„MICROSOFT“

- კურსი:

ქსელების შესწავლისა და აგების საფუძვლები

/JES & Co, USA: Understanding and Building Basic Networks/

თარგმანი და საქართველოსათვის ლოკალიზება შესრულებულია
ბათუმის შოთა რუსთაველის სახელობის სახელმწიფო უნივერსიტეტის
საინჟინრო-ტექნოლოგიური ფაკულტეტის
პროფესორის ენვერ ხალვაშის მიერ

http://www.microsoft.com/

ბათუმი, 2011

ძვირფასო მკითხველო!

თქვენს წინაშეა სახელმღვანელო - „ქსელების შესწავლისა და აგების საფუძვლები“, რომელიც შექმნილია კორპორაცია Microsoft-ის დაკვეთით JES & Co, USA კომპანიის სპეციალისტების მიერ. კურსის ორიგინალური სახელწოდებაა „Understanding and Building Basic Networks“.

კურსი მიმართულია სხვადასხვა საგნობრივ დარგებში ინფორმაციული ტექნოლოგიების გამოყენებისათვის. ერთერთი ასეთი დარგია ტელეკომუნიკაცია, რომლის სისტემებში ინტენსიურად აგრძელებს შესვლას ინფორმაციული ტექნოლოგიები.

სახელმძღვანელოს მიზანია - შეასწავლოს ტელეკომუნიკაციის სპეციალობის სტუდენტებს ქსელებისა და ინტერნეტის აგების საფუძვლები, დაეხმაროს ინფოტელეკომუნიკაციური ქსელების შექმნაში და გამოყენებაში, WWW და სხვა ინტერნეტ-მომსახურებების მოქმედების პრინციპების გაცნობიერებაში, ქსელური შეერთებების უსაფრთხოების უზრუნველყოფის საფუძვლების დაუფლებაში.

სახელმძღვანელო დაწერილია გასაგები, სასაუბრო ენით და ამავდროულად შეიცავს დარგისათვის უაღრესად მნიშვნელოვან ინფორმაციას.

კურსში კომპაქტურადაა მოყვანილი აუცილებელი თეორიული მასალა და პრაქტიკული საქმიანობისათვის განსაკუთრებით სასარგებლო მითითებები. ხაზგასმით უნდა აღინიშნოს, რომ სახელმძღვანელო არაჩვეულებრივ მეგზურობას გაუწევს დაინტერესებულ მკითხველს რეალური, უახლესი კაბელური და უკაბელო ინფოტელეკომუნიკაციური ქსელების აგებისას და ექსპლუატაციისას.

კურსი დიდ სარგებელს მოუტანს აგრეთვე უფროსი კლასების მოსწავლეებს.

Microsoft-კურსები თარგმნილია მსოფლიოს მრავალ ენაზე. ქართულ ენაზე თარგმანი და საქართველოსათვის ლოკალიზება ტელეკომუნიკაციაში უახლესი მიღწევების გათვალისწინებით შესრულებულია ბათუმის შოთა რუსთაველის სახელობის სახელმწიფო უნივერსიტეტის საინჟინრო-ტექნოლოგიური ფაკულტეტის პროფესორის ენვერ ხალვაშის მიერ. სახელმძღვანელოს რედაქტირება შესრულებულია ბათუმის შოთა რუსთაველის სახელობის სახელმწიფო უნივერსიტეტის საინჟინრო-ტექნოლოგიური ფაკულტეტის ასისტენტ პროფესორის მარინა ჩხარტიშვილის მიერ.

კორპორაცია Microsoft-ის საერთაშორისო ინიციატივის ფარგლებში „პარტნიორობა განათლებაში“ შესრულებულია კურსის ლოკალიზება რუსეთის ფედერაციისათვის სახელწოდებით «Основы компьютерных сетей», რომლითაც თარგმნის დროს ვისარგებლეთ.

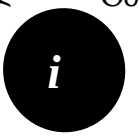
სახელმძღვანელოში მიღებულია ტექსტის შემდეგი გამოყოფები და თანმხლები ნიშნები:

- კურსივით გამოყოფილია მნიშვნელოვანი ცნებები და ტერმინები;
- **მუქი შრიფტით** გამოყოფილია გრაფიკული ინტერფეისების ფანჯრების სახელები, მენიუს პუნქტები და მმართველი ელემენტები (ტექსტური ველები, ღილაკები და სხვა), აგრეთვე საკვანძო ტერმინები და განმარტებები;
- დასკვნები და მნიშვნელოვანი მითითებები აღნიშნულია

  ნიშნით;

- მასალები, რომლებშიც მოყვანილია დამატებითი მნიშვნელოვანი და საინტერესო ინფორმაცია

  მითითებულია 

  ნიშნით;

- ყოველი თავის ბოლოში დასკვნებს და კითხვებს თან

  ახლავს 

  ნიშანი.

თავი 1

რა არის ქსელი

ამ თავში
თქვენ ნახავთ პასუხებს
შემდეგ კითხვებზე:

- რა არის ქსელი?
- როგორი ტიპის ქსელებია შესაძლებელი?
- როგორია ერთრანგიანი და სერვერის საფუძველზე ქსელების თავისებურებები?
- რა არის კომბინირებული ქსელები?
- როგორი აპარატურული და პროგრამული საშუალებებია საჭირო კომპიუტერებს შორის ურთიერთქმედების უზრუნველსაყოფად?

შევეცადოთ წარმოვიდგინოთ მსოფლიო მიახლოებით ოცდათხუთმეტი - ორმოცი წლის წინათ. მსოფლიო, საყოველთაოდ ხელმისაწვდომი კომპიუტერული ქსელების გარეშე. მსოფლიო, რომელშიც თითოეულ კომპიუტერს უნდა ჰქონოდა საკუთარი მონაცემების საცავი და საკუთარი პრინტერი. მსოფლიო, რომელშიც არ იყო ელექტრონული ფოსტა და მყისიერი შეტყობინებების გაცვლის სისტემები (მაგალითად, ICQ). რაც არ უნდა უცნაურად ჟღერდეს, კომპიუტერული ქსელების გამოჩენამდე ყოველივე ასე იყო.

კომპიუტერები - დღევანდელი მსოფლიოს მნიშვნელოვანი ნაწილია, ხოლო კომპიუტერული ქსელები აადვილებენ ჩვენს ცხოვრებას, აჩქარებენ სამუშაოს შესრულებასა და ხდიან დასვენებას უფრო საინტერესოს. დღეს ტელეკომუნიკაციური მოწყობილობები (ტელეფონი და სხვა) სულ უფრო ემსგავსება კომპიუტერს. ამ წიგნის შემწეობით თქვენ გაიგებთ, როგორაა მოწყობილი და როგორ მუშაობენ კომპიუტერული ქსელები, ისწავლით მათ დაპროექტებასა და შექმნას, აითვისებთ მუშაობას ყველაზე პოპულარულ ქსელურ გამოყენებებთან.

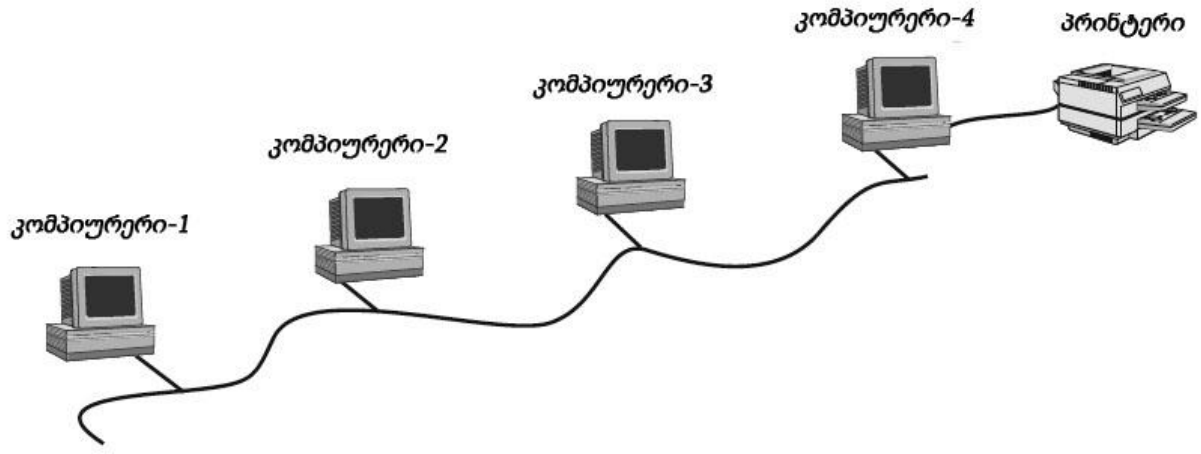
ელექტრონული გამომთვლელი მანქანების გამოჩენის შემდეგ პრაქტიკულად მაშინვე წამოიჭრა კომპიუტერების ერთმანეთთან ურთიერთქმედების აწყობის საკოთხი იმისათვის, რომ უფრო ეფექტურად დავამუშოთ ინფორმაცია და გამოვიყენოთ პროგრამული და აპარატურული რესურსები. გამოჩნდა პირველი ქსელებიც, რომლებიც აერთიანებდენ დიდ ეგმ-ს დიდ კომპიუტერულ ცენტრებში. მაგრამ ნამდვილი ”ქსელური ბუმი” დაიწყო პერსონალური კომპიუტერის გამოჩენასთანავე, გახდნენ რა სწრაფად ხელმისაწვდომი მომხმარებლების ფართო წრისათვის - ჯერ სამსახურში, შემდგომ სახლშიც. დაიწყო კომპიუტერების გაერთიანება ლოკალურ ქსელებში, ხოლო ლოკალური ქსელების - ერთმანეთთან შეერთება, მიერთება რეგიონალურ და გლობალურ ქსელებთან. შედეგად, ბოლო თხუთმეტი-ოცი წლის განმავლობაში მსოფლიოში ასობით მილიონი კომპიუტერი გაერთიანდა ქსელებში, და მილიარდზე მეტმა მომხმარებელმა მიიღო ერთმანეთთან ურთიერთობის საშუალება.

დღეს თამამად შეიძლება ითქვას, რომ კომპიუტერული ქსელები გახდნენ ჩვენი ცხოვრების განუყრელი ნაწილი, ხოლო მათი გამოყენების არე მოიცავს ადამიანის საქმიანობის პრაქტიკულად ყველა სფეროს.

ქსელი (Network) - ინფორმაციის გასაცვლისა და რესურსების ერთობლივად გამოყენებისათვის ერთმანეთთან ფიქსირებულად ან/და მობილურად დაკავშირებულ კომპიუტერების ჯგუფი.

წარმოიდგინეთ, რომ თქვენ გაქვთ რამოდენიმე, ერთმანეთთან ქსელით დაუკავშირებელი კომპიუტერი. იმისათვის, რომ ასეთ *ავტონომიურ* გარემოში იმუშაოთ ერთიდაიგივე მონაცემებთან, ერთი კომპიუტერის ფაილების ასლები უნდა მოვათავსოდ რაღაც მატარებლზე (მაგალითად, დისკეტაზე), რის შემდეგ გადავიტანოთ ეს ფაილები სხვა კომპიუტერებზე. ხოლო საბუთების სწრაფი ამობეჭდვისათვის მოგვიწევს ყოველი კომპიუტერის აღჭურვა ცალკეული პრინტერით. რამოდენიმე მომხმარებლის ერთდროული მუშაობა ერთნაირ საბუთებთან ასეთ ვითარებაში უბრალოდ გამორიცხულია.

ახლა შევაერთოთ კომპიუტერები ქსელში (ნახ. 1.1) და ავაწყოთ საერთო შეღწევა მოთხოვნილ რესურსებთან. აღმოჩნდება, რომ ჩვენ დისკეტები უკვე აღარ გვესაჭიროება, პრინტერიც დაგვჭირდება მხოლოდ ერთი. მომგებიანიცაა და მოხერხებულიც!

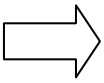


ნახ. 1.1. უმარტივესი ქსელი: რამოდენიმე კომპიუტერი და საერთო პრინტერი.

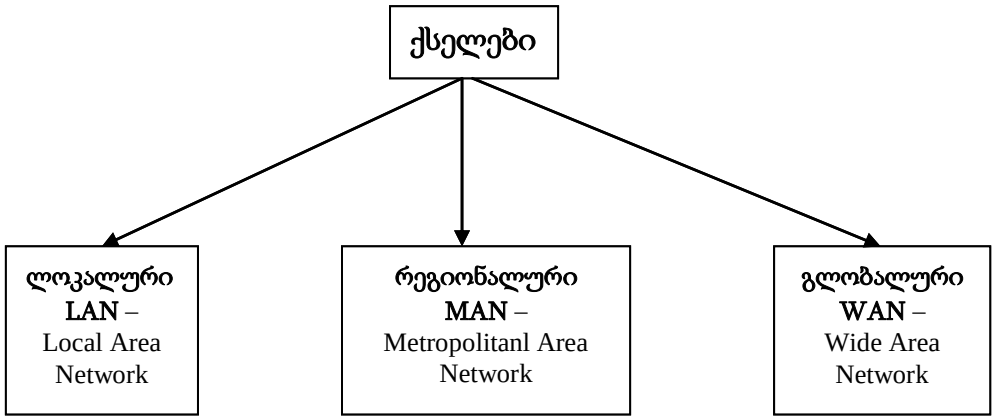
რესურსი - პროგრამები, მონაცემთა ფაილები, აგრეთვე პრინტერები და ქსელში სხვა ერთობლივად მოხმარებადი პერიფერიული მოწყობილობები.

ქსელების სხვადასხვა ტიპები

შესაძლებელია კომპიუტერული ქსელების კლასიფიკაციის მრავალი სხვადასხვა ხერი. აქ ჩვენ განვიხილავთ მათგან მხოლოდ ძირითადებს.



შემაკავშირებელ კვანძებს შორის მანძილების მიხედვით ქსელები შეიძლება დაიყოს სამ ძირითად კლასად: *ლოკალურად, რეგიონალურად* და *გლობალურად* (ნახ. 1.2).



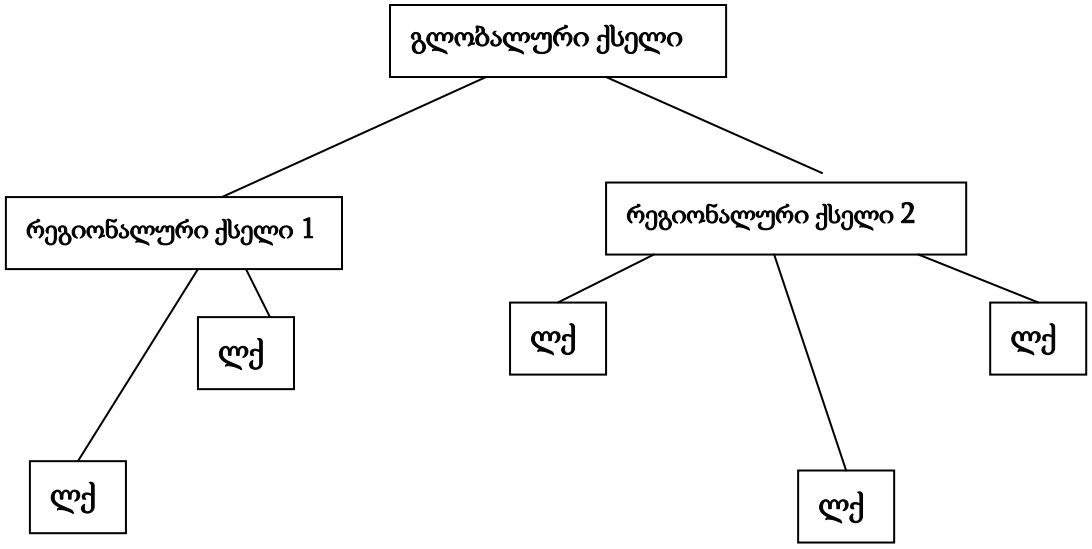
ნახ. 1.2. ქსელების კლასიფიცირება კვანძებს შორის მანძილებით.

