაში. სვიჩიან Ethernet ქსელში ეს თითქმის 0-ის ტოლია. და ეს ანიჭებს სვიჩიან ქსელებს საგრძნობლად უკეთესს გამტარუნარიანობას.

სრული-დუპლექსის რეჟიმი

სვიჩინგი (კომუტაცია) იძლევა ნებას, რომ ქსელმა იმუშაოს სრული-დუპლექსის რეჟიმში. სანამ კომუტაცია გაჩნდებოდა Ethernet მხოლოდ ნახევარ-დუპლექსის რეჟიმში მუშაობდა. ეს ნიშნავდა, რომ დროის ნებისმიერ მომენტში მოწყობილობა ან აგზავნიდა მონცემებს ან იღებდა. მოწყობილობები რომლებიც პირდაპირ შეერთებულიბი არიან სვიჩთან, იძლევიან საშუალებას ერთდროულად მიიღონ და გადასცენ ინფორმაცია სრული გამტარის გამტარუნარიანობით.

თუ კავშირი მოწყობილობასა და სვიჩს შორის არის უკოლიზიო, მაშინ ამის შედეგად ორჯერ იზრდება გადაცემის სიჩქარე ნახევარ-

დუპლექსიან ქსელებთან შედარებით. თუ ქსელის სიჩქარე არის 100მბიტ/წამი, თითოეულ მოწყობილობას შეუძლია ერთდროულად გადასცეს 100მბიტ/წამით და მიიღოს 100მბიტ/წამით.

სვიჩების გამოყენება კონცენტრატორების მაგივრად

თანამედროვე Ethernet-ში უმეტესად გამოიყენება სვიჩები და სრული-დუპლექსის რეჟიმი. იმის გამო, რომ სვიჩები ზრდიან გამტარუნარიანობას სწორი შეკითხვა იქნება თუ ვიკითხავთ თუ რატომ არ გამოიყენება სვიჩები ყველა Ethernet ლოკალურ ქსელში? არის 3 მიზეზი :

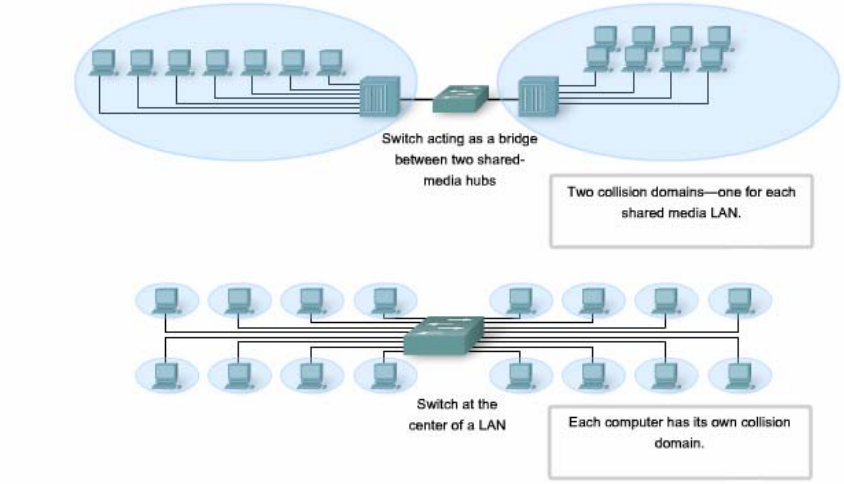
ასორტიმენტი – ლოკალური ქსელების სვიჩები არ იყო შემუშავებული ადრეულ 90-იან წლებამდე და ამიტომ ზოგიერთ ლოკალურ ქსელებში ჯერ კიდევ გამოიყენება.

ეკონომიკა – თავდაპირველად სვიჩები ძალიან ძვირი ღირდა და რაც ფასი დაეცა კონცენტრატორების გამოყენებამ დაიკლო, და ფასიც ნაკლებად მნიშვნელოვანი ფაქტორი გახდა გადაწყვეტი-ლებების მიღებაში.

მოთხოვნილება - ადრეული ლოკალური ქსელები წარმოიშვა დაშორებულ მომხმარებლებს შორის ფაილების გასაცვლელად და პრინტერების გამოსაყენებლად. ქსელების განვითარებამ მოითხოვა მეტი გამტარუნარიანობა, თუმცა ზოგან ჯერ კიდევ აკმაყოფილებთ კონცენტრატორის მუშაობა.

Ethernet სვიჩები ინდივიდუალურ კადრებს მიმართავენ მიმღები პორტიდან იმ პორტისკენ, რომელზეც არის დანიშნულების ადგილი. ეს შეგვიძლია წარმოვიდგინოთ როგორც მომენტალური

კავშირის შექმნა გადამცემ და მიმღებ მოწყობილობებს შორის. კავშირი ხდება მხოლოდ იმ დროით რომელიც არის საჭირო ერთი ფრეიმის გადასაგზავნად. ამ მომენტში ამ მოწყობილობებს აქვთ სრული გამტარუნარიანობა ერთმანეთთან და წარმოადგენენ ლოგიკურ წერტილიდან-წერტილზე კავშირს.



ნახაზი 97. სვიჩების გამოყენება

თუმცა უფრო ზუსტად თუ ვიტყვით ეს კავშირი არ ხდება უშუალოდ საბოლოო მოწყობილობებს შორის, რადგანაც გადაცემა შეუძლია მოწყობილობას იმ შემთხვევაშიც თუ მიმღები მოწყობილობა დაკავებულია, სვიჩი მიიღებს ფრეიმს და ბუფერში შეინახავს მას და შემდგომ გადააგზავნის. ამას ე.წ. Store And Forward რეჟიმი ეწოდება. ამის გამოყენებით სვიჩი იღებს მთლიან ფრეიმს, ამოწმებს მას შეცდომებზე ან დაზიანებაზე და შემდგომ აგზავნის ფრეიმს დანიშნულების ადგილისაკენ. იმის გამო, რომ მოწყობილობებს არ სჭირდებათ ლოდინი როდის იქნება გამტარი

თავისუფალი, მოწყობილობებს შეუძლიათ აგზავნონ და მიიღონ ინფორმაცია გამტარის სრული სიჩქარით, დანაკარგების გარეშე.

გადართვა(ერთი პორტიდან მეორე პორტზე გადაგზავნა) დაფუძნებულია ადრესატის ფიზიკური მისამართის მიხედვით

სვიჩს აქვს ცხრილი რომელსაც ეწოდება MAC Table.

MAC Address	Send Port
M1 M2 M3 ... Mn	Port P1 Port P2 Port P3 ... Port Pn

ნახაზი 98. სვიჩის ცხრილი - MAC Table

მასში ის პოულობს დანიშნულების ადგილის მისამართის შესაბამის პორტს და თუ იპოვის ინფორმაციას აგზავნის მასში. ამ ცხრილს ბევრნაირად მოიხსენიებენ, მათ შორის ხშირად როგორც სვიჩის ცხრილს. იმის გამო რომ გაჩნდა სვიჩინგი უფრო ძველი ტექნოლოგიიდან, რომელსაც ერქვა გამჭვირვალე ხიდი, ცხრილს ზოგჯერ ეძახიან ხიდის ცხრილს. ამიტომ ბევრი პროცესი რომელიც ხდება სვიჩში შეიძლება სახელში შეიცავდეს ხიდს.

ხიდი არის მოწყობილობა რომელიც ადრინდელ ლოკალურ ქსელებში გამოიყენებოდა ორი ქსელური სეგმენტის დასაკავში-რებლად. ბევრი სხვა ტექნოლოგია შეიქმნა ლოკალური ქსელის სვიჩინგის გარშემო. ერთი ადგილი სადაც ხიდები დღესაც

აქტუალურია ეს უკაბელო ქსელები. უკაბელო ხიდები გამოიყენება ორი უკაბელო ქსელის სეგმენტის ერთმანეთთან დასაკავშირებლად. შესაბამისად ორივე ტერმინს შეხვდებით ქსელების ინდუსტრიაში.

სვიჩის მუშაობა

მუშაობისთვის სვიჩები იყენებენ ხუთ ძირითად ოპერაციას:

- სწავლა;
- დაბერება;
- ჩაციკვლა;
- არჩევითი გადამისამართება;
- ფილტრაცია;
- სწავლა.

სვიჩის ცხრილი უნდა შეივსოს ფიზიკური მისამართებით და მათი შესაბამისი პორტებით. სწავლების პროცესი საშუალებას იძლევა რომ ეს მოხდეს ჩვეულებრივი მუშაობის რეჟიმში. როდესაც ფრეიმი ხვდება სვიჩში, ის უყურებს წყაროს ფიზიკურ მისამართს, შემდგომ ეძებს მას თავის ცხრილში, თუ ის არ მოიპოვება ის დაამატებს მას.

მისამართებს, რომლებიც არიან ცხრილში გააჩნიათ ვადა. ეს ვადა გამოიყენება იმისთვის, რომ წაიშალოს ძველი მისამართები ცხრილიდან. მისამართის დამატებისას იწყება ათვლა და მას შემდეგ რაც ის მიაღწევს ნულს წაიშლება.

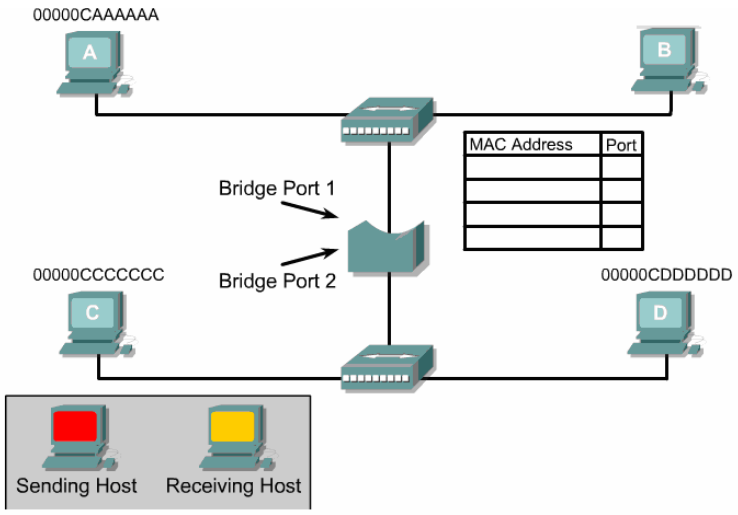
თუ სვიჩმა არ იცის ,რომელ პორტს გაუგზავნოს ფრეიმი, იმიტომ რომ ამ შემთხვევაში მის ცხრილში დანიშნულების ადგილის ფიზიკური მისამართი არ მოიპოვება, სვიჩი აგზავნის ფრეიმს ყველა პორტზე გარდა იმისა რომლიდანაც მოვიდა. ასევე იგზავნება ყველა პორტზე ფრეიმი, როდესაც ხდება ფართომაუწყებლობითი კადრების გასაგზავნა.

არჩევითი გადამისამართება

არჩევითი გადამისამართება არის პროცესი, როდესაც ხდება შემოსული ფრეიმის შემოწმება და დანიშნულების ადგილის ფიზიკური მისამართისა პოვნა, მისამართის ცხრილში და მისი გადაგზავნა შესაბამის პორტში. ეს არის სვიჩის მთავარი ფუნქცია.

ფილტრაცია

ზოგიერთ შემთხვევაში ფრეიმის გადამისამართება არ ხდება. მაგ. თუ ფრეიმი დაზიანებულია, დამატებით მიზეზი შეიძლება იყოს უსაფრთხოების ზომები, თუ სვიჩის კონფიგურაციაში აკრძალულია რომელიმე ფიზიკური მისამართისკენ ან მისგან კადრების გადაცემა.



ნახაზი 99. ხიდის მუშაობის პრონციპი

შემდეგი ნაბიჯები აღწერენ ხიდის მუშაობას:

- თუ ხიდი ახალი ჩართულია, მაშინ ცხრილი თავისუფალია. ხიდი ელოდება ქსელურ ტრაფიკს და როდესაც ტრაფიკს შეამჩნევს ის იწყებს მუშაობას.

- ჰოსტი **A** უგზავნის ინფორემაციას ჰოსტ **B**-ს. ეს ინფორმაცია იგზავნება მთლიან კოლიზიურ დომეინში, ორივე ხიდიც და ჰოსტი **B**-ც ამუშავებენ ამ პაკეტს.

- ხიდი ამატებს ფრეიმიდან გამომგზავნის მისამართს ცხრილში და აფიქსირებს რომ ეს მისამართი მიიღო პირველი პორტიდან. ამიტომ ეს მისამართი ასოცირებული იქნება პირველ პორტთან.

- ადრესატის მისამართი იქნება შემოწმებული ცხრილთან მიმართებაში. სანამ მისამართი არ არის ცხრილში, თუნდაც ის იყოს იმავე სეგმენტში საიდანაც ფრეიმი გავრცელდა, გადა-

გზავნილი იქნება სხვა სეგმენტშიც. ჰოსტი **B**-ს მისამართი ჯერ კიდევ არ არის ჩაწერილი ცხრილში.

- ჰოსტი **B-ს** მოთხოვნის პასუხად ჰოსტი **A** უბრუნებს პასუხს ჰოსტ **B-ს.** მონაცემები გავრცელდება ამ კოლიზიურ დომეინში. ორივე ხიდიც და ჰოსტი **A**-ც ამუშავებენ ამ პაკეტს.

- ხიდი ამატებს გამომგზავნის ჰოსტი **A**–ს მისამართს ცხრილში და აფიქსირებს რომ ეს მისამართი მიიღო პირველი პორტიდან, ამიტომ ეს მისამართი ასოცირებული იქნება პირველ პორტთან.