ლოკალური ქსელი (ლქ) - ერთმანეთთან დაკავშირებული და, ჩვეულებრივ, ერთი შენობის ან ორგანიზაციის ფარგლებში განლაგებული კომპიუტერების მცირე ჯგუფი.

რეგიონალური ქსელი - ქსელი, რომელიც აერთიანებს ბევრ ლოკალურ ქსელს ერთი რაიონის, ქალაქის ან რეგიონის ფარგლებში.

გლობალური ქსელი - ქსელი, რომელიც აერთიანებს სხვადასხვა ქალაქების, რეგიონების და სახელმწიფოების კომპიუტერებს.

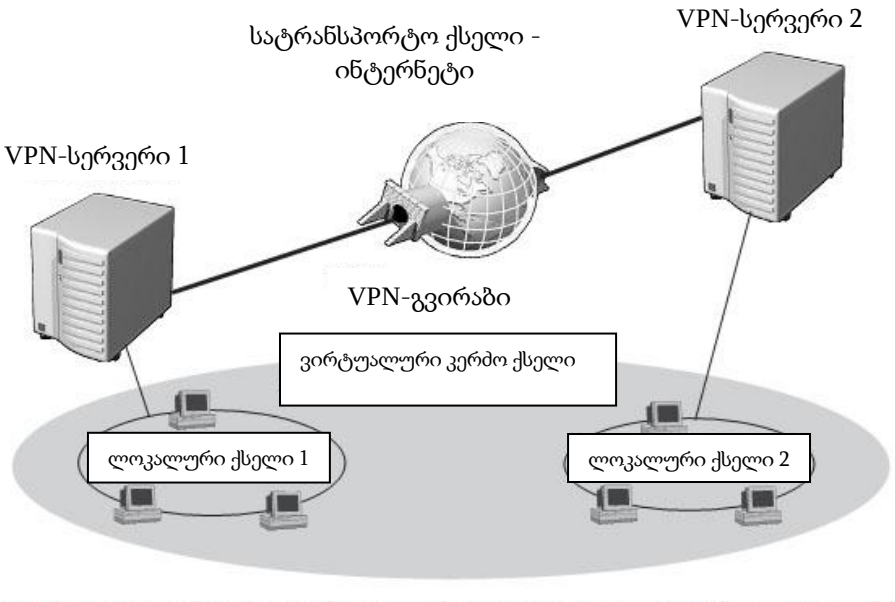
გლობალური, რეგიონალური და ლოკალური ქსელების გაერთიანება იძლევა მრავალდონიანი იერარქიების შექმნის საშუალებას, რომლებიც იძლევიან მონაცემთა უზარმაზარი მასივების დამუშავებისა და ინფორმაციული რესურსებისადმი პრაქტიკულად შეუზღუდავი ხელმისაწვდომობის მძლავრ საშუალებებს. ქსელების შესაძლო იერარქია მოყვანილია ნახ. 1.3-ზე.



ნახ. 1.3. ქსელების გაერთიანების მაგალითი.

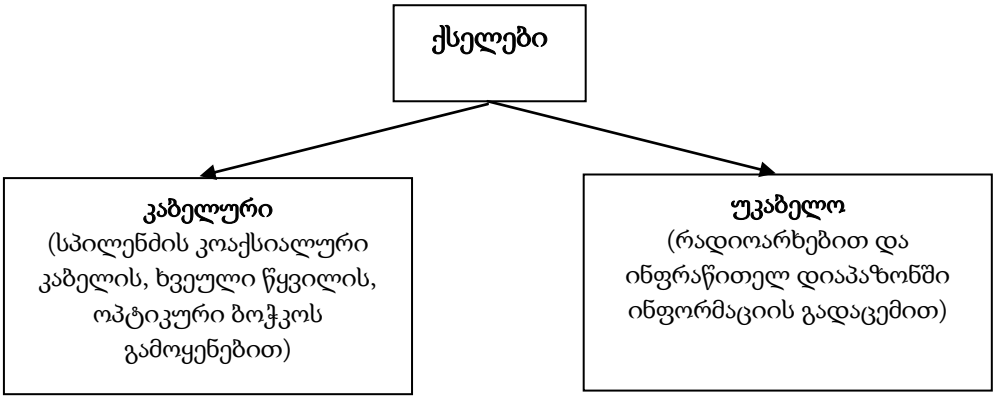
ლოკალური ქსელები (ლქ) შეიძლება შედიოდნენ რეგიონულ ქსელებში კომპონენტების სახით; რეგიონალური ქსელები - გაერთიანდნენ გლობალური ქსელის შემადგენლობაში; დაბოლოს, გლობალურმა ქსელებმა შეიძლება შექმნან უფრო მსხვილი სტრუქტურები. პლანეტა დედამიწის მასშტაბით დღეისათვის კომპიუტერული ქსელების ყველაზე დიდი გაერთიანებაა "ქსელთა ქსელი" - *ინტერნეტი*.

ლოკალური და გლობალური ქსელების გაერთიანების საინტერესო მაგალითია *ვირტუალური კერძო ქსელი* (*Virtual Private Network, VPN*). ასე ეწოდება ორგანიზაციის ქსელს, რომელიც მიიღება ორი ან რამოდენიმე ტერიტორიულად განცალკევებული ლოკალური ქსელის გაერთიანებით საყოველთაოდ ხელმისაწვდომი გლობალური ქსელების არხების დახმარებით, მაგალითად, ინტერნეტით (ნახ. 1.4).



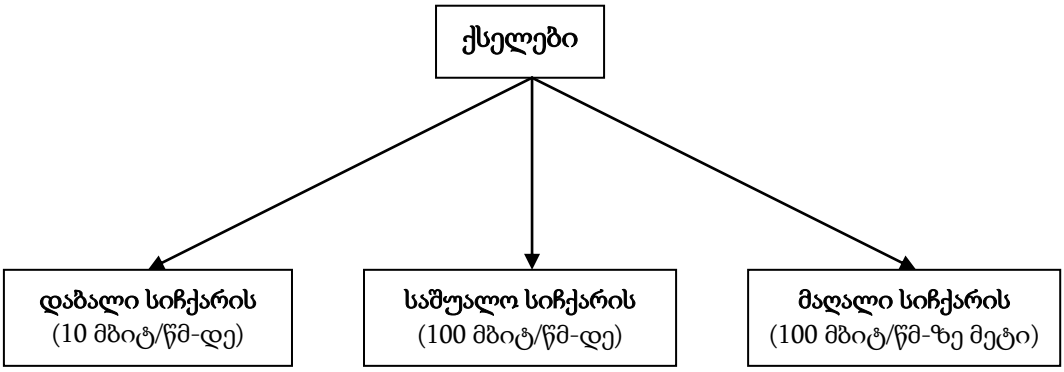
ნახ. 1.4. ვირტუალური კერძო ქსელი - ინტერნეტით გაერთიანებული წარმოების რამოდენიმე ლოკალური ქსელი.

მონაცემების გადაცემის ტიპის მიხედვით ქსელები იყოფიან *კაბელურ* და *უკაბელო* ქსელებად (ნახ. 1.5).



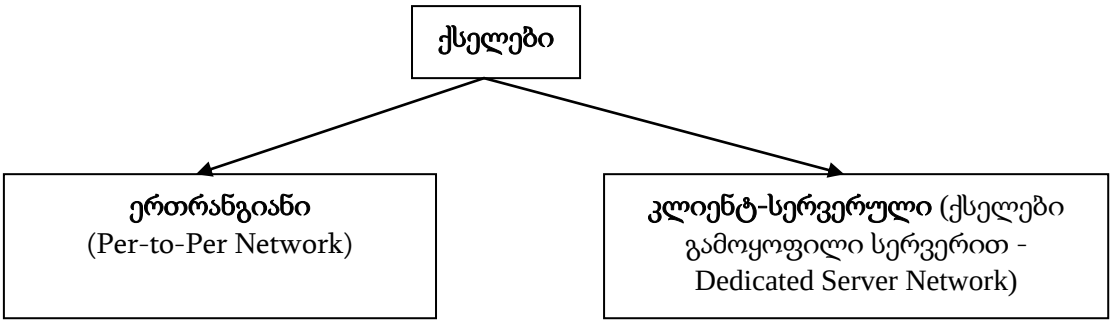
ნახ. 1.5. ქსელების კლასიფიცირება გადაცემის გარემოს მიხედვით.

ინფორმაციის გადაცემის სიჩქარის მიხედვით ქსელები შეიძლება დავყოთ *დაბალი*, *საშუალო*, და *მაღალი სიჩქარის* ქსელებად (ნახ. 1.6).



ნახ. 1.6. ქსელების კლასიფიცირება ინფორმაციის გადაცემის სიჩქარით

კომპიუტერებს შორის როლების განაწილების თვალსაზრისით ქსელები არსებობენ *ერთრანგიანი* და *კლიენტ-სერვერული* (ნახ. 1.7).



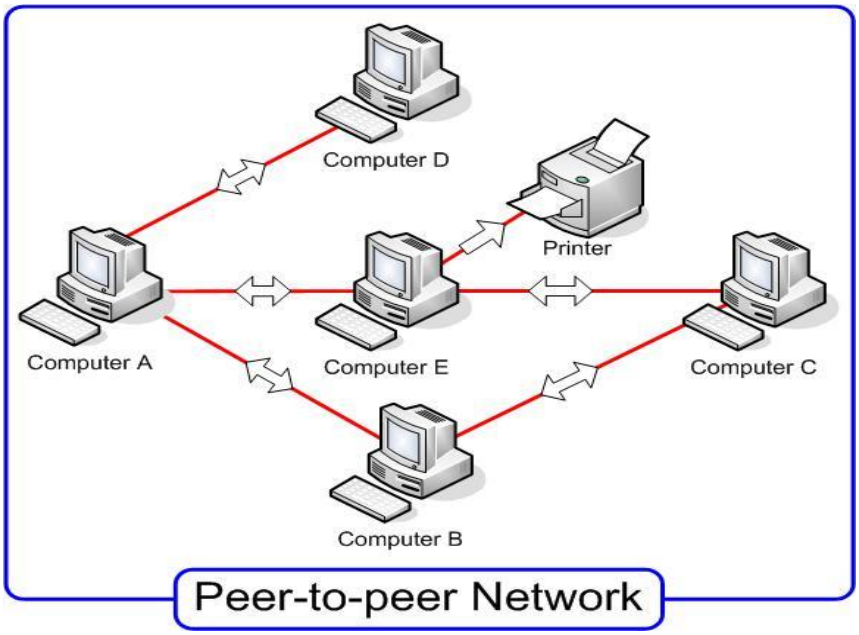
ნახ. 1.7. ქსელების კლასიფიკაცია კომპიუტერებს შორის როლების განაწილების მიხედვით

რადგან ერთრანგიანი და კლიენტ-სერვერული ქსელების ცნებები ძალიან მნიშვნელოვანია, განვიხილოთ ისინი უფრო დაწვრილებით.

ერთრანგიანი ქსელები

ერთრანგიან ქსელში (ნახ. 1.8) ყველა კომპიუტერი თანასწორ-უფლებიანია. ყოველ მათგანს შეუძლია შეასრულოს როგორც სერვერის როლი, ე. ი. მიაწოდოს ფაილები და აპარატურული რესურსები (დამგროვებლები, პრინტერები და სხვა) დანარჩენ კომპიუტერებს, ასევე კლიენტის როლი, რომელიც სარგებ-

ლობს სხვა კომპიუტერების რესურსებით. მაგალითად, თუ თქვენს კომპიუტერზე დაყენებულია პრინტერი, მაშინ მისი დახმარებით ქსელის დანარჩენ მომხმარებლებს შეუძლიათ ამობეჭდონ თავისი დოკუმენტები, ხოლო თქვენ, თავის მხრივ, შეგეძლებათ იმუშაოთ ინტერნეტთან, რომელთანაც მიერთებული ხართ მეზობელი კომპიუტერით.



ნახ. 1.8. ერთრანგიანი ქსელის მაგალითი

ქსელის ადმინისტრატორი - ადამიანი, რომელსაც გააჩნია ქსელში კომპიუტერების, მომხმარებლური მოწყობილობების და რესურსების მართვის ყველა უფლებამოსილებები.

ქსელის ადმინისტრირება - კომპიუტერების, ქსელური და მომხმარებლური მოწყობილობების მუშაობის მართვის, მონაცემების დაცვის, რესურსებისადმი შეღწევის უზრუნველყოფისა და სისტემური და გამოყენებითი პროგრამული უზრუნველყოფის დაყენებისა და მოდერნიზაციის ამოცანების მთელი კომპლექსის გადაწყვეტა.

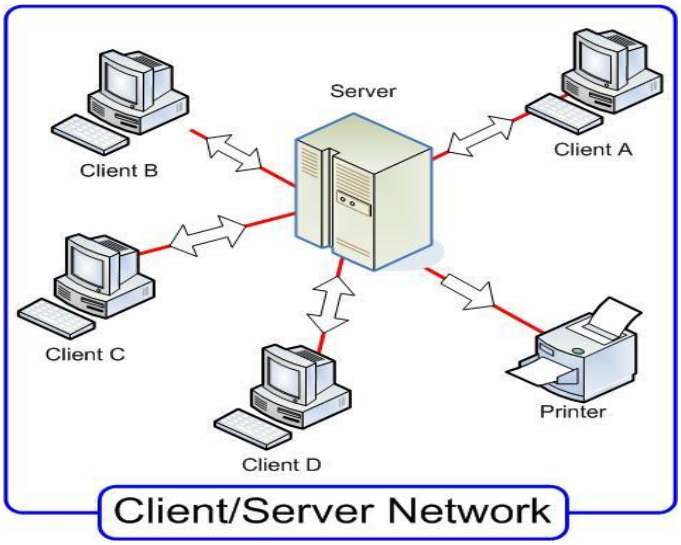
ერთრანგიანი ქსელების უპირატესობები და ნაკლოვანებები

უპირატესობები	*ნაკლოვანებები*
V გაშლის და აწყობა-გამართვის სიმარტივე;	X იმდენი პაროლის დამახსოვრების აუცილებლობა, რამდენი დამოუკიდებელი რესურსიცაა (ქსელებისათვის Windows 95/96 საფუძველზე), ან შესვლისათვის საჭირო სახელებისა და პაროლების დამახსოვრება (ქსელებისათვის Windows NT/2000/XP საფუძველზე);
V ცალკეული კომპიუტერებისა და მათი რესურსების ერთმანეთისგან დამოუკიდებლობა;	
V მომხმარებლისათვის საკუთარი კომპიუტერის რესურსების კონტროლირების საშუალება;	X ყოველ კომპიუტერზე ცალკე სარეზერვო კოპირების განხორციელების აუცილებლობა, იმისათვის რომ დაცულ იქნას ერთობლივად გამოყენებადი მონაცემები;
V გაშლისა და მხარდაჭერის შედარებით დაბალი ღირებულება;	
V დამატებითი პროგრამული უზრუნველყოფის აუცილებლობის არარსებობა;	X ქსელის ცენტრალიზებული მართვისა და მონაცემებისადმი ხელმისაწვდომობის შესაძლებლობის არარსებობა;
V ქსელის ადმინისტრატორის გამუდმებული ყოფნის აუცილებლობის არარსებობა.	X როგორც შედეგი - ქსელის და მონაცემების დაბალი დაცულობა

ერთრანგიან ქსელებში კომპიუტერების რაოდენობა ჩვეულებრივად არ აღემატება 10-ს - აქედან მათი სხვა სახელწოდებაც - *მუშა ჯგუფი*. მუშა ჯგუფების ტიპიური მაგალითებია საშინაო ან მცირე ოფისების ქსელები.

ქსელები გამოყოფილი სერვერით ("კლიენტ-სერვერ" ტიპის ქსელები)

ქსელები, როგორც წესი, იქმნება დაწესებულებებში ან მსხვილ ორგანიზაციებში. ასეთ ქსელებში (ნახ. 1.9) ხდება ერთი ან რამოდენიმე კომპიუტერის გამოყოფა - ე. წ. *სერვერების*, რომლის ამოცანა მდგომარეობს სხვა კომპიუტერების - *კლიენტების* მრავალრიცხოვანი მოთხოვნების სწრაფ და ეფექტურ დამუშავებაში. ამავე დროს *კლიენტური მოთხოვნები* შეიძლება იყოს სრულიად განსხვავებული, დაწყებული უმარტივესით - სისტემაში შესვლისას მომხმარებლის სახელის და პაროლის შემოწმებით, დამთავრებული მონაცემთა ბაზებისადმი რთული საძიებო მოთხოვნებით, რომელთა დამუშავებას თანამედროვე მრავალპროცესორიანმა კომპიუტერმაც კი შეიძლება რამოდენიმე საათი მოანდომოს.



ნახ. 1.9. გამოყოფილი სერვერით ქსელის მაგალითი

სერვერი - სპეციალურად გამოყოფილი მაღალმწარმოებლური კომპიუტერი, აღჭურვილი შესაბამისი პროგრამული უზრუნველყოფით, რომელიც ცენტრალიზებულად მართავს ქსელის მუშაობას და/ან აწვდის ქსელის სხვა კომპიუტერებს თავის რესურსებს (მონაცემთა ფაილებს, დამგროვებლებს, პრინტერს და ა. შ.).

კლიენტური კომპიუტერი (კლიენტი, მუშა სადგური) - ქსელის რიგითი მომხმარებლის კომპიუტერი, რომელიც ღებულობს დაშვებას სერვერის (სერვერების) რესურსებისადმი.

ჩვეულებრივ სერვერის როლში გვევლინებიან უფრო მძლავრი და საიმედო კომპიუტერები, ვიდრე მომხმარებლური მუშა სადგურები. სერვერები ხშირად აღიჭურვებიან სპეციალიზირებული მოწყობილობებით, მაგალითად მონაცემთა ტევადი საცავებით (მყარი დისკოებით და მათ საფუძველზე ე. წ. ”როუდ-მასივებით”), სარეზერვო კოპირებისათვის მაგნიტურ ფირზე დამგროვებლებით, მაღალსიჩქარიანი ქსელური ადაპტერებით და ა. შ. ასეთი კომპიუტერები მუშაობენ მუდამ, დღედაღამივად აწვდიან მომხმარებლებს თავიანთ რესურსებს და უზრუნველყოფენ მათ დაშვებას თავიანთი სამსახურებისადმი.

კლიენტ-სერვერული ქსელების უპირატესობები და ნაკლოვანებები

უპირატესობები	*ნაკლოვანებები*
V მძლავრი სერვერული მოწყობილობების გამოყენებით რესურსებისადმი სწრაფი შეღწევისა და კლიენტური მოთხოვნების ეფექტური დამუშავების საშუალება;	X სერვერის გაუმართაობა იწვევს პრაქტიკულად მთელი ქსელის ქმედითუუნარობას და რესურსების - მიუწვდომლობას;
V მონაცემებისა და რესურსების ცენტრალიზაციით ინფორმაციისა და მომხმარებლური მონაცემების მკაფიო მართვის აწყობის საშუალება;	X გაშლისა და მხარდაჭერის სირთულე მოითხოვს კვალიფიცირებული პერსონალის არსებობას, რაც ზრდის ქსელის მომსახურების საერთო ღირებულებას;
V სერვერზე მონაცემების განლაგებით სარეზერვო კოპირების პროცედურის საგრძნობი გაამარტივება;	X გამოყოფილი მოწყობილობებისა და სპეციალიზირებული პროგრამული უზრუნველყოფის მოთხოვნილების გამო ქსელის თანხლების ღირებულების ზრდა;
V ქსელის საერთო დაცულობის გაზრდა და მონაცემთა შენახვის უზრუნველყოფა.	X ერთ (უფრო ხშირად კი - რამოდენიმე) სამუშაო ადგილზე მუდმივად მყოფი ადმინისტრატორის საჭიროება.

სამსახურები (Services) – სერვერებზე მომუშავე პროგრამები, რომლებიც ასრულებენ რაიმე ქმედებებს კლიენტის მოთხოვნით.

როგორ ლაპარაკობენ კომპიუტერები ერთმენეთთან ქსელით?

დაბოლოს, მოკლედ განვიხილოთ როგორ ურთიერთქმედებენ ერთმანეთთან კომპიუტერები ქსელში. ასეთი მუშაობა რომ იყოს შესაძლებელი, ჯერ როგორღაც უნდა შევაერთოთ ქსელის ყველა მონაწილე - სერვერები, მომხმარებლების სტაციონარული მუშა სადგურები, *ნოუთბუკები, ჯიბის პერსონალური კომპიუტერები* (*ჯპკ*), მონაცემთა ქსელური საცავები და ა. შ. ამ მიზნებისათვის გამოიყენება სხვადასხვა ტიპის *ქსელური კაბელები, სატელეფონო* ან *თანამგზავრული არხები*, ბოლო დროს კი სულ უფრო პოპულარული ხდება *უკაბელო*

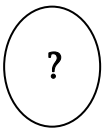
დღეისათვის რამოდენიმე კომპანიამ (მაგალითად, Microsoft და Hewlett-Packard-მა ერთობლივად) წარმოადგინეს ე. წ. დაფური (tablet–ური, პლანშეტური) კომპიუტერები, რომლებიც შეიძლება წარმოვიდგინოთ როგორც ლეპტოპისა და სმარტფონის ჰიბრიდი. ისინი იძლევიან ინტერნეტში მუშაობის საშუალებას 3G მობილური და Wi-Fi, WiMAX, LTE (4G) უკაბელო ქსელებით Windows Phone 7 და სხვა ოპერაციული სისტემის ხელმძღვანელობით.

გადაწყვეტილებები (WLAN, Wi-Fi, WiMAX, LTE). კაბელების გამოყენებისას ჩვეულებრივად საჭიროა სპეციალური *კონექტორები*, რომლებიც დამაგრებულია მათ ბოლოებზე. შემდეგ კაბელი ერთი ბოლოთი ჩაისმება *ქსელურ ადაპტერში* - სპეციალურ პლატაში (*network interface cards*), რომელიც დაყენებულია კომპიუტერზე და საშუალებას იძლევა მივუერთოთ ის ქსელს, ხოლო მეორე ბოლოთი - *კავშირგაბმულობის* რომელიმე *მოწყობილობაში* (კონცენტრატორი, ხიდი, კომუტატორი, მარშრუტიზატორი, რაბი და ა. შ.). თანამედროვე კომპიუტერების უმრავლესობაში ქსელური ადაპტერი ჩაშენებულია (შესაბამისი გასართი უშუალოდ Motherboard-ზე). თუკი გამოიყენება *უკაბელო ქსელური ადაპტერი*, მაშინ ქსელთან ურთიერთქმედება ხდება რადიოსიგნალების გადაცემით ადაპტერსა და ქსელთან შეერთებულ *შეღწევის წერტილს* შორის.

მაგრამ კომპიუტერების ერთმანეთთან შეერთება არ არის საკმარისი - ჯერ მათ უნდა "ვასწავლოთ ერთმანეთთან ლაპარაკი". ამისათვის საჭიროა *ქსელური ოპერაციული სისტემები*, რომლებიც მხარს უჭერენ *პროტოკოლების* ერთიდაიგივე *კრებულს*, ანუ ენებს, და რომელთა დახმარებით კომპიუტერები ურთიერთობენ ქსელში. მხოლოდ ამის შემდეგ, ავამოქმედებთ რა *ქსელურ გამოყენებს*, შეიძლება მოვახერხოთ, მაგალითად, ურთიერთობა მეგობართან, რომელიც იმყოფება დედამიწის სულ სხვა „ბოლოში".

მიზეზი, რისთვისაც ქსელური პროტოკოლები ესაჭიროებათ კომპიუტერებს, ისეთივეა, როგორც გარკვეული წესები - ადამიანებს ურთიერთობისათვის. თუ საგანს, რომელზაც სხედხართ თქვენ უწოდებთ სკამს, ხოლო თქვენი მეზობელი - კლდეს, მასთან ურთიერთობა გაგიჭირდებათ. ხერხებს, რომლებითაც ადამიანები ურთიერთობენ ერთმანეთთან ასევე ესაჭიროება წესების მთელი რიგი. მაგალითად, თუ თქვენ ცხოვრობთ საზოგადოებაში, სადაც მისალმებას გამოხატავენ ლოყაზე ხელის მოსმით, ეს დიდ გაუგებრობას გამოიწვევს საქართველოში, სადაც თავაზიანი მისალმების პროტოკოლი ითხოვს ხელის ჩამორთმევას. იაპონიაში მისალმების პროტოკოლი მოითხოვს თავის დაკვრას. პროტოკოლები ეხმარებიან ადამიანებს ურთიერთობაში, კომპიუტერული პროტოკოლები კი ეხმარებიან კომპიუტერებს ერთმანეთთან ურთიერთქმედებაში. ამის შესახებ თქვენ წაიკითხავთ შემდეგ თავებში.

კითხვები და დავალებები



1. რა არის ქსელი?
2. როგორი ტიპის ქსელები იცით?
3. როგორ უპირატესობებს იძლევა ქსელი?
4. რა არის ერთრანგიანი ქსელი? როგორია მისი უპირატესობები და ნაკლოვანებები?
5. რა არის ”კლიენტ-სერვერული” ქსელი? როგორია მისი უპირატესობები და ნაკლოვანებები?
6. რას გულისხმობს ცნება ”ქსელის ადმინისტრირება”?
7. როგორი აპარატურული და პროგრამული საშუალებებია საჭირო ქსელში კომპიუტერების ურთიერთქმედების უზრუნველსაყოფად?
8. დაახასიათეთ თქვენი სასწავლო დაწესებულების ქსელი.
9. დახატეთ თქვენი კომპიუტერული კლასის ლოკალური ქსელის სქემა.
10. როგორაა ორგანიზებული თქვენი სასწავლო დაწესებულების ლოკალური ქსელის ადმინისტრირება? რამდენი პკ შედის თქვენი სასწავლო დაწესებულების ქსელში?

თავი 2

როგორ „ლაპარაკობენ“ კომპიუტერები ერთმანეთთან ქსელით?

ამ თავში თქვენ ნახავთ პასუხებს შემდეგ კითხვებზე:

- **რა არის ეტალონური მოდელი OSI?**
- **როგორია OSI მოდელის ყოველი დონის ფუნქცია?**
- **როგორ განვმარტოთ OSI მოდელის დონეები, რომლებზედაც ხორციელდება კონკრეტული ქსელური ოპერაციები?**
- **OSI მოდელის როგორი გაფართოებებია შესაძლებელი IEEE-ს მხრიდან?**

წინა თავში ჩვენ გავიგეთ რა არის კომპიუტერული ქსელი, გავეცანით ქსელების ძირითად ტიპებს და გავიგეთ, როგორ ურთიერთობენ ერთმანეთთან ქსელში კომპიუტერები (უფრო ზუსტად, მათზე მომუშავე პროგრამები). ახლა განვიხილოთ უფრო დაწვრილებით ქსელში კომპიუტერების ურთიერთქმედების ძირითადი პრინციპები.

ადამიანები ურთიერთობისათვის ხშირად მიმართავენ ზეპირსიტყვიერებას. ასეთი უშუალო ურთიერთობა შესაძლებელია თუ მოსაუბრეები იმყოფებიან საჰაერო გარემოში ერთმანეთის გვერდით. წარმოიდგინეთ, მონაცემები უნდა გადასცეთ მეგობარს, რომელიც ცხოვრობს სხვა ქალაქში, ან უფრო მეტიც - სხვა ქვეყანაში. აქ უკვე გვერდს ვერ ავუვლით მთელ რიგ ქმედებებს: ქაღალდის ფურცელზე უნდა დაწეროთ ტექსტი, მოაწეროთ ხელი, ჩადოთ კონვერტში, მიუთითოთ მასზე გამგზავნის და მიმღების მისამართები, დააწებოთ მარკა და მისცეთ ფოსტალიონს (ან ჩააგდოთ საფოსტო ყუთში). ამის შემდეგ წერილის ბედ-იღბალი თქვენზე უკვე არაა დამოკიდებული, არამედ - საფოსტო სამსახურზე. როგორმე - მატარებლით, გემით თუ თვითმფრინავით - ასე თუ ისე, წერილი მიაღწევს ქვეყანას და ქალაქს, რომელშიც ცხოვრობს თქვენი მეგობარი, შემდეგ მიეწოდება მის საფოსტო განყოფილებას დაბოლოს მოხვდება მის საფოსტო ყუთში. მხოლოდ ყოველივე ამის შემდეგ შეძლებს თქვენი მეგობარი კონვერტის გახსნას და თქვენი შეტყობინების წაკითხვას. თუ მიტანის რომელიმე სტადია ვერ იმუშავებს, მაგალითად, ფოსტალიონის არარსებობის გამო ან სხვადასხვა ქვეყნებში მისამართების ჩაწერის განსხვავებულობის გამო, ინფორმაცია თქვენს მეგობრამდე ვერ მიაღწევს.

ზუსტად ასევე იქცევიან კომპიუტერები ქსელში მუშაობისას. უშუალო ურთიერთობის ხერხები ადამიანებივით, მათ არ გააჩნიათ. ერთმანეთთან საუბარი კომპიუტერებს ჯერჯერობით ვერ ასწავლეს. ამიტომ იურთიერთობისათვის ისინი მიმართავენ მთელ რიგ თანმიმდევრობით შესრულებად

პროცედურებს, რომლებსაც *ქსელურ პროტოკოლებს* უწოდებენ. იმისათვის, რომ პროტოკოლებმა იმუშაონ საიმედოდ და შეთანხმებულად, მათში ყოველი ოპერაცია მკაცრად რეგლამენტირებულია. ხოლო სხვადასხვა მწარმოებლის პროგრამებმა და მოწყობილობებმა რომ შეძლონ ერთმანეთთან ურთიერთქმედება პროტოკოლები უნდა შეესაბამებოდენ გარკვეულ *სამრეწველო სტანდარტებს.*

პროტოკოლი - წესებისა და პროცედურების კრებული, რომელიც აწესრიგებს ქსელში კომპიუტერების ურთიერთქმედებას.