- ადრესატის მისამართი იქნება შემოწმებული ცხრილთან მიმართებაში. თუ ადრესატის მისამართი არსებობს ცხრილში მაშინ ის გადაიგზავნება იმ პორტზე რომელ სეგმენტთანაც არის ასოცირებული აღნიშნული ადრესატი. რადგანაც ჰოსტი **A**–ს მისამართი ასოცირებულია პირველ პორტთან, ფრეიმი არ გადაიგზავნება სხვა სეგმენტში.

- ჰოსტი **A** უგზავნის ინფორემაციას ჰოსტ **C**-ს. როდესაც ეს ინფორფაცია გაიგზავნება კოლიზიურ დომეინში, ორივე ხიდიც და ჰოსტი **B-ც** ამუშავებენ ამ ფრეიმს. ჰოსტი **B** გადააგდებს ამ ფრეიმს რადგანაც ამ ფრეიმში ჩაწერილი ადრესატის მისამართი არ ემთხვევა თავის მისამართს.

- ხიდი ამატებს გამომგზავნის მისამართს ცხრილში და როდესაც მოხდება მისამართის დამატება, ცხრილი განახლდება.

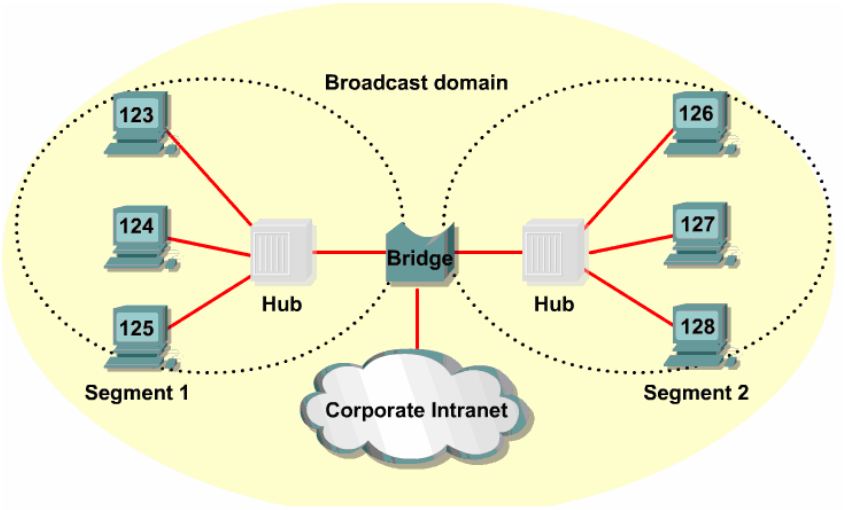
- ადრესატის მისამართი იქნება შემოწმებული ცხრილთან მიმართებაში. სანამ მისამართი არ არის ცხრილში, ის გადაგზავნილი იქნება სხვა სეგმენტშიც. ჰოსტი **C**-ს მისამართი ჯერ კიდევ არ არის ჩაწერილი ცხრილში.

- ჰოსტი **A-ს** მოთხოვნის პასუხად ჰოსტი **C** უბრუნებს პასუხს ჰოსტ **A-ს.** მონაცემები გავრცელდება ამ მთლიან კოლიზიურ დომეინში. ორივე ხიდიც და ჰოსტი **D**-ც ამუშავებენ ამ პაკეტს. ჰოსტი **D** გადააგდებს ამ ფრეიმს რადგან ფრეიმში ადრესატის მისამართი არ არის თანხვედრი მის მისამართთან.

- ხიდი ამატებს გამომგზავნის ჰოსტი **C**–ს მისამართს ცხრილში და აფიქსირებს, რომ ეს მისამართი მიიღო მეორე პორტიდან. ამიტომ ეს მისამართი ასოცირებული იქნება მეორე პორტთან.

- ადრესატის მისამართი იქნება შემოწმებული ცხრილთან მიმართებაში. რადგანაც ადრესატის მისამართი არსებობს ცხრილში და ასოცირებულია პირველ პორტთან, ის გადაიგზავნება პირველ პორტზე.

ძირითადად ხიდი არის ორ პორტიანი მოწყობილობა და კოლიზიურ დომეინს ყოფს ორ ნაწილად. ყველა გადაწყვეტილებას ხიდი იღებს მეორე დონის MAC მისამართის მიხედვით. ხიდის საშუალებით იქმნება ერთიანი ფართომაუწყებლობითი დომეინი.



ნახაზი 100. ერთიანი ფართომაუწყებლობითი დომეინი

სვიჩი არის ფუნქციონალურად იგივე ტიპის მოწყობილობა, ოღონდ მას გააჩნია მეტი პორტი. სვიჩს რამდენი პორტიც აქვს იმდენი კოლიზიური დომეინი იქნება. სვიჩი არის მრავალპორტიანი ხიდი.

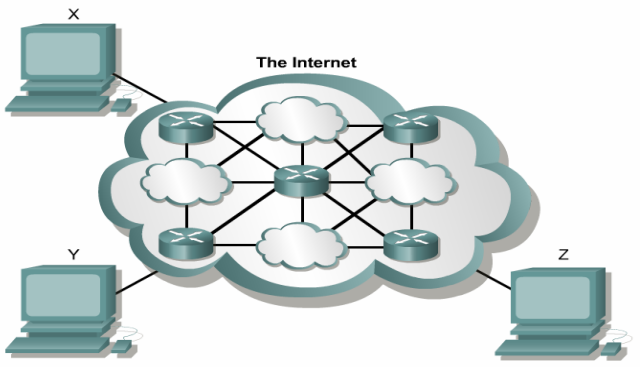
კოლიზიური დომეინი არის ქსელის ფიზიკური სეგმენტი, სადაც შესაძლებელია მოხდეს კოლიზია.

ინტერნეტის არქიტექტურა

ინტერნეტი არის ქსელი, რომელიც იძლევა შესაძლებლობას მთელი მსოფლიოს მასშტაბით იქნას უზრუველყოფილი მონაცემების გაცვლა ნებისმიერ პიროვნებას შორის, ნებისმიერ ადგილას და ნებისმიერ დროს.

ლოკალური ქსელი როგორც ვიცით არის შეზღუდული გეოგრაფიული გარემოთი. მიუხედავად ამისა მას გააჩნია ტექნოლოგიური უპირატესობები, მას გააჩნია გადაცემის მაღალი სიჩქარე და საიმედოობა. პრობლემა არის მისი დისტანცია.

ინტერნეტი შეიქმნილია ერთმანეთისგან დამოუკიდებელი ტექნოლოგიებით და ტოპოლოგიებით. მთელი მსოფლიოს მასშტაბით ეს ქსელები ერთიანდებიან ერთმანეთთან მარშუტიზატორების გამოყენებით და ქმნიან ინტერქსელს ანუ ქსელთა ქსელს.