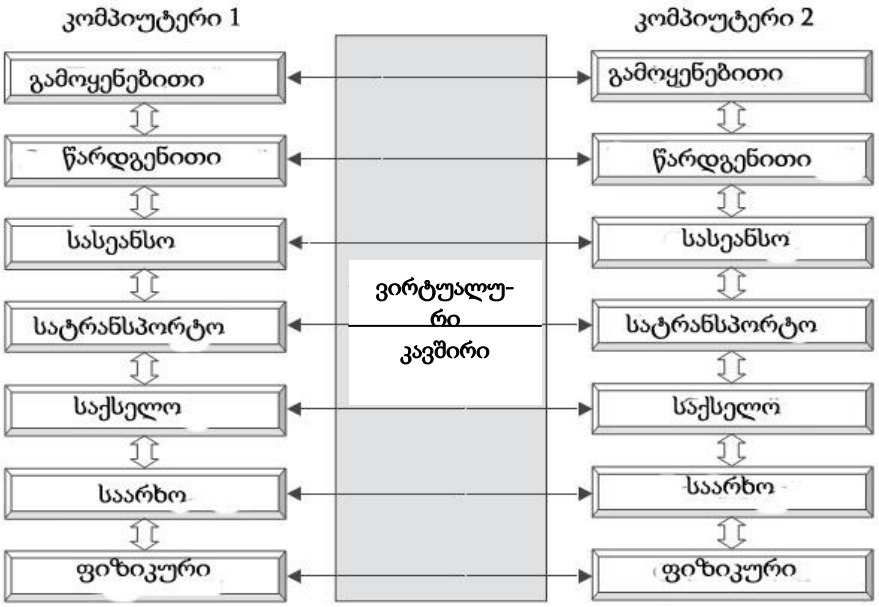
კომპიუტერული ქსელების მრავალწლიანი არსებობის განმავლობაში შეიქმნა უამრავი სხვადასხვა პროტოკოლი - როგორც ღია (გამოქვეყნებული უფასო მოხმარებისათვის), ასევე დახურული (შემუშავებული კომერციული კომპანიების მიერ და მათი სარგებლობისათვის აუცილებელია ლიცენზიის შეძენა). მაგრამ ყველა ამ პროტოკოლის შედარება მიღებულია ე. წ. *ღია სისტემების ურთიერთკავშირების ეტალონურ მოდელთან* (*Open Systems Interconnection Reference Model*), ან უბრალოდ - *OSI მოდელთან.* მისი აღწერა გამოქვეყნდა 1984 წელს სტანდარტიზაციის საერთაშორისო ორგანიზაციის მიერ (International Standards Organization, ISO), ამიტომ, ხშირად გამოიყენება სახელწოდება - *ISO/OSI მოდელი.* ეს მოდელი წარმოადგენს სპეციფიკაციების კრებულს, რომელიც აღწერს ქსელებს არაერთგვაროვანი მოწყობილობებით, მოთხოვნებს მათ მიმართ, და აგრეთვე მათ შორის ურთიერთქმედების წესებს.

OSI მოდელის სტრუქტურა

OSI მოდელს აქვს ვერტიკალური სტრუქტურა, რომელშიც ყველა ქსელური ფუნქცია განაწილებულია შვიდ *დონეს* შორის (ნახ. 2.1). ყოველ ასეთ დონეს შეესაბამება *მკაცრად განსაზღვრული ოპერაციები, მოწყობილობები* და *პროტოკოლები.*

დონეების რეალური ურთიერთქმედება, ე. ი. ინფორმაციის გადაცემა ერთი კომპიუტერის შიგნით, შესაძლებელია *მხოლოდ ვერტიკალით და მხოლოდ მეზობელ დონეებს შორის* (ზემოთ- და ქვემოთ განლაგებულებს შორის).

ლოგიკური ურთიერთქმედება (ამა თუ იმ პროტოკოლის წესების მიხედვით) *ხორციელდება ჰორიზონტალურად* - კავშირგაბმულობის ხაზის მეორე ბოლოზე *სხვა კომპიუტერის ანალოგიურ დონესთან*. OSI მოდელის ყოველი მაღალი დონე სარგებლობს უშუალოდ მის ქვემოთ მყოფი დონის მომსახურებით, იცის რა, როგორი სახით და როგორი წესით (ე. ი. როგორი *ინტერფეისით*) უნდა მიაწოდოს მას მონაცემები.



ნახ. 2.1. ურთიერთკავშირები OSI მოდელის დონეებს შორის

OSI მოდელის თითოეული ქვედა დონის ამოცანაა - მიიღოს მონაცემები ზედა დონიდან, დაამატოს თავისი ე. წ. სამსახურეობრივი ინფორმაცია (მაგალითად, მაფორმატირებელი ან სამისამართო, რომელიც საჭიროა ხაზის მეორე ბოლოზე კომპიუტერის ასეთივე დონესთან სწორი ურთიერთქმედებისათვის) და გადასცეს მონაცემები შემდეგს. მხოლოდ ქსელური მოდელის ყველაზე დაბალი, ფიზიკური დონის მიღწევისას, ინფორმაცია მოხვდება გადაცემის გარემოში და მიაღწევს კომპიუტერ-მიმღებს. სადაც ის საწინააღმდეგო მიმართულებით გაივლის ყველა „ფენას“, მანამ არ მიაღწევს იმ დონეს, საიდანაც გამოიგზავნა კომპიუტერ-გამგზავნიდან.

ყოველივე ეს ძალიან ჰგავს ჩვენს მაგალითს - პროგრამები ქსელით ურთიერთობენ ერთმანეთთან ისევე, როგორც თქვენ

მეგობართან ფოსტით. თქვენი ქაღალდის ფურცელი ტექსტით გადაიცემა ზედა დონიდან ქვევით, გაივლის რა მრავალ აუცილებელ სტადიას. ამასთანავე მას დაემატა სამსახურეობრივი ინფორმაცია (გარკვეული სახის კონვერტი, მისამართი კონვერტზე, საფოსტო ინდექსი) და განიცადა გარკვეული დამუშავება (ფოსტალიონი განყოფილებაში იღებს წერილს, აწებს კონვერტზე მარკებს, სვამს ბეჭედს, ხოლო დახარისხების შემდეგ ხვდება სხვა ქალაქში გადასაგზავნ კონტეინერში). ამგვარად თქვენი ინფორმაცია დავიდა ყველაზე დაბალ დონემდე - საფოსტო ტრანსპორტამდე, რომლითაც ის გადაიტანება დანიშნულების პუნქტში. იქ ხდება უკუ-პროცესი: გაიღება კონტეინერი, წაიკითხება მისამართი, რის შემდეგ ფოსტალიონს მიაქვს წერილი თქვენს მეგობართან. ამის შემდეგ თქვენი მეგობარი ღებულობს ინფორმაციას პირვანდელი სახით - როდესაც იღებს წერილს კონვერტიდან, ამოწმებს ხელწერას და კითხულობს ტექსტს.

ამგვარად, თქვენ მეგობართან *ლოგიკურად გაქვთ პირდაპირი კავშირი*, და მიტანის დეტალები დიდად არ გაწუხებთ. ფოსტალიონებს აგრეთვე აქვთ პირდაპირი კავშირი: უცხო ქალაქში იღებს ზუსტად იგივეს, რაც თქვენ გადაეცით თქვენს ფოსტალიონს - კონვერტს წერილით და სამისამართო ინფორმაციით. ფოსტალიონებს, ამასთან, არ აღელვებთ, მაგალითად, რკინიგზელების პრობლემები, რომლებიც სინამდვილეში ახორციელებენ კორესპონდენციის გადაზიდვას.

ახლა უფრო ახლო გავეცნოთ OSI მოდელის დონეებსა და განვსაზღვროთ ქსელური მომსახურებები, რომლებსაც ისინი აწვდიან მომიჯნავე დონეებს.

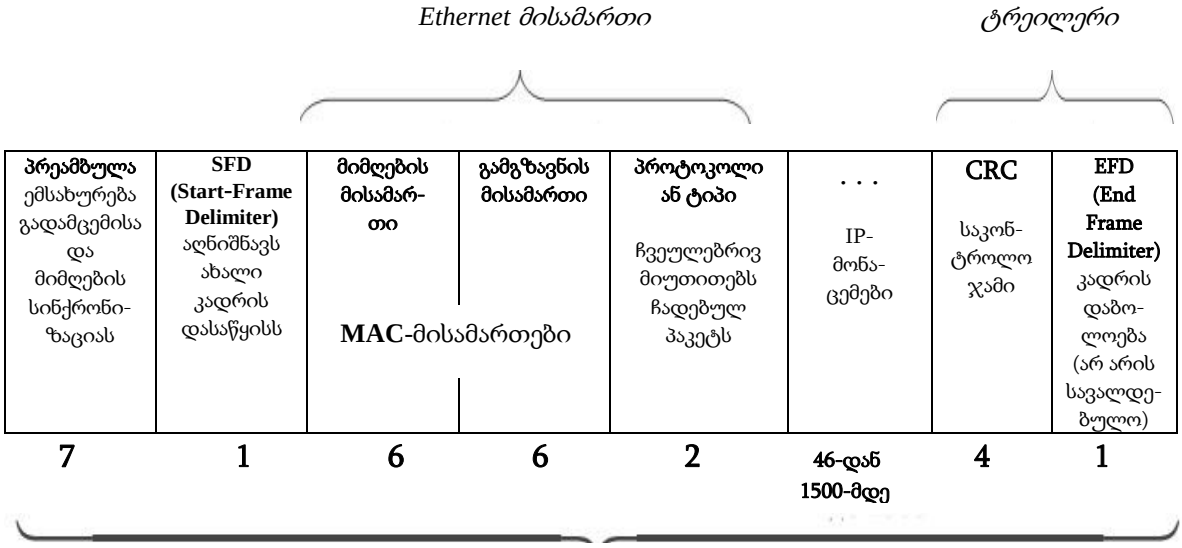
OSI მოდელის დონეები

დონე 0 - არ არის განსაზღვრული საერთო სქემაში (ნახ. 2.1-ზე), მაგრამ ერთობ მნიშვნელოვანია გაგებისათვის. აქ წარმოდგენილია შუამავლები, რომლებითაც ხდება სიგნალე-ბის გადაცემა: სხვადასხვა ტიპის კაბელები, რადიო-, ინფრაწითელი სიგნალები და ა. შ. ამ დონეზე არაფერი აღიწერება, 0 დონე აწვდის ფიზიკურ 1 დონეს მხოლოდ *გადაცემის გარემოს.*

დონე 1 - ფიზიკური (Physical). აქ ხორციელდება ზედა 2 დონიდან მიღებული ბიტების არასტრუქტურირებული ნაკადის გადაცემა ფიზიკური გარემოთი - მაგალითად, ელექტრული ან სინათლის სიგნალების სახით. ფიზიკური დონე *კავშირის მხარდაჭერის* (*Link*) პასუხისმგებელია და დეტალურად აღწერს ელექტრულ, ოპტიკურ, მექანიკურ და ფუნქციონალურ ინტერფეისებს გადაცემის გარემოსთან:

დაძაბულობებს, სიხშირეებს, ტალღის სიგრძეებს, კონექტორების ტიპებს, კონტაქტების რაოდენობასა და ფუნქციონალურობას, სიგნალების კოდირების სქემებს და ა. შ.

დონე 2 - საარხო (Date Link). უზრუნველყოფს ზემოდან, ქსელური 3-ე დონიდან მიღებული *მონაცემების უშეცდომო გადაცემას* პირველი ფიზიკური დონით, რომელიც თავის მხრივ არ იძლევა შეცდომების არქონის გარანტიებსა და შეუძლია დაამახინჯოს მონაცემები. ამ დონეზე ინფორმაცია თავსდება *კადრებში* (*Frame*), სადაც დასაწყისში (*კადრის სათაურში*) მოთავსებულია მიმღებისა და გამგზავნის მისამართები, აგრეთვე მმართველი ინფორმაცია, ხოლო ბოლოში - *საკონტროლო ჯამი*, რომელიც იძლევა გადაცემის დროს წარმოქმნილი შეცდომების გამოვლინების საშუალებას (ნახ. 2.2).



ნახ. 2.2. კადრის სტრუქტურა

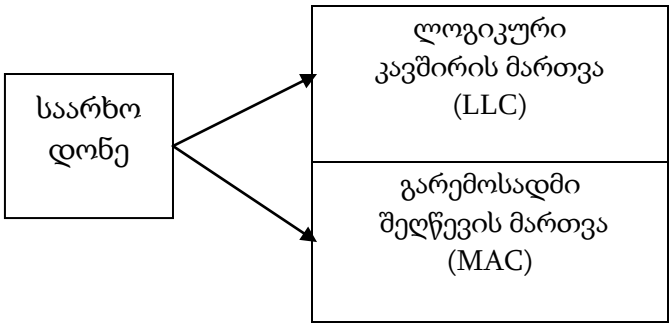
საარხო დონეზე *მონაცემების მიღებისას* ბიტების ნაკადში დგინდება კადრის დასაწყისი და ბოლო, ხდება ნაკადიდან თავად კადრის ამოღება და შემოწმება შეცდომების არსებობაზე. გადაცემისას დაზიანებული კადრები და აგრეთვე კადრები, რომელთათვის არაა მიღებული *დადასტურება მიღების შესახებ*, გადაიგზავნებიან ხელახლა (*რეტრანსლირდებიან*). დაბოლოს, საარხო დონეზე ხდება გადაცემის გარემოსადმი შეღწევის მართვის უზრუნველყოფა.

საარხო დონე საკმაოდ რთულია, ამიტომ IEEE (Institute Electrical and Electronics Engineers) სტანდარტების შესაბამისად,

რომელიც გამოშვებულია 1980 წლის თებერვალში "პროექტი 802"-ს ჩარჩოებში (*Project 802*), მას ხშირად ყოფენ ორ ქვედონედ (ნახ. 2.3): *გარემოსადმი შეღწევის მართვისა* (*Media Access Control*, *MAC*) და *ლოგიკური კავშირის მართვის* (*Logical Linc Control*, *LLC*).

MAC დონე უზრუნველყოფს ფიზიკური დონისადმი ქსელური ადაპტერების ერთობლივ შეღწევას, კადრების საზღვრების დადგენას, *კადრების დანიშნულებისეული მისამართების* ამოცნობას (ამ მისამართებს ხშირად *ფიზიკურს* ან *MAC-მისამართებს* უწოდებენ).

LLC დონე, რომელიც მოქმედებს MAC დონეს ზემოდან, პასუხისმგებელია კავშირგაბმულობის არხის დადგენაზე და მონაცემებიანი შეტყობინების უშეცდომო გაგზავნა-მიღებაზე.

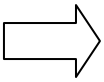


ნახ. 2.3. საარხო დონის გაყოფა MAC და LLC ქვედონეებად

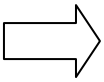
დონე 3 - ქსელური (Network). პასუხისმგებელია ქსელის ნებისმიერ ორ წერტილს შორის, თუნდაც დედამიწის სხვადასხვა "ბოლოში" *კავშირის უზრუნველყოფაზე*. ეს დონე ახორციელებს *შეტყობინების გაყვანას ქსელით*, რომელიც შეიძლება შედგებოდეს მრავალი ცალკეული ქსელისაგან, შეერთებული კავშირგაბმულობის მრავალი ხაზით. ასეთი მიტანა საჭიროებს *მარშრუტიზაციას*, ე. ი. *შეტყობინების მიტანის გზის დადგენას*, და აგრეთვე მონაცემთა ნაკადების მართვისა და გადაცემის შეცდომების დამუშავების ამოცანების გადაწყვეტას.