ნახაზი 101. ინტერნეტის არქიტექტურა

როგორც ზემოთ ავღნიშნეთ, იმისათვის რომ მოხდეს ინფორმაციის გაცვლა, საჭიროა ინტერნეტი ჩართული ყოველი

ჰოსტი იდენტიფიცირებული იქნას უნიკალურიი მისამართებით. ამისათვის შეიქმნა ინტერნეტიის დამისამართების ერთიანი სისტემა, ისევე როგორც სატელეფონო ქსელებში.

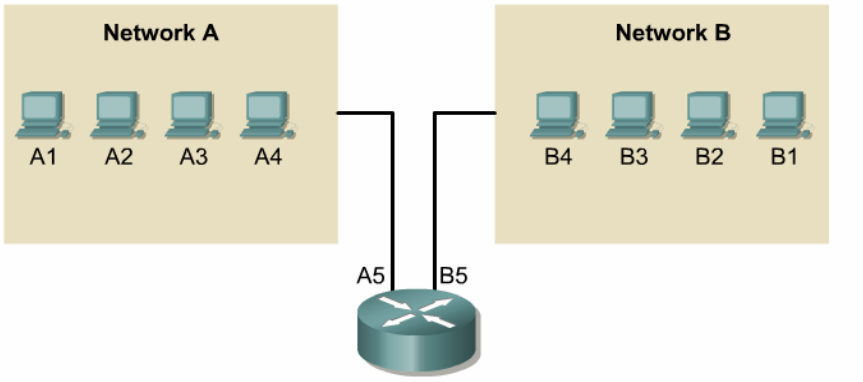
IP დამისამართება

კომპიუტერების ქსელის შექმნის პროცესში, ერთ-ერთ პრობლემას წარმოადგენს დამისამართება. კომპიუტერის ანუ ჰოსტის მისამართი უნდა იყოს უნიკალური, რადგან შესაძლებელი იყოს მისი დარეგისტრირება ნებისმიერ ქსელში. მას უნდა ქონდეს იერარქიული სტრუქტურა, რადგან მოსახერხებელი იყოს დიდი ქსელების ასაგებად. თუ მისამართს არ ექნება იერარქიული სტრუქტურა, მაშინ საკომუტაციო საშუალებებს ადრესატის მდებარეობის დასადგენად მოუწევთ უამრავი მისამართების ცხრილების გაანალიზება.

როგორც ზემოთ ავღნიშნეთ მისამართები არის ორი ტიპის: ლოგიკური და ფიზიკური. ლოგიკური მისამართები ადამიანებისთვის გაცილებით ადვილი დასამახსოვრებელია, რადგანაც ის არის იერარქიული. ლოგიკური მისამართი ყოველთვის გვეხმარება თუ როგორ ვიპოვოთ ფიზიკური მისამართი.

კომპიუტერი უნდა იყოს დაკავშირებული არა უმცირეს ერთ ქსელთან და შესაბამისად მას უნდა ჰქონდეს ერთი მისამართი. ყოველი მისამართი იდენტიფიცირებულია სხვადასხვა ქსელში. IP მისამართი ლოგიკურად გაყოფილია ორ ნაწილად, ქსელის მისამართი და ჰოსტის მისამართი. ქსელის მისამართისა და ჰოსტის მისამართის კომბინაცია იძლევა უნიკალურ მისამართს ყოველი მოწყობილობისათვის ქსელში. ეს მისამართი მუშაობს ქსელურ დონეზე და იძლევა შესაძლებლობას ერთმა კომპიუტერმა

აღმოაჩინოს მეორე კომპიუტერი ქსელში. ყველა კომპიუტერს აგრეთვე გააჩნია უნიკალური ფიზიკური მისამართი, რომელიც ცნობილია როგორც MAC მისამართი. ეს მისამართი ენიჭება მწარმოებელი ფირმის მიერ ქსელურ ადაპტერს წარმოების დროს და ის მუდმივად არის ჩაწერილი ადაპტერში. ის მუშაობს OSI მოდელის არხის დონეზე.



ნახაზი 102. მისამართების დაჯგუფების კონცეფცია

IP მისამართი არის 32 ბიტიანი რიცხვი. IP მისამართებთან ადვილად სამუშაოდ, მთლიანი მისამართი დაყოფილია 4 ნაწილად, ანუ 4 ბაიტად წერტილების საშუალებით და წარმოდგენილია ათობითი ფორმატით. მაგალითად ერთი კომპიუტერის IP მისამართი შეიძლება იყოს 192.168.7.1, მეორესი 172.16.2.2. ყოველ ნაწილს უწოდებენ ოქტეტებს, რადგანაც თითოეულში შედის 8 ბიტი. მაგალითად, IP მისამართი 192.168.1.8 ორობით ფორმატში იქნება 11000000.10101000.00000001.00001000, კომპიუტერში IP მისამართის მინიჭება ხდება ათობით ფორმატში, რადგანაც ათობითი ფორმატის წარმოდგენა გაცილებით იოლია ვიდრე ორობითის.

მარშუტიზატორი როგორც ვიცით არის მოწყობილობა, რომელიც გამოიყენება პაკეტების ქსელიდან ქსელში გადაცემისას. ის გადასცემს პაკეტებს გადამცემი ქსელიდან ადრესატ ქსელში. ყოველ პაკეტს უნდა ჰქონდეს როგორც ადრესატის ასევე გამომგზავნის მისამართი. მარშუტიზატორი იყენებს ადრესატის ქსელის მისამართს, რომ მან შეძლოს შესაბამისი ქსელის გზის მონახვა და ამ ქსელამდე პაკეტის მიწოდება.

როგორც ზემოთ ავღნიშნეთ IP მისამართი შედგება ორი ნაწილისგან, ერთი აღნიშნავს ქსელის მისამართს მეორე ჰოსტის მისამართს. ყოველი ოქტეტი იცვლება 0 დან 255-მდე.

ასეთი სისტემის მისამართებს იერარქიულ მისამართებსაც უწოდებენ, რადგან ისინი შედგებიან ორი ნაწილისაგან, ჯამში ციფრი უნდა იყოს უნიკალური, წინააღმდეგ შემთხვევაში შეუძლებელი გახდება მარსუტიზაცია.

IP მისამართები იყოფა კლასებად: დიდი, საშუალო და მცირე ქსელებისთვის. A კლასის მისამართები ენიჭებიან დიდ ქსელებს, B კლასის მისამართები საშუალო ზომის ქსელებს, ხოლო C კლასის მისამართები მცირე ზომი ქსელებს.

ყოველი 32 ბიტიანი IP მისამართი იყოფა ქსელის და ჰოსტის ნაწილად, პირველი ბიტი ან ბიტების ჯგუფი განსაზღვრავს მისამართების კლასს. არსებობს სულ 5 კლასი.

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

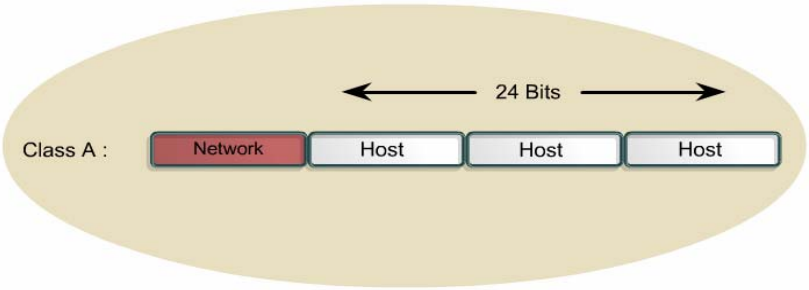
Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

ნახაზი 103. IP მისამართების კლასები

მეხუთე კლასი E გამოიყენება ექსპერიმენტული მიზნებისთვის.

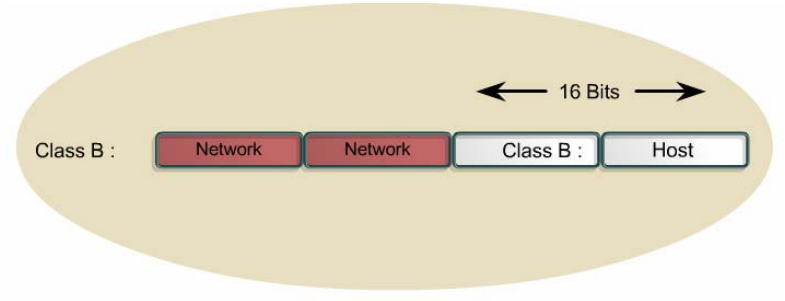
A კლასის გამოიყენება დიდი ქსელების დასამისამართებლად. ერთი A კლასის ქსელი დაახლოებით შეიცავს 16 მილიონი ჰოსტის მისამართს. ამ კლასში ქსელის მისამართი არის პირველი ოქტეტი, დანარჩენი 3 ოქტეტი არის ამ ქსელში ჰოსტის მისამართი. აქედან გამომდინარე ყველაზე მცირე რაოდენობით არის A კლასის ქსელები, მაგრამ თითოეულში ჰოსტების მისამართების დიდი რაოდენობით.



ნახაზი 104. A კლასი

A კლასის მისამართში პირველი ბიტი ყოველთვის არის 0. ყველაზე დაბალი რიცხვი რომელიც პირველი ბიტის 0 ის არსებობის შემთხვევაში იქნება არის 00000000 ანუ ათობითში 0. უდიდესი რიცხვი კი 01111111, ათობითში 127. რიცხვები 0 და 127 არის რეზერვირებული და არ გამოიყენება ქსელის მისამარებად. დანარჩენი მისამართები 1-დან 126, წარმოადგენს A კლასის ქსელის მისამართებს. 127.0.0.0 ქსელი არის რეზერვირებული Loopback ტესტირებისთვის.

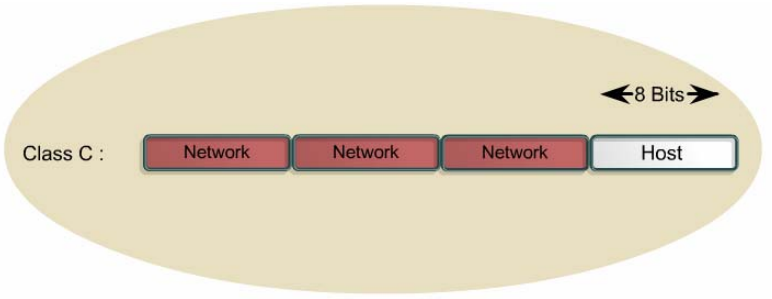
B კლასის მისამართები შეიქმნა საშუალო ზომის ქსელების დასამისამართებლად. B კლასის მისამართი იყენებს პირველ ორ ოქტეტს ქსელის დასამისამართებლად, ხოლო დანარჩენ ორ ოქტეტს ჰოსტების დასამისამართებლად.



ნახაზი 105. B კლასი

პირველი ორი ბიტი B კლასის მისამართში არის 10. დანარჩენი 6 ბიტი ივსება 0 და 1–ით. ყველაზე დაბალი რიცხვი წარმოდგენილია 10000000, ათობითში არის 128. უდიდესი რიცხვი კი 10111111, ათობითში არის 191. B კლასის ქსელის მისამართების პირველი ოქტეტი მოქცეულია დიაპაზონში 128- 191.

C კლასის მისამართები არის ყველაზე გამოყენებდი. ის უზრუნველყოფს მცირე ქსელების დამისამართებას (მაქსიმუმ 254 ჰოსტი).



ნახაზი 106. C კლასი

C კლასის მისამართები იწყება 110-ით. ყველაზე დაბალი რიცხვი წარმოდგენილია 11000000, ათობითში არის 192. უდიდესი რიცხვი კი 11011111, ათობითში არის 223. B კლასის ქსელის მისამართების პირველი ოქტეტი მოქცეულია დიაპაზონში 192- 223.

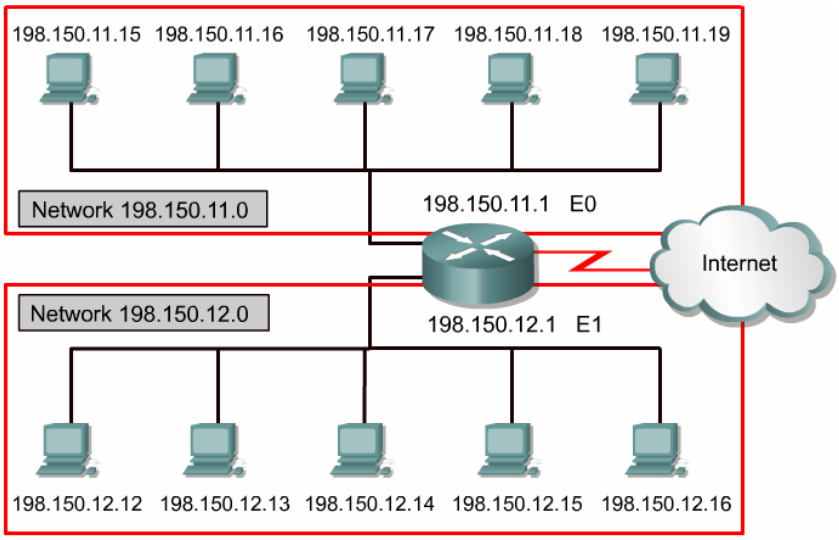
IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)

ნახაზი 107. კლასების მისამართების დიაპაზონი

D კლასის მისამართები გამოიყენება მულტიმაუწყებლობისთვის ანუ ერთდროული შეტყობინობის დასაგზავნად. პირველი ოთხი

ბიტი იწყება 1110, უმცირესი რიცხვი არის 11100000 ხოლო უდიდესი 11101111 ანუ 224 და 239.