დონე 4 - სატრანსპორტო (Transport). იძლევა ერთი კომპიუტერიდან მეორესათვის *ინფორმაციის მიწოდების* გარანტიას. გამგზავნი კომპიუტერის ამ დონეზე მონაცემთა დიდი ბლოკები იშლება უფრო მცირე *პაკეტებად*, რომლებიც *საჭირო თანმიმდევრობით*, *დანაკარგებისა და დუბლირების გარეშე* მიეწოდება კომპიუტერ-მიმღებს. მიმღები

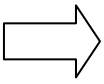
კომპიუტერის სატრანსპორტო დონეზე პაკეტები ხელახლა იკრიბება მონაცემთა თავდაპირველ ბლოკებად. ამგვარად, სატრანსპორტო დონე *ამთავრებს მონაცემთა გადაცემის პროცესს*, „უმალავს“ რა მის ზედა დონეებს ყველა დეტალს და პრობლემას, რომელიც დაკავშირებულია *ნებისმიერი მოცულობის* ინფორმაციის გადატანასთან მთელს ქსელში *ნებისმიერ წერტილებს შორის*.



დონე 5 - სასეანსო (Session). საშუალებას აძლევს ორ *ქსელურ გამოყენებას* სხვადასხვა კომპიუტერებზე დაამყაროს, შეინარჩუნონ და დაასრულონ შეერთება, რასაც *ქსელური სეანსი* ეწოდება. ეს დონე აგრეთვე პასუხისმგებელია ავარიულად შეწყვეტილი კავშირის აღდგენაზე. გარდა ამისა, მე-5-ე დონეზე ხდება ადამიანებისათვის მოსახერხებელი კომპიუტერების სახელების გარდაქმნა ქსელურ მისამართებად (*სახელების ამოცნობა*), და აგრეთვე ხორციელდება *სეანსის დაცვის* ფუნქცია.



დონე 6 - წარდგენითი, ან მონაცემთა წარდგენის დონე (Presentation). განსაზღვრავს კომპიუტერებს შორის გადაცემადი ინფორმაციის *ფორმატებს*. ამ დონეზე აგრეთვე ხდება ისეთი ამოცანების გადაწყვეტა, როგორიცაა *გადაკოდირება* (ინფორმაციის გადაყვანა სახეში, რომელიც გასაგებია გაცვლაში მონაწილე ყველა კომპიუტერისათვის), მონაცემთა შეკუმშვა და გახსნა, დაშიფრვა და განშიფრვა, ქსელური ფაილური სისტემის მხარდაჭერა და სხვა.

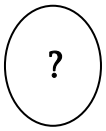


დონე 7 - გამოყენებითი (Application), ანუ გამოყენებათა დონე. უზრუნველყოფს ქსელის კომპიუტერებზე მომუშავე პროგრამების ურთიერთქმედების *ინტერფეისს*. სწორედ ამ პროგრამების დახმარებით ხდება ხელმისაწვდომი მომხმარებლისათვის ისეთი ქსელური მომსახურებები, როგორიცაა ფაილების გაცვლა, ელექტრონული ფოსტის გადაცემა, დაშორებული ტერმინალური შეღწევა და სხვა.

OSI მოდელის გამოჩენის მომენტისათვის უკვე არსებობდა *პროტოკოლების მაღალეფექტური კრებულები* (*სტეკები*), მაგალითად სტეკი *TCP/IP*. ამიტომ OSI პროტოკოლთა სტეკმა ფართო გავრცელება ვერ მოიპოვა. თანამედროვე ქსელური არქიტექტურებისა და პროტოკოლების კრებულების

უმრავლესობა მხოლოდ რამდენადმე შეესაბამება ამ მოდელს. მიუხედავად ამისა, თავად ISO/OSI მოდელი დღემდე ფართოდ გამოიყენება ქსელურ გარემოებებში ურთიერთქმედებების აღსაწერად.

კითხვები და დავალებები



11. როგორ გავიგოთ ტერმინი "ქსელური პროტოკოლი"?
12. როგორი ქსელური ფუნქციები ხორციელდება OSI მოდელში?
13. რომელი დონეა პასუხისმგებელი მონაცემების გადაცემის მარშრუტის არჩევაზე OSI მოდელის თანახმად?
14. OSI მოდელის რომელ დონეზე ურთიერთქმედებენ პროგრამები, რომლებიც უზრუნველყოფენ ელექტრონული ფოსტის შეტყობინებების გადაცემას?
15. იპოვეთ ინტერნეტში დამატებითი ინფორმაცია ქსელური კომუნიკაციების საერთაშორისო სტანდარტის "ღია სისტემების ურთიერთკავშირების ეტალონური მოდელის" შესახებ.

თავი 3

ქსელური ტოპოლოგიები და მონაცემთა გადაცემის გარემოსთან შეღწევის ხერხები

ამ თავში თქვენ ნახავთ პასუხებს შემდეგ კითხვებზე:

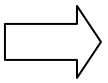
- **როგორი ქსელური ტოპოლოგიები არსებობენ?**
- **როგორია სხვადასხვა ტოპოლოგიების უპირატესობები და ნაკლოვანებები?**
- **როგორი ტიპის ქსელია ამჟამად ყველაზე პოპულარული?**
- **მონაცემთა გადაცემის გარემოსთან შეღწევის როგორი ხერხები (მეთოდები) არსებობს?**

კომპიუტერული ქსელის ორგანიზებისას განსაკუთრებით მნიშვნელოვანია ქსელური *ტოპოლოგიის* შერჩევა, ე. ი. *ქსელური მოწყობილობებისა და კაბელური ინფრასტრუქტურის ურთიერთშერწყმული კომპლექტაციის შერჩევა*. უნდა შევარჩიოთ ისეთი ტოპოლოგია, რომელიც უზრუნველყოფს ქსელის საიმედო და ეფექტურ მუშაობას, ქსელური მონაცემების ნაკადების მოხერხებულ მართვას. სასურველია აგრეთვე, რომ ქსელი, შექმნის ღირებულებით გამოვიდეს იაფი, მაგრამ ამავე დროს დარჩეს შესაძლებლობა მისი შემდგომი გაფართოებისათვის, და, სასურველია, ტელეკომუნიკაციის მაღალსიჩქარულ ტექნოლოგიებზე გადასვლისათვის.

ეს არ არის მარტივი ამოცანა! რომ გადავწყვიტოთ, საჭიროა ვიცოდეთ საერთოდ როგორი ქსელური ტოპოლოგიები არსებობს. ამავდროულად უნდა განვასხვაოთ ერთმანეთისაგან *ფიზიკური ტოპოლოგიის* ცნება, ე. ი. კომპიუტერების, ქსელური მოწყობილობებისა და მათი კაბელური ინფრასტრუქტურის დახმარებით შეერთების განლაგების ხერხისა, და *ლოგიკური ტოპოლოგიის* - კომპიუტერების ურთიერთქმედების სტრუქტურისა და ქსელით სიგნალების გავრცელების ხასიათით.

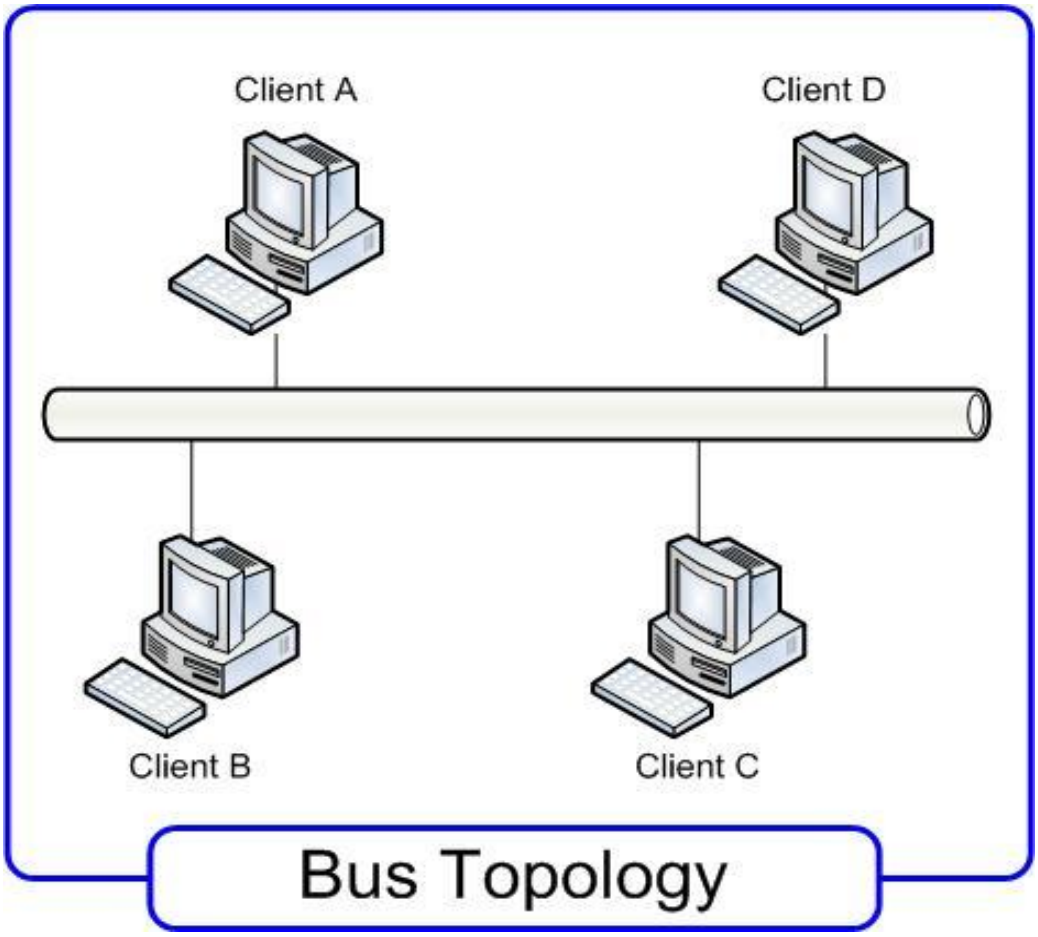
საბაზო ქსელური ტოპოლოგიები

არსებობს სამი საბაზო ტოპოლოგია, რომლის საფუძველზე ხდება ქსელების უმრავლესობის აგება.



”სალტე” (Bus). ამ ტოპოლოგიაში ყველა კომპიუტერი შეერთებულია ერთმანეთთან *ერთი კაბელით* (ნახ. 3.1). ასეთ ქსელში გაგზავნილი მონაცემები გადაეცემა ამ ქსელის ყველა

კომპიუტერს, მაგრამ მონაცემებს დაამუშავებს მხოლოდ ის კომპიუტერი, რომლის ქსელური ადაპტერის აპარატურული MAC-მისამართი ჩაწერილია კადრში, როგორც მიმღების მისამართი.



ნახ. 3.1. ქსელი ტოპოლოგიით "სალტე"

ეს ტოპოლოგია განსაკუთრებით მარტივია გასახორციელებლად და იაფია (ითხოვს ყველაზე ნაკლებ კაბელს), მაგრამ აქვს მთელი რიგი არსებითი ნაკლოვანებები.

ტოპოლოგია "სალტეს" ნაკლოვანებები

X

ძნელია ასეთი ქსელების *გაფართოება* (კომპიუტერების და *სეგმენტების* - კომპიუტერების შემაერთებელი კაბელების ცალკეული მონაკვეთების რაოდენობის გაზრდა).

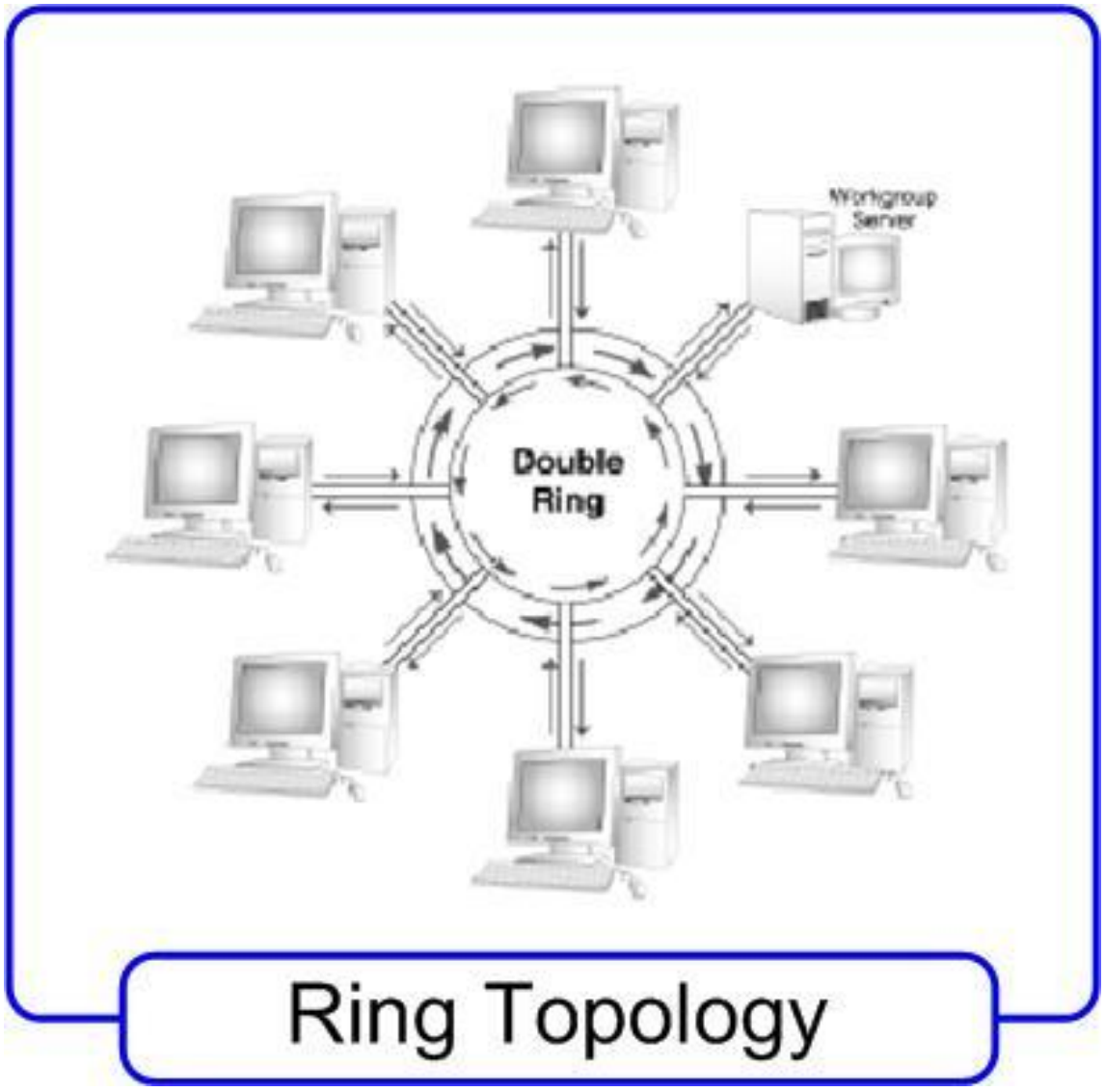
X რადგან სალტე გამოიყენება ერთობლივად, დროის ყოველ მომენტში გადაცემა შეიძლება აწარმოოს *კომპიუტერთაგან მხოლოდ ერთმა*. თუ გადაცემას ერთდროულად იწყებს ორი ან მეტი კომპიუტერი, მაშინ წარმოიქმნება სიგნალის დამახინჯება (*შეჯახება* ანუ *კოლიზია*), რასაც მოჰყვება ყველა კადრის დაზიანება. ამის გამო კომპიუტერები იძულებული არიან შეაჩერონ გადაცემა და შემდგომ, რიგრიგობით აწარმოონ კადრების რეტრანსლირება. შეჯახებების გავლენა მით უფრო შესამჩნევია, რაც უფრო დიდია ქსელით გადაცემული ინფორმაციის მოცულობა და რაც უფრო მეტი კომპიუტერია მიერთებული სალტეზე. ორივე ეს ფაქტორი, ბუნებრივია, ამცირებს როგორც მაქსიმალურად შესაძლებელ, ასევე ქსელის საერთო წარმადობას, რაც იწვევს ქსელის მუშაობის შენელებას.