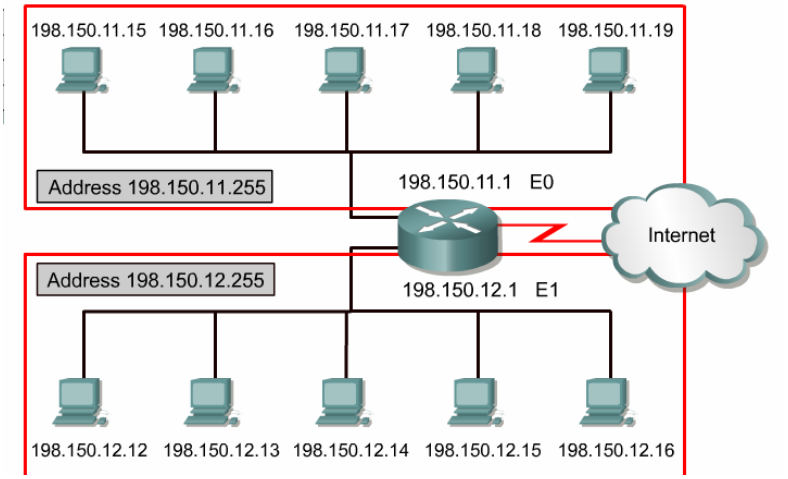
არსებობს რამოდენიმე ჰოსტის მისამართი, რომელიც არ შეიძლება მინიჭებული იქნას ჰოსტზე. ეს არის ქსელის მისამართი. ქსელის მისამართი განსაზღვრავს მთლიანად ქსელს.



ნახაზი 108. ქსელის მისამართი

მოცემულ ნახაზზე ზედა ოთკუთხედში წარმოდგენილია 198.150.11.0 ქსელი. მონაცემები რომლებიც იგზავნება ნებისმიერი ჰოსტიდან (198.150.11.1- 198.150.11.254) ქსელში გარედან ჩანს, როგორც 198.150.11.0 ქსელი. ქვედა ოთხკუთხედშიც მოცემულია იგივე ქსელის სტრუქტურა რაც ზედა ოთკუთხედში, ოღონდ განსხვავებულია მხოლოდ ქსელის მისამართი 198.150.12.0

მეორე მისამართი რომელიც არ შეიძლება იქნას მინიჭებული ჰოსტზე არის ფართომაუწყებლობითი მისამართი (**Broadcast Address**)

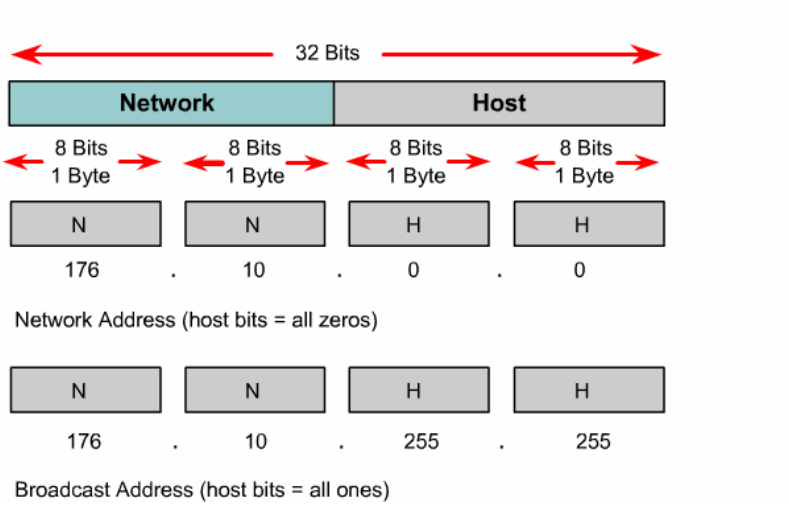


ნახაზი 109. ფართომაუწყებლობითი მისამართი

ნახაზის ზედა ოთკუთხედში წარმოდგენილია მისამართი 198.150.11.255, რომელიც წარმოადგენს ფართომაუწყებლობით მისამართს. მონაცემები რომლებიც იგზავნება ამ მისამართზე გადაეცემა ყველა ამ ქსელში ჩართულ ჰოსტს (198.150.11.1-198.150.11.254) და დამუშავდება მათ მიერ.

IP მისამართი, რომელსაც ჰოსტისთვის განკუთვნილ სამისამართო ბიტებში უწერია 0, ნიშნავს, რომ ასეთი მისამართი რეზერვირებულია ქსელის მისამართად. მაგალითად, A კლასის ქსელში, მისამართი 113.0.0.0 არის ქსელის IP მისამართი, მარშუტიზატორი სწორედ ამ მისამართებს იყენებს როდესაც ის იღებს გადაწყვეტილებას პაკეტების მარშუტიზაციის დროს.

B კლასის ქსელის მისამართში პირველი ორი ოქტეტი არის ქსელის მისამართი. ბოლო ორი ოქტეტი კი შეიცავს 0-ებს. ეს 16 ბიტი არის ჰოსტისთვის განკუთვნილი ანუ იმ მოწყობილობების დასამისამართებლად, რომლებიც მიერეთებულნი იქნებიან ამ ქსელში.



ნახაზი 110. IP მისამართის სტრუქტურა

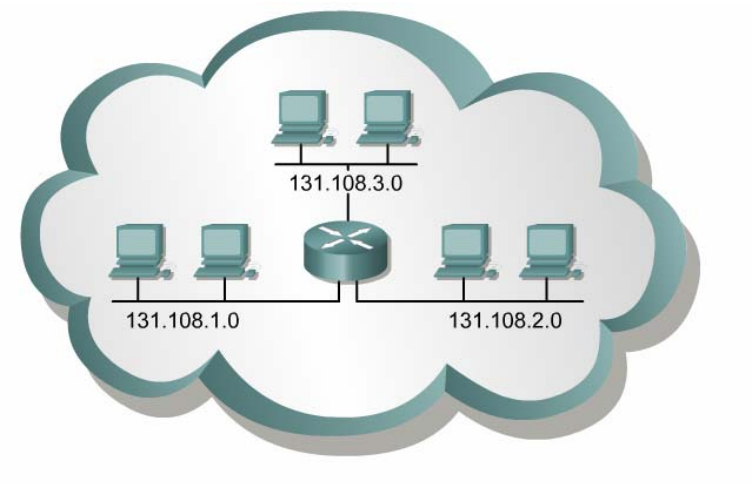
B კლასის ქსელში ქსელის IP მისამართი შეიძლება იყოს 176.10.0.0. ეს მისამართი არასოდეს ენიჭება ჰოსტს. ჰოსტის მისამართი კი შეიძლება იყოს 176.10.16.1 ამ მაგალითის მიხედვით მისამართის ქსელის ნაწილია 176.10 ხოლო ჰოსტის ნაწილია 16.1.

ინფორმაციის ყველა ქსელში ჩართული ჰოსტისთვის ერთდროულად გასაგზავნად ფორმირდება ფართომაუწყებლობითი მისამართი. რომ მივღოთ აღნიშნული მისამართი, ჰოსტისთვის განკუთვნილ სამისამართო ბიტებში იწერება 1-ები.

მაგალითად, ფართომაუწყებლობითი მისამართი არის 176.10.255.255.

ქვექსელების შექმნა

ქვექსელების შექმნა არის მეთოდი, რომ ვმართოთ IP მისამართები, როგორც ეს მოცემულია ნახაზზე



ნახაზი 111. ქვექსელების ორგანიზება

ქსელი 131.108.0.0 დაყოფილია 131.108.1.0, 131.108.2.0 და 131.108.3.0 ქვექსელად. ეს მეთოდი ქსელის მისამართს ყოფს მცირე ნაწილებად, რაც საშუალებას იძლევა უფრო ეფექტურად იქნას გამოყენებული სამისამართო სივრცე და უფრო ადვილია ქსელის მართვა. აღნიშნული მეთოდით ერთიანი სამისამართო სივრცე დაყოფილი რამოდენიმე ნაწილად, შეიძლება განაწილდეს რამოდენიმე ლოკალური ქსელზე მის დასამისამართებლად. ზოგჯერ პატარა ქსელისთვის არ არის აუცილებელი ქვექსელად დაყოფა. ქვექსელად დაყოფა არის აუცილებელი, როდესაც საქმე

გვაქვს დიდი ზომის ქსელებთან. ქვექსელად დაყოფისთვის იყენებენ *ქვექსელის ნიღაბს*. მაგალითად, სატელეფონო სისტემა დაყოფილია სხვადასხვა ადგილის მიხედვით კოდებად: 995 32 330607, სადაც 995 ქვეყნის კოდია, 32 ქალაქის კოდი, 33 სატელეფონო სადგურის მისამართი, 0607 აბონენტის მისამართი. ჯამში ამ რიცხვების კომბინაცია სატელეფონო სისტემაში არის უნიკალური. მსგავსი რიცხვების კომბინაცია მსოფლიო სატელეფონო ერთიან სისტემაში არის ერთადერთი. ასევეა კომპიუტერულ ქსელებშიც. IP მისამართი არის უნიკალური მთელ ინტერნეტის სამისამართო სივრცეში.

სისტემური ადმინისტრატორი წყვეტს რამდენ ნაწილად და რა პორციით უნდა მოხდეს ქსელის დაყოფა ქვექსელად. მან უნდა იცოდეს რამდენი ქვექსელი არის საჭირო, ხოლო თითოეულ ქვექსელში რამდენი ჰოსტი. ნებისმიერი კლასის ქსელი იყოფა ქვექსელად.

ქვექსელის მისამართი მოიცავს ქსელის პორციას პლიუს ქვექსელის და ჰოსტის ველი. ქვექსელის და ჰოსტის ველები იქმნება მთლიანი ქსელის ორიგინალური ჰოსტის პორციიდან. ქვექსელად დაყოფის შესაძლებლობა ქსელის ადმინისტრატორს აძლევს საშუალებას უფრო ადვილად გადაწყვიტოს დამისამართების პრობლემა.

ქვექსელის შესაქმნელად, ქსელის ადმინისტრატორი იღებს ბიტებს ჰოსტის ველიდან და გადასცემს ქვექსელის ველს. როდესაც იქმნება ქვექსელი და არ არის ნასესხები არცერთი ბიტი, მაშინ ფართომაუწყებლობითი მისამართი არის 255. მაქსიმალური ბიტების რაოდენობა რომელიც შეიძლება იქნას ნასესხები ჰოსტის

ნაწილიდან შეიძლება იყოს ნებისმიერი, ოღონდ ბოლო ბაიტში უნდა დარჩეს 2 ბიტი ჰოსტისთვის.

Decimal Notation for First Host Octet	Number of Subnets	Number of Class A Hosts per Subnet	Number of Class B Hosts per Subnet	Number of Class C Hosts per Subnet
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

ნახაზი 112. ქვექსელის მიღების სქემა

ქვექსელად დაყოფის წესები

ქვექსელის სტრუქტურის შესაქმნელად, ჰოსტისთვის განკუთვნილი ბიტების ნაწილი უნდა გადაკეთდეს ქსელურ ბიტებად. ხშირად ამას ნასესხებ ბიტებს უწოდებენ. ბიტების სესხება უნდა მოხდეს ქსელის მისამართთან ყველაზე ახლოსმდგომი ჰოსტის ბიტებიდან.

Class C network address 192.168.10.0

11000000.10101000.00001010.00000000
N . N . N . H

11000000.10101000.00001010.00000000
N . N . N . sN H

In this example three bits have been assigned to designate the subnet.

ნახაზი 113. ქვექსელის მიღების წესი

როგორც ნახაზზე ჩანს, C კლასის ქსელის ჰოსტის პორციიდან ნასესხებია 3 ბიტი (წითლად მონიშნული) და ეს 3 ბიტი გადაეცემა ქვექსელს. ამის შედეგად გაიზრდება ქსელების რიცხვი, მაგრამ თითოეულ ქსელში შემცირდება ჰოსტების დასამისამართებლად განკუთვნილი მისამართები. ქვექსელად დაყოფა იძლევა საშუალებას უფრო უკეთ გაკონტროლდეს სამისამართო სივრცე და უკეთ იქნას ორგანიზებული ქსელის უსაფრთხოების საკითხები.

ქვექსელების ორგანიზება არის ქსელის შიდა ფუნქცია. ლოკალური ქსელი გარედან ჩანს როგორც ერთი მთლიანი ქსელი. ასეთი ხედვა ამცირებს ჩანაწერების რიცხვს მარშუტიზაციის ცხრილებში, რაც ნაკლებად ტვირთავს მარშუტიზატორს.

ბიტების რაოდენობის არჩევა ქვექსელის ორგანიზების დროს დამოკიდებულია ჰოსტების რაოდენობაზე, რომელიც უნდა იყოს ქვექსელში. ბოლო ორი ბიტი ბოლო ოქტეტში არასოდეს უნდა იქნას გამოყენებული ქვექსელის შესაქმნელად მიუხედავად იმისა, თუ რომელი კლასის ქსელს ვყოფთ ქვექსელად. ბოლო ორი ბიტით იქმნება 4 მისამართი, აქედან პირველი არის ქსელის მისამართი, ბოლო კი ფართომაუწყებლობითი მისამართი. რჩება მხოლოდ ორი გამოყენებადი მისამართი ჰოსტებისთვის, რომელსაც ხშირად ორი მოწყობილობის დაკავშირებისას გამოიყენებენ.