X ”სალტე” არის *პასიური ტოპოლოგია* - კომპიუტერები მხოლოდ ”უსმენენ” კაბელს და არ შეუძლიათ გააძლიერონ ქსელში გადაცემისას შესუსტებული სიგნალები. იმისათვის რომ ქსელი დავაგრძელოთ, უნდა გამოვიყენოთ *გამმეორებლები* (*რეპიტერები*), რომლებითაც ხდება მეორე სეგმენტში გადასაცემი სიგნალის გაძლიერება.

X ”სალტური” ტოპოლოგიის ქსელის საიმედოობა არის დაბალი. როდესაც ელექტრული სიგნალი აღწევს კაბელის ბოლოს, ის (თუ არ არის მიღებული სპეციალური ზომები) აირეკლება და არღვევს ქსელის მთელი სეგმენტის მუშაობას. სიგნალების ასეთი არეკვლის თავიდან ასაცილებლად, სალტის ტოპოლოგიის ქსელის კაბელის ბოლოებს უერთებენ სპეციალურ *რეზისტორებს* (*ტერმინატორებს*), რომლებიც სიგნალებს შთანთქავენ. თუ კაბელი გაწყდება ნებისმიერ ადგილას - მაგალითად, კაბელის მთლიანობის დარღვევისას ან კონექტორის უბრალო გამოღებისას, - წარმოიქმნება არატერმინირებული ორი სეგმენტი, რომელთა ბოლოებზე სიგნალები იწყებენ არეკვლას და მთელი ქსელის მუშაობა წყდება.

”სალტეს” ტოპოლოგიისათვის დამახასიათებელმა პრობლემებმა მიგვიყვანეს იქამდე, რომ ათი წლის წინათ პოპულარული ქსელები ამჟამად პრაქტიკულად არ გამოიყენება.

”რგოლი” (Ring). მოცემულ ტოპოლოგიაში ყოველი კომპიუტერი შეერთებულია ორ სხვასთან ისე, რომ ერთისგან მიიღოს ინფორმაციას, ხოლო მეორეს გადასცეს (ნახ. 3.2). ბოლო კომპიუტერი უერთდება პირველს, და რგოლი *იკვრება*.

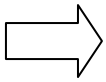


ნახ. 3.2. ქსელი ტოპოლოგიით "რგოლი"

”რგოლური” ტოპოლოგიის ქსელების უპირატესობები და ნაკლოვანებები

უპირატესობები	*ნაკლოვანებები*
V რადგან ამ ტოპოლოგიის ქსელს არა აქვს თავისუფალი ბოლოები, ამიტომ არ არის საჭირო ტერმინატორები;	X სიგნალი ”რგოლში” გადის თანმიმდევრულად (და მხოლოდ ერთი მიმართულებით) ყველა კომპიუტერში, რომელთაგან თითოეული ამოწმებს, მისთვის ხომ არ არის დამისამართებული ინფორმაცია, ამიტომ გადაცემის დრო შეიძლება იყოს საკმაოდ დიდი;
V ყოველი კომპიუტერი გამოდის გამმეორებლის როლში (აძლიერებს სიგნალს), რაც იძლევა საშუალებას აიგოს გრძელი ქსელები;	X ქსელში ახალი კომპიუტერის ჩართვა ხშირად მოითხოვს მის გაჩერებას, რაც არღვევს ყველა დანარჩენი კომპიუტერის მუშაობას;
V შეჯახებების არარსებობის გამო ტოპოლოგიას გააჩნია მდგრადობა დიდი გადატვირთვების მიმართ, რის გამოც უზრუნველყოფს ეფექტურ მუშაობას ქსელში გამავალი ინფორმაციის დიდ ნაკადებთან.	X ქსელის ერთი მაინც კომპიუტერის ან მოწყობილობის მწყობრიდან გამოსვლა არღვევს მთელი ქსელის მუშაობას;
	X რგოლის კაბელების ნებისმიერ ადგილას წყვეტა ან მოკლე ჩართვა, მთელი ქსელის მუშაობას ხდის შეუძლებელს;
	X იმისათვის, რომ კომპიუტერის მტყუნებისას ან კაბელის გაწყვეტისას რგოლური ტოპოლოგიის ქსელის მუშაობის გაჩერებას აარიდონ თავი, ჩვეულებრივად გაყავთ ორი რგოლი, რითაც ქსელი ხდება საგრძნობლად ძვირი.

აქაც, ისევე როგორც ”სალტური” ტოპოლოგიის ქსელებისათვის, ნაკლოვანებებმა რამდენადმე გადაწონეს უპირატესობები, რის შედეგადაც ადრე პოპულარული რგოლური ქსელები ახლა გაცილებით იშვიათად გამოიყენება.

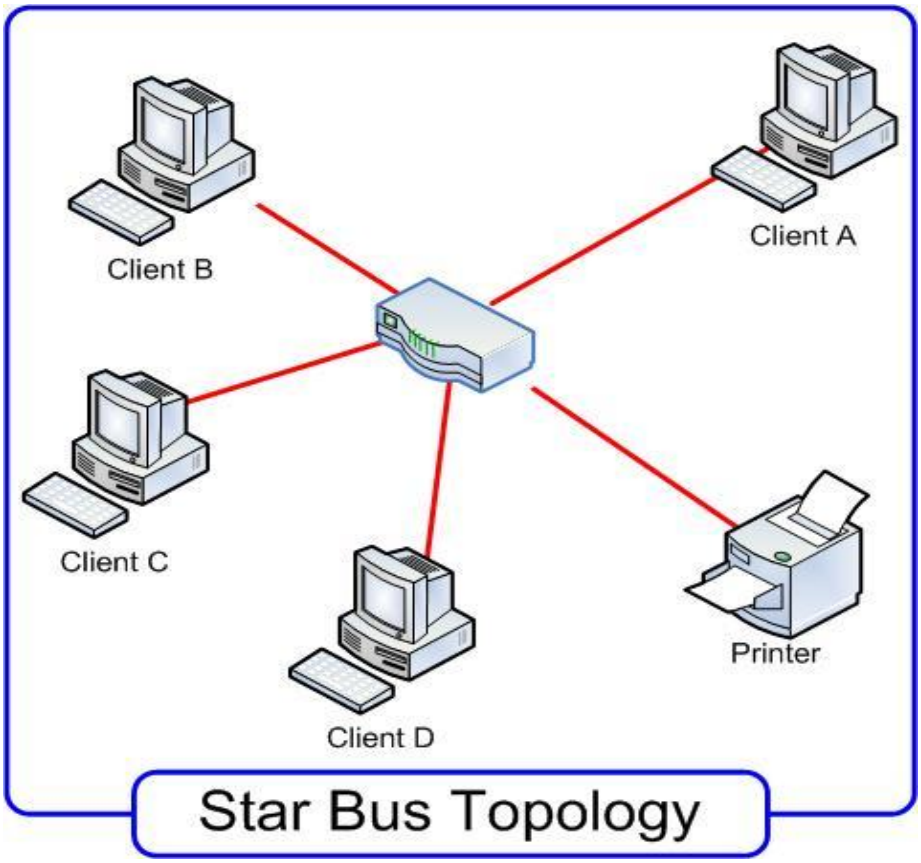


აქტიური ტოპოლოგია "ვარსკლავი" (Active Star). ეს ტოპოლოგია გამოჩნდა გამოთვლითი ტექნიკის გარიჟრაჟზე, როდესაც მძლავრ ცენტრალურ კომპიუტერს უერთდებოდა ქსელის ყველა დანარჩენი აბონენტი. ასეთი კონფიგურირებისას მონაცემთა მთელი ნაკადი გადიოდა ცენტრალურ კომპიუტერში; თავადაც იყო მთლიანად პასუხისმგებელი ქსელის ყველა მონაწილეს შორის ინფორმაციული გაცვლის მართვაზე. ურთიერთქმედების ასეთი ორგანიზებისას კონფლიქტები ქსელში შეუძლებელია, მაგრამ ცენტრალური კომპიუტერის დატვირთვა იმდენად დიდი იყო, რომ, როგორც წესი, ქსელის მართვის გარდა ვერაფერს აკეთებდა. მისს მწყობრიდან გამოსვლას მოყვებოდა მთელი ქსელის მტყუნება, მაშინ როდესაც პერიფერიული კომპიუტერის მტყუნება ან მასთან კავშირის გაწყვეტა დანარჩენი ქსელის მუშაობაზე გავლენას ვერ ახდენდა. ამჟამად ასეთი ქსელები გვხვდება საკმარისად იშვიათად.

გაცილებით უფრო გავრცელებული ტოპოლოგიაა მსგავსი ვარიანტი - **"ვარსკვლავი-სალტე" (Star-Bus)** ანუ **"პასიური ვარსკვლავი"** (ნახ. 3.3). აქ პერიფერიული კომპიუტერები, უერთდებიან არა ცენტრალურ კომპიუტერს, არამედ *პასიურ კონცენტრატორს* ანუ *ჰაბს* (*hub*). უკანასკნელს, ცენტრალური კომპიუტერისგან განსხვავებით, მონაცემთა ნაკადების მართვაზე არავითარი პასუხისმგებლობა არა აქვს, არამედ ასრულებს იგივე ფუნქციებს, რასაც გამმეორებელი, ე. ი. აღადგენს შემომავალ სიგნალებს და გადაუგზავნის მასთან მიერთებულ ყველა კომპიუტერსა და მოწყობილობას. სწორედ ამის გამო, მოცემული ტოპოლოგია ფიზიკურად გამოიყურება როგორც "ვარსკვლავი", მაგრამ ლოგიკურად არის ტოპოლოგია "სალტე" (რაც ასახულია კიდეც მის სახელწოდებაში).

მიუხედავად კაბელის დიდი ხარჯისა, რაც დამახასიათებელია "ვარსკვლავის" ტიპის ქსელებისათვის, ამ ტოპოლოგიას აქვს არსებითი უპირატესობები დანარჩენებთან შედარებით, რაც განაპირობებს მის ფართო გამოყენებას თანამედროვე ქსელებში.

"ვარსკვლავი-სალტე" ტიპის ქსელების უპირატესობები



ნახ. 3.3. ქსელი ტოპოლოგიით "ვარსკვლავი-სალტე"

- *საიმედოობა* - ცენტრალურ კონცენტრატორთან მოწყობილობის მიერთება ან მისგან გამორთვა არ აისახება დანარჩენი ქსელის მუშაობაზე; კაბელის წყვეტები მოქმედებენ კომპიუტერთაგან მხოლოდ ერთეულებზე; ტერმინატორები არ არის საჭირო.

- *სიადვილე მომსახურებისას და პრობლემების მოხსნისას* - ყველა კომპიუტერი და ქსელური მოწყობილობა უერთდება ცენტრალურ კონცენტრატორს, რაც საგრძნობლად ამარტივებს ქსელის მომსახურებასა და შეკეთებას.

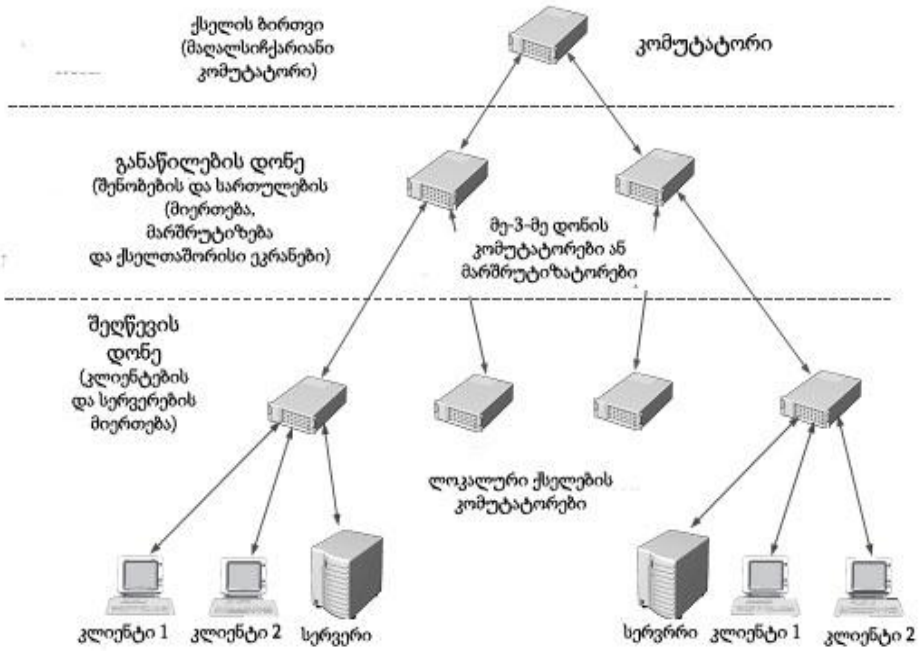
- *დაცულობა* - მიერთების წერტილების კონცენტრაცია ერთ ადგილას საშუალებას იძლევა ადვილად შეიზღუდოს შეღწევა ქსელის სასიცოცხლოდ მნიშნელოვანი ობიექტებისადმი.

აღვნიშნოთ, რომ კონცენტრატორების ნაცვლად უფრო "ინტელექტუალური" მოწყობილობების გამოყენებით *(ხიდების, კომუტატორებისა და მარშრუტიზატორების* - მათ შესახებ უფრო დაწვრილებით მოგიყვებით მოგვიანებით) მიიღება "შუალედური" ტიპის ტოპოლოგია აქტიურსა და პასიურ ვარსკვლავებს შორის. ამ შემთხვევაში ტელეკომუნიკაციური მოწყობილობა მიღებულ სიგნალებს არა მხოლოდ რეტრანსლირებს, არამედ ახორციელებს მათი გაცვლის მართვასაც.

სხვა შესაძლო ქსელური ტოპოლოგიები

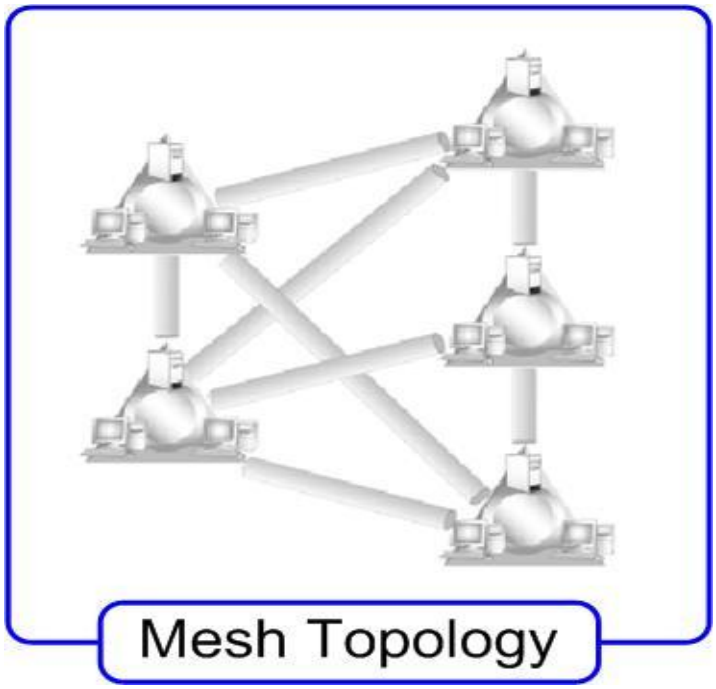
რეალური კომპიუტერული ქსელები მუდმივად ფართოვდებიან და მოდერნიზირდებიან, ამიტომ ასეთი ქსელი თითქმის ყოველთვის არის *ჰიბრიდული* - ე. ი. მისი ტოპოლოგია წარმოდგენილია რამოდენიმე საბაზო ქსელის კომბინაციით. იოლი წარმოსადგენია ჰიბრიდული ტოპოლოგიები, რომლებიც წარმოადგენენ "ვარსკვლავის" და "სალტეს" ან "რგოლისა" და "ვარსკვლავის" კომბინაციებს.

მაგრამ განსაკუთრებით უნდა გამოიყოს **ტოპოლოგია "ხე" (Tree)**, რომელიც შეიძლება განვიხილოთ როგორც რამოდენიმე "ვარსკვლავის" გაერთიანება (ნახ. 3.4). სწორეთ ასეთი ტოპოლოგიაა დღეს ყველაზე პოპულარული ლოკალური ქსელების აგებისას.



ნახ. 3.4. ქსელი ჰიბრიდული ტოპოლოგიით "ხე"

დაბოლოს, უნდა ვახსენოთ **ბადური (mesh) ტოპოლოგია**, რომელშიც ყველა ან ნაწილი კომპიუტერებისა და სხვა მოწყობილობებისა უშუალოდაა მიერთებული ერთმანეთთან (ნახ. 3.5).



ნახ. 3.4. ბადური ჰიბრიდული ტოპოლოგიის ქსელი

ასეთი ტოპოლოგია განსაკუთრებულად საიმედოა - ნებისმიერი არხის დაზიანებისას მონაცემთა გადაცემა არ წყდება, რადგან შესაძლებელია *ინფორმაციის მიტანის რამოდენიმე მარშრუტი.* ბადური ტოპოლოგიები (უფრო ხშირად არა სრული, არამედ ნაწილობრივი) გამოიყენება იქ, სადაც *მაქსიმალურად უნდა გამოირიცხოს მტყუნება*, მაგალითად, მსხვილი საწარმოს ქსელის რამოდენიმე უბნის გასაერთიანებლად ან ინტერნეტთან მიერთებისას, მაგრამ რასაკვირველია, მოგვიწევს გადახდა: საგრძნობლად იზრდება კაბელის ხარჯი, რთულდება ქსელური მოწყობილობა და მისი გაწყობა.

შეღწევა გადაცემის გარემოში

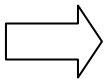
ქსელურ ტოპოლოგიებთან მჭიდროდაა დაკავშირებული *გადაცემის გარემოში შეღწევის ხერხის* ცნება - იგულისხმება

ინტერნეტის თავისებური "წინამორბედი" იყო ქსელი ARPANet-ი, თავდაპირველად შექმნილი აშშ-ს თავდაცვის სამინისტროს შეკვეთით. ამ პროექტის მიზანი იყო კავშირგაბმულობის ისეთი სისტემის შექმნა, რომელიც შეძლებდა ფუნქციონირებას ატომური ომის პირობებშიც კი. ამჟამინდელი ინტერნეტი, როგორც თავისუფლად ხელმისაწვდომი მსოფლიო კომპიუტერული ქსელი, ნაწილობრივ გახდა სამხედრო შემუშავებების მოულოდნელი "კონვერსიული" შედეგი.

წესების კრებული, რომლითაც განისაზღვრება სწორედ თუ როგორ უნდა გააგზავნონ და მიიღონ მონაცემები ქსელით კომპიუტერებმა.

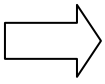
ასეთი ხერხი შესაძლებელია რამოდენიმე. მათგან ძირითადებია:

- მრავალჯერადი შეღწევა გადამტანის კონტროლითა და შეჯახებების აღმოჩენით;
- მრავალჯერადი შეღწევა გადამტანის კონტროლითა და შეჯახებების თავიდან აცილებით;
- მარკერის გადაცემა.



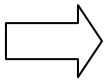
მრავალჯერადი შეღწევა გადამტანის კონტროლითა და შეჯახებების აღმოჩენით (Carrier Sense Multiple Access with Collision Detection, CSMA/CD) მეთოდის შემთხვევაში ყველა კომპიუტერი (*მრავალჯერადი შეღწევა*) "უსმენს" კაბელს (*გადამტანის კონტროლი*) იმის დასადგენად, გადაიცემა თუ არა კაბელში მონაცემები. თუ კაბელი თავისუფალია, ნებისმიერ კომპიუტერს შეუძლია დაიწყოს გადაცემა, მაშინ დანარჩენებმა უნდა მოიცადონ, სანამ კაბელი არ გათავისუფლდება. თუ კომპიუტერებმა ერთდროულად დაიწყეს გადაცემა და მოხდა შეჯახება, ყველა (თითოეული - დროის სხვადასხვა შუალედით) შეაჩერებს გადაცემას (*შეჯახებების აღმოჩენა*), რის შემდეგ ახდენენ მონაცემების რეტრანსლირებას.

ამ ხერხის სერიოზული ხარვეზია ის, რომ დიდი რაოდენობის კომპიუტერების შემთხვევაში და ქსელზე დიდი დატვირთვისას შეჯახებების რაოდენობა იზრდება, ხდება გამტარუნარიანობის დაცემა, ზოგჯერ ძალიან მნიშვნელოვნად. რადგან ეს ხერხი ტექნიკურად ძალიან მარტივად განხორციელებადია, ამიტომ გამოიყენება დღეს ყველაზე პოპულარულ *Ethernet ტექნოლოგიაში*. იმისათვის, რომ შეამცირონ შეჯახებების რაოდენობა, თანამედროვე ქსელებში გამოიყენება ისეთი მოწყობილობები, როგორიცაა ხიდები, კომუტეტორები და მარშრუტიზატორები.



მეთოდი **მრავალჯერადი შეღწევა გადამტანის კონტროლითა და შეჯახებებების თავიდან აცილებით** (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) იმით განსხვავდება წინასაგან, რომ მონაცემების გადაცემის დაწყებამდე კომპიუტერი ქსელში აგზავნის სპეციალურ მცირე პაკეტს ("უწყებას"), რითაც ამცნობს დანარჩენ კომპიუტერებს, რომ განზრახული აქვს დაიწყოს ტრანსლაცია. ამით სხვა

კომპიუტერები ”იგებენ”, რომ რომელიღაც მათგანი აპირებს გადაცემის დაწყებას. ეს იძლევა შეჯახებების თავიდან აცილების საშუალებას. რა თქმა უნდა, ასეთი ”უწყებები” ზრდიან ქსელზე საერთო დატვირთვას და ამცირებენ მის გამტარუნარიანობას (ამის გამო მეთოდი CSMA/CA მუშაობს უფრო ნელა ვიდრე CSMA/CD), მაგრამ ის უდაოდ საჭიროა, მაგალითად, უკაბელო ქსელების მუშაობისათვის.



მარკერის გადაცემით (Token Passing) ქსელებში ერთი კომპიუტერიდან მეორესაკენ წრეზე მუდმივად კურსირებს მონაცემების მცირე ბლოკი, რომელსაც *მარკერი* ეწოდება. თუ კომპიუტერს, რომელმაც მიიღო მარკერი, არა აქვს ინფორმაცია გადაცემისათვის, მაშინ ის უბრალოდ გადაუგზავნის (Passing) მარკერს შემდეგ კომპიუტერს. თუ კომპიუტერს, რომელმაც მიიღო მარკერი, აქვს ინფორმაცია გადაცემისათვის, მაშინ ის ”დაიჭერს” მარკერს, შეავსებს მას მონაცემებით და უგზავნის შემდეგ კომპიუტერს წრეზე. ასეთი საინფორმაციო პაკეტი გადაეცემა კომპიუტერიდან კომპიუტერს, მანამ პაკეტი არ მიაღწევს დანიშნულების სადგურს. რადგან მონაცემების გადაცემის მომენტში ქსელში მარკერი არ არის, სხვა კომპიუტერებს არაფრის გადაცემა აღარ შეუძლიათ, ამიტომ მარკერის გადაცემის ქსელებში შეჯახებები და შეყოვნებები შეუძლებელია, ამოთ ისინი საწარმოების ავტომატიზაციის სისტემებში ფრიად მიმზიველი ხდებიან გამოყენებისათვის.

ქსელის არჩევა

განვიხილეთ რა დღეს ყველაზე ხშირად გამოყენებადი ტოპოლოგიები და შეღწევის მეთოდები, შევეხოთ სხვა ფაქტორებსაც, რომლებიც განაპირობებენ საჭირო ტიპის ქსელის შერჩევას.

ამასთანავე უნდა გავითვალისწინოთ:

- არსებული საკაბელო სისტემა და მოწყობილობები - არის თუ არა თქვენს სახლში, სასწავლებელში, ოფისში ქსელი, რომელსაც ესაჭიროება უბრალოდ გაფართოება, ან გაქვთ მხოლოდ ცალკეული კომპიუტერები;
- ფიზიკური ადგილმდებარეობა - მნიშვნელოვანია იმის გათვალისწონება თუ როგორაა განლაგებული კომპიუტერები და სად აპირებთ ქსელური

მოწყობილობების განლაგებას. კომპიუტერების გაერთიანება ერთ ოთახში საკმაოდ მარტივია, მაგრამ თუ თქვენი კომპიუტერები განლაგებულია შენობის სხვადასხვა სართულებზე, ან სულაც რამოდენიმე შენობაში, საჭიროა კარგი გააზრება, როგორი უნდა იყოს მომავალი ქსელის საუკეთესო კონფიგურაცია და ტოპოლოგია;

- დასაგეგმი ქსელის ზომები - თუ თქვენ გაქვთ რამოდენიმე კომპიუტერი, მაშინ ქსელის სტრუქტურა იქნება საკმაოდ მარტივი; მაგრამ, თუ მათი რაოდენობა - ასობით ან ათასობითაა, მაშინ, ყველაზე მეტად სავარაუდოა, რომ თქვენი არჩევანის ობიექტი იქნება რთული ჰიბრიდული ტოპოლოგია;
- ერთობლივი მოხმარებისათვის ინფორმაციის მოცულობა და ტიპი - საჭირო ტიპის ქსელის არჩევისას ეს პარამეტრები აუცილებლად არის გასათვალისწინებელი: გადაიცემა თუ არა დიდი ფაილები - მუსიკალური, ვიდეო- ან გრაფიკული. ასეთ შემთხვევაში თქვენ დაგჭირდებათ მაღალსიჩქარიანი ქსელი, რომელიც იძლევა ასეთი ინფორმაციის სწრაფად და შეყოვნების გარეშე გადაცემის საშუალებას.

!

თანამედროვე ქსელების აბსოლუტურ უმრავლესობაში გამოიყენება ტოპოლოგია ”ვარსკვლავი” ან ჰიბრიდული ტოპოლოგია, რომელიც წარმოადგენს რამოდენიმე ”ვარსკვლავის” გაერთიანებას (მაგალითად, ასეთი ტიპის ტოპოლოგიაა ”ხე”), და გარემოში შეღწევის CSMA/CD მეთოდი (მრავალჯერადი შეღწევა გადამტანის კონტროლითა და შეჯახებების აღმოჩენით).

?

კითხვები და დავალებები

1. რაში მდგომარეობს სხვაობა ფიზიკურ და ლოგიკურ კავშირებს შორის?
2. ჩამოთვალეთ საბაზო ქსელური ტოპოლოგიები.
3. როგორია კონფიგურაცია "ვარსკვლავის" უპირატესობები და ნაკლოვანებები? რომელ ლოკალურ ქსელებში გამოიყენება ის?
4. როგორია ტოპოლოგია "რგოლის" უპირატესობები და ნაკლოვანებები? რომელ ლოკალურ ქსელებში გამოიყენება ის?
5. როგორია კონფიგურაცია "სალტეს" უპირატესობები და ნაკლოვანებები? რომელ ლოკალურ ქსელებში გამოიყენება ის?
6. როგორი ჰიბრიდული ტოპოლოგიებია თქვენთვის ცნობილი?
7. როგორი ფაქტორების გათვალისწინებაა აუცილებელი ქსელის დაგეგმვისას?

თავი 4

ვაგებთ ქსელს: კავშირგაბმულობის ხაზები

ამ თავში თქვენ ნახავთ პასუხებს შემდეგ კითხვებზე:

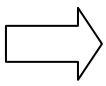
- **სიგნალების გადაცემის გარემოს როგორი სახეობები შეიძლება გამოვიყენოთ კომპიუტერულ ქსელებში?**
- **როგორი ტიპებისა და კატეგორიების კაბელური შეერთებებია შესაძლებელი?**
- **როგორ კეთდება კაბელური შეერთებები?**
- **როგორი ტიპის გასართები (კონექტორები) არსებობენ?**
- **როგორი ტიპის უკაბელო ქსელებია შესაძლებელი?**

იმისათვის, რომ კომპიუტერებმა შეძლონ ურთიერთქმედება, საჭიროა რაიმე გარემო, რომელიც უზრუნველყოფს სიგნალების გადაცემას ფიზიკურ დონეზე. ეს *გადაცემის გარემო* შეიძლება წარმოადგენდეს სხვადასხვა ტიპის *საკაბელო ინფრასტრუქტურას*, ე. ი. სხვადასხვა ტიპის კაბელების კრებულებს, დამაკავშირებელ *გასართებს* (*კონექტორებს*) და *ტელეკომუნიკაციურ მოწყობილობებს*. მაგრამ ის შეიძლება იყოს უბრალოდ ატმოსფერო ან უჰაერო სივრცე - მთავარია იყოს საშუალება როგორმე *გადაიცეს სიგნალი* ერთი კომპიუტერიდან მეორესკენ.