ქვექსელის ნიღაბი არის ის საშუალება რომელიც გამოიყენება ქვექსელის შესაქმნელად. ქვექსელის ნიღაბი აძლევს მარშუტიზატორს ინფორმაციას თუ რამდენი ბიტია ქსელის მისამართი და რამდენი ბიტია ჰოსტის მისამართი. ქვექსელის ნიღაბი არის 4 ბაიტიანი რიცხვი და იქმნება ბინარული ერთიანებით, რომელიც ლოგიკური გამრავლებით ედება IP მისამართს. ბინარული ერთიანებით ივსება მხოლოდ ქსელის

დასამისამართებლად განკუთვნილი ბიტების ნაწილი, ხოლო ჰოსტებისთვის გაკუთვნილ ნაწილში იწერება ბინარული ნულები. ანუ ქვექსელის ნიღაბი გამოიყენება იმისათვის, რომ განისაზღვროს თუ რამდენი ბიტია გამოყენებული ქსელისა და ქვექსელის მისამართის შესაქმნელად.

ქვექსელის ნიღაბის გამოთვლისას მნიშვნელოვანია ორი მნიშვნელობის ცოდნა: პირველი - მისამართის კლასი და მეორე - საჭირო ქვექსელების რაოდენობა. ქვექსელის შექმნის გარეშე სტანდარტულ კლასებს ქვექსელის ნიღაბში განესაზღვრებათ ბინარული ერთიანები მხოლოდ ქსელისთვის განსაზღვრულ ნაწილში. A კლასს 255.0.0.0, B კლასს 255.255.0.0, C კლასს 255.255.255.0.

Slash format	/25	/26	/27	/28	/29	/30	N/A	N/A
Mask	128	192	224	240	248	252	254	255
Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1
Total Subnets		4	8	16	32	64		
Usable Subnets		2	6	14	30	62		
Total Hosts		64	32	16	8	4		
Usable Hosts		62	30	14	6	2		

ნახაზი 114. ქვექსელის ნიღაბის გამოთვლა

იმ ბიტების რაოდენობის განსაზღვრისთვის, რომელიც საჭიროა ქვექსელის შესაქმნელად, ქსელის ადმინისტრატორმა უნდა გამოთვალოს ქვექსელებში გასაწევრიანებელი ჰოსტების რაოდენობა და ქვექსელის რაოდენობაც. მაგალითად, ქსელში საჭიროა 6 ქვექსელი, თითოეულში 25 ჰოსტით. იმისათვის, რომ

განსაზღვროთ ბიტების რაოდენობა რომლებიც უნდა ვისესხოთ დავაკვირდეთ ცხრილს.

თუ დავაკვირდებით ველს „გამოყენებადი ქვექსელები“ (Usable Subnets) იგი მიანიშნებს, რომ საჭიროა ვისესხოთ 3 ბიტი ჰოსტის ველიდან. ცხრილში ასევე მითითებულია რომ გამოყენებადი ჰოსტების (Usable Hosts) რაოდენობა ასეთი დაყოფის შემთხვევაში არის 30. განსხვავება საერთო ჰოსტების რაოდენობასა და გამოყენებადი ჰოსტების რაოდენობას შორის არის იმიტომ, რომ პირველი მისამართი არის ქსელის მისამართი, ხოლო ბოლო მისამართი დიაპაზონში არის ფართომაუწყებლობითი მისამართი (Broadcast Address).

მეთოდში, რომელითაც იქნა აგებულ ზემდგომი ცხრილი, გამოიყენება შემდეგი ფორმულა:

გამოყენებადი ქვექსელების რაოდენობა = ორი აყვანილი ნასესხები ბიტების ხარისხში და გამოკლებული ორი.

$2^{\text{ნასესხები ბიტები}} - 2 =$ გამოყენებადი ქვექსელები.

$2^3 - 2 = 6$.

გამოყენებადი ჰოსტების რაოდენობა = ორი აყვანილი ჰოსტისთვის დარჩენილი ბიტების ხარისხში და გამოკლებული ორი (ეს ორი არის ქსელის და ფართომაუწყებლობითი მისამართები).

$2^{\text{ნასესხები ბიტები}} - 2 =$ გამოყენებადი ჰოსტები.

$2^5 - 2 = 30$.

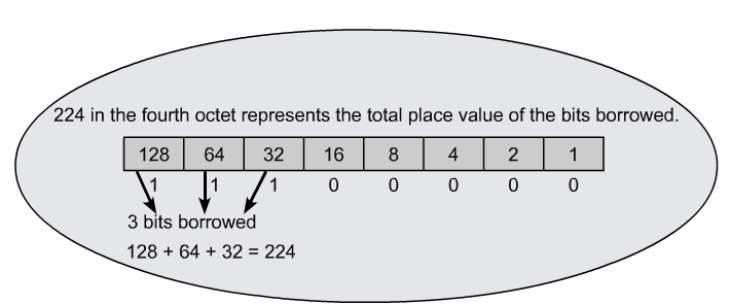
ქვექსელის ნიღაბის მინიჭება

ქვემოთ ნაჩვენებ ნახაზზე მოცემულია ქვექსელების და ჰოსტების მისამართების განაწილება, როდესაც ნასესხებია 3 ბიტი. ამ განაწილებით იქმნება 8 ქვექსელი, თითოეულში 32 ჰოსტის მისამართით.

Subnetwork #	Subnetwork ID	Host Range	Broadcast ID
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

ნახაზი 115. ქვექსელების და ჰოსტების მისამართების განაწილება

პირველს უწოდებენ ნულოვან ქვექსელს. ასეთი განაწილების მისაღებად გამოიყენება ქვექსელის ნიღაბი 255.255.255.224, რომელიც ბინარულ რიცხვში წარმოდგენილი იქნება 11111111.11111111.11111111.11100000 სახით.



ნახაზი 116. . ნიღაბის გამოთვლის მაგალითი

ისევე როგორც სტანდარტულ ქსელებში, ქვექსელშიც ქვექსელის მისამართია ის მისამართი სადაც ჰოსტებისთვის განკუთვნილ სამისამართო სივრცის ყველა ბიტში წერია 0, ხოლო თუ ჰოსტებისთვის განკუთვნილ სამისამართო სივრცის ყველა ბიტში წერია 1, მაშინ ასეთი მისამართი არის ფართომაუწყებლობითი (Broadcast). მაგალითად, ასეთი დაყოფის შემთხვევაში ქვექსელის მისამართი შეიძლება იყოს 192.168.10.32, რომელიც ბინარულ რიცხვში წარმოდგენილი იქნება 11111111.11111111. 11111111.001**00000** სახით, შესაბამისად ფართომაუწყებლობითი მისამართი იქნება 192.168.10.63 - ბინარულ რიცხვში 11111111.11111111. 11111111.001**11111** სახით.

იბეჭდება ავტორთა მიერ წარმოდგენილი სახით

გადაეცა წარმოებას 01.05.2009. ხელმოწერილია დასაბეჭდად 25.06.2009. ქაღალდის ზომა 60X84 1/16. პირობითი ნაბეჭდი თაბახი 13. ტირაჟი 100 ეგზ.

საგამომცემლო სახლი ,,ტექნიკური უნივერსიტეტი'', თბილისი, კოსტავას 77