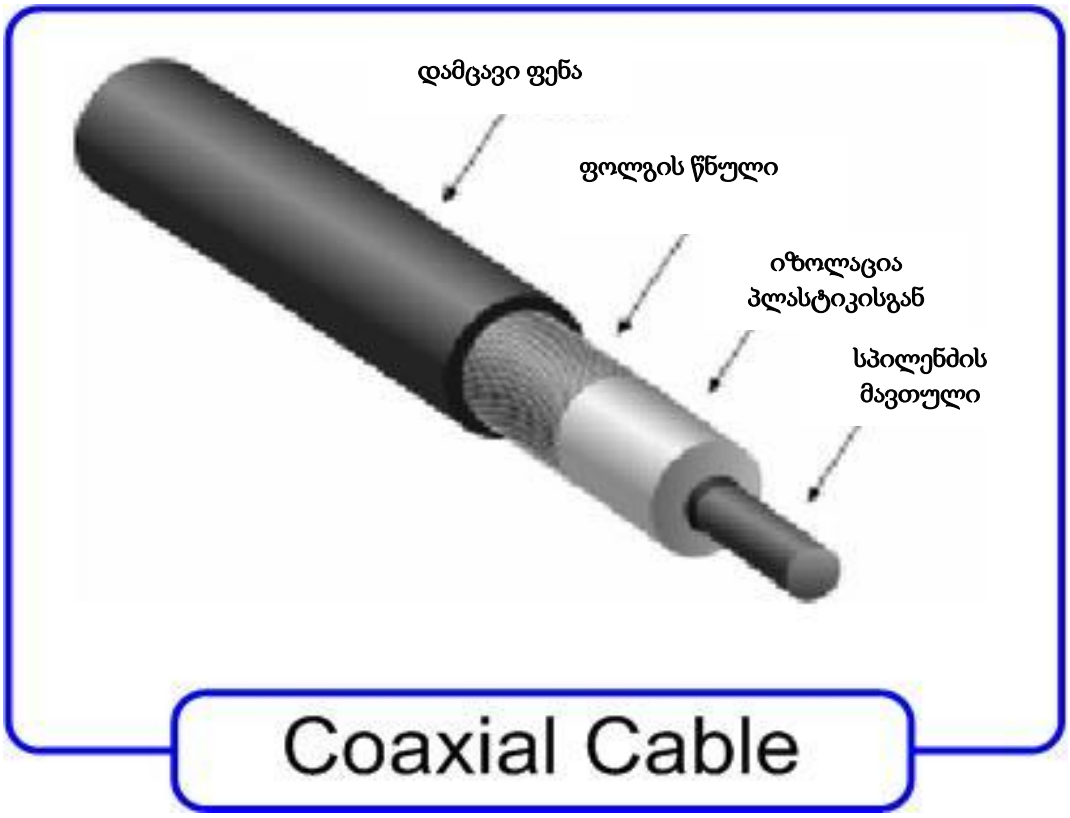
კაბელური შეერთებები

კომპიუტერებს ან სხვა ქსელურ მოწყობილობებს შორის ელექტრული ან ოპტიკური სიგნალების გადასაცემად ქსელებში ყველაზე უფრო ხშირად გამოიყენება კაბელური შეერთებები. ამასთანავე გამოიყენება კაბელების შემდეგი ტიპები:

- კოაქსიალური კაბელი (coaxial cable);
- ხვეული წყვილი (twisted pair);
    - არაეკრანირებული (unshielded, UTP),
    - ეკრანირებული (shielded, STP);
- ბოჭკოვან-ოპტიკური ან ოპტიკურ-ბოჭკოვანი (fiber optic).



ჯერ კიდევ ათი - თხუთმეტი წლის წინათ ქსელების შექმნისას ძირითადად გამოიყენებოდა *კოაქსიალური კაბელი*, რომელიც შედგებოდა სპილენძის ან ალუმინის ძარღვისაგან, იზოლაციის ფენისაგან, სპილენძის მავთულების ან ალუმინის ფოლგისაგან დამზადებული მაეკრანირებელი წნულისაგან და გარე დამცავი გარსისაგან (ნახ. 4.1). სიგნალის გადასაცემად



ნახ. 4.1. კოაქსიალური კაბელი

კოაქსიალურ კაბელში გამოიყენებოდა ცენტრალური ძარღვი, მაშინ როდესაც მაეკრანირებელი წნული იყო დამიწებული და თამაშობდა ელექტრული ნულის როლს.

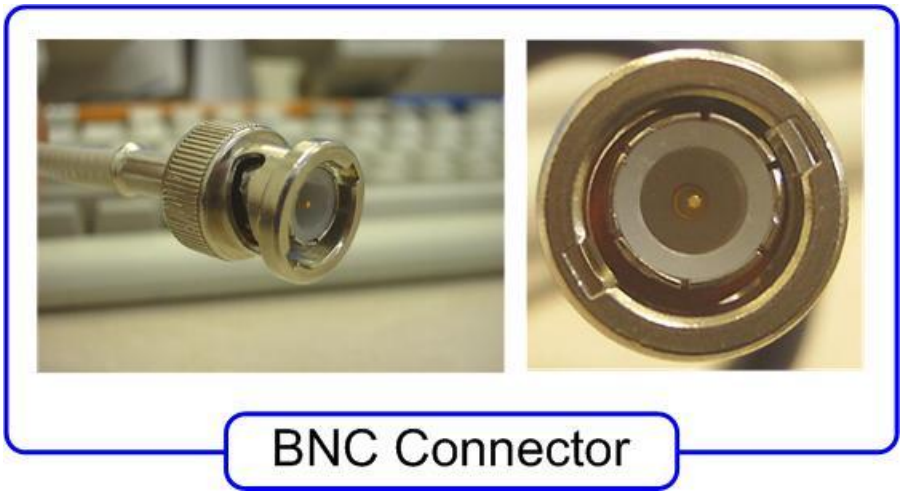
ამასთანავე გამოიყენებოდა კაბელის ორი შესაძლო ტიპი - ”წვრილი” და ”მსხვილი”.

წვრილი კოაქსიალური კაბელი - მოქნილი, მიახლოებით 0.5 სმ დიამეტრის, რომლითაც მონაცემების გადაცემა მილევის გარეშე შეიძლებოდა 185 მ-დე (რეალურ ქსელებში კი 300 მ-დეც კი).

კაბელის ქსელურ მოწყობილობებთან მისაერთებლად გამოიყენებოდა სპეციალური *BNC ტიპის გასართები.*

კაბელის მონაკვეთის ბოლოებზე მონტაჟდებოდა უბრალო BNC-კონექტორები (ნახ. 4.2). ამ მონაკვეთების ერთმანეთთან გადაბმისათვის გამოიყენებოდა BNC **I**-კონექტორები (ანუ ”ბარელ-კონექტორები”), ხოლო ქსელურ ადაპტერებთან და მოწყობილობებთან მისაერთებლად გამოიყენებოდა BNC **T**-კონექტორები.

არეკვლილი სიგნალის შთანთქმისათვის კოაქსიალური კაბელის ბოლოებზე აყენებდნენ BNC-ტერმინატორებს, რომელთაგან ერთ-ერთი აუცილებლად იყო დამიწებული.

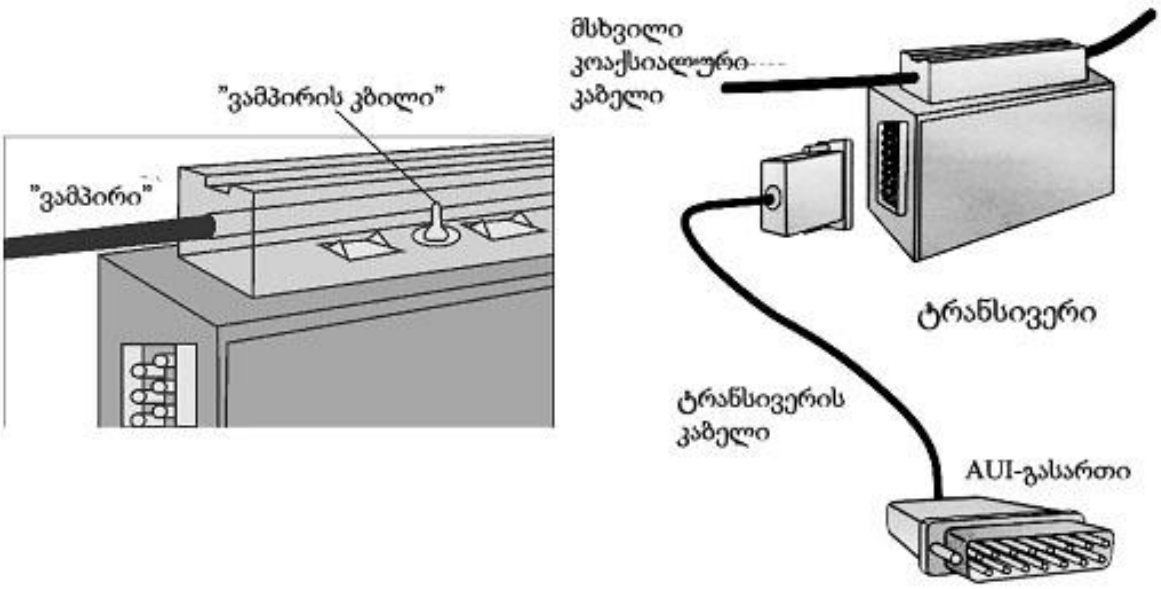


ნახ. 4.2. BNC-კონექტორი

მსხვილი კოაქსიალური კაბელი - შედარებით ხისტი, დიამეტრით 1 სმ-ზე ოდნავ მეტი. მასში სპილენძის ძარღვი უფრო მსხვილია ვიდრე წვრილ კოაქსიალურ კაბელში და, შესაბამისად, მისი ელექტრული წინაღობა - ნაკლები. ამიტომ მსხვილი კოაქსიალური კაბელი იძლეოდა სიგნალების გადაცემის საშუალებას 500 მ მანძილზე.

მსხვილ კოაქსიალურ კაბელთან მისაერთებლად გამოიყენებოდა სპეციალური მოწყობილობები - ტრანსივერები (”transmitter-receiver”-დან - ”მიმღებ-გადამცემი”) საკმაოდ ორიგინალური სახელწოდებით - ”ქსელური ვამპირი”. გასართებად გამოიყენებოდა AUI- ან DIX-კონექტორები (ნახ. 4.3).

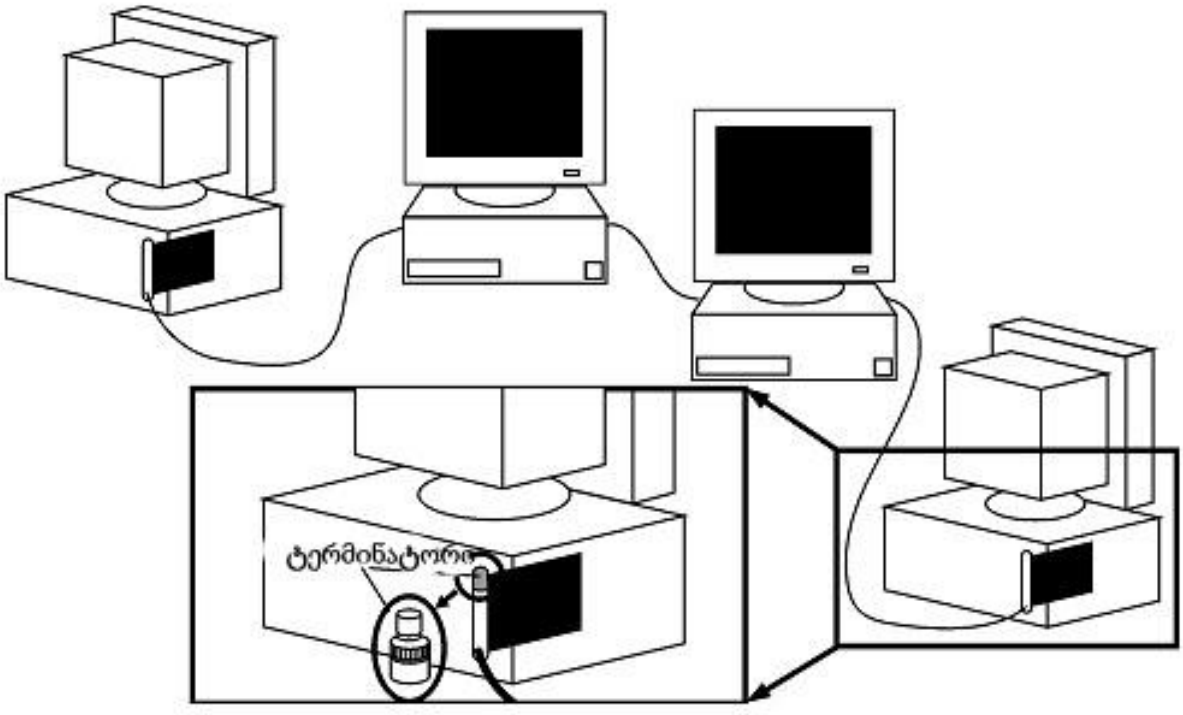
კოაქსიალური კაბელის საფუძველზე აგებული ქსელების ფართო გავრცელება გამოწვეული იყო ორი გარემოებით: სიიაფით (განსაკუთრებით ქსელებისათვის წვრილი კოაქსიალური კაბელით) - კაბელებზე და კონექტორებზე მინიმალური ხარჯებით - საკმარისი იყო მაგისტრალური



ნახ. 4.3. მიერთება ტრანსივერით "ქსელური ვამპირი".

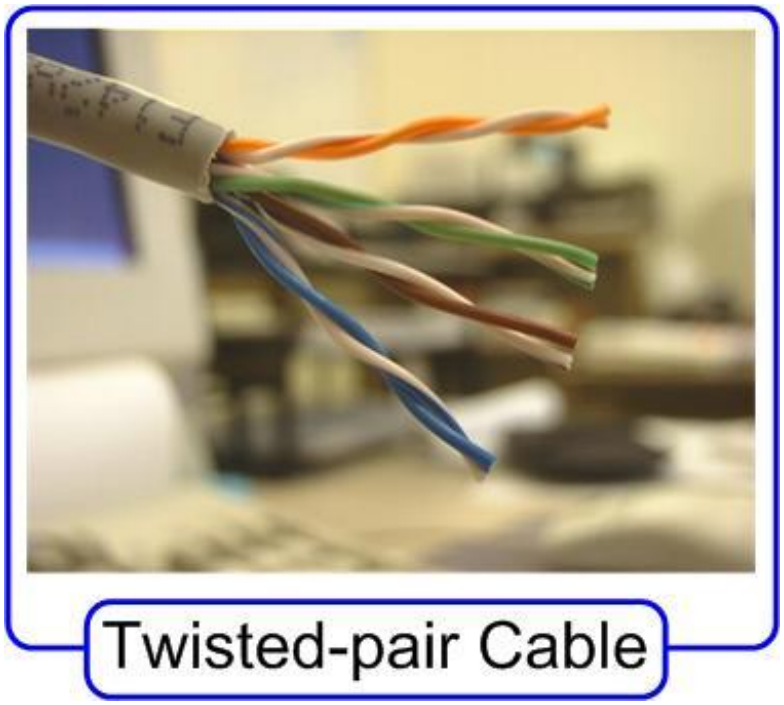
კაბელის გაყვანა, მის ბოლოებზე ტერმინატორების დაყენება და მასთან კომპიუტერების მიერთება, - და ქსელი მზად იყო (ნახ. 4.4)

მიუხედავად ამისა, ქსელების უმრავლესობაში კოაქსიალური კაბელი შეცვლილია ხვეული წყვილით ან ოპტიკური კაბელებით.



ნახ. 4.4. ქსელის მაგალითი წვრილი კოაქსიალური კაბელით

ხვეული წყვილი - ორი ერთმანეთზე გადაგრეხილი და ერთმანეთისაგან იზოლირებული სპილენძის მავთული. ხვეული წყვილის საფუძველზე არსებული კაბელების აბსოლუტური უმრავლესობა შედგება ოთხი წყვილისგან, რომლებიც გადაგრეხილებია სხვადასხვა ბიჯით მეზობელი წყვილებისა და გარე წყაროების მავნე ელექტრული გამოსხივებისაგან დასაცავად და დაფარული არიან პლასტიკური გარსით (ნახ. 4.5). *ეკრანირებულ ხვეულ*



ნახ. 4.5. ხვეული წყვილი

წყვილში, გარდა ამისა, გამოიყენება ერთი ან რამდენიმე ალუმინის ან სპილენძის კილიტა, რომლებიც საგრძნობლად ამაღლებენ კაბელის მდგრადობას ხელშეშლებისადმი.

ასეთი კაბელები გამოდის EIA/TIA 568 (გაყვანილობის ამერიკული სტანდარტი კომერციულ შენობებში) სტანდარტის მიხედვით და იყოფა *კატეგორიებად*. სხვადასხვა კატეგორიის ხვეული წყვილის კაბელები ერთმანეთისაგან განსხვავდებიან, პირველ რიგში, წყვილების ერთმანეთზე გადაგრეხის ბიჯით. რაც უფრო ნაკლებია ბიჯი, მით მაღალია კაბელის კატეგორია და მით უფრო მაღალია მონაცემების გადაცემის სიჩქარე.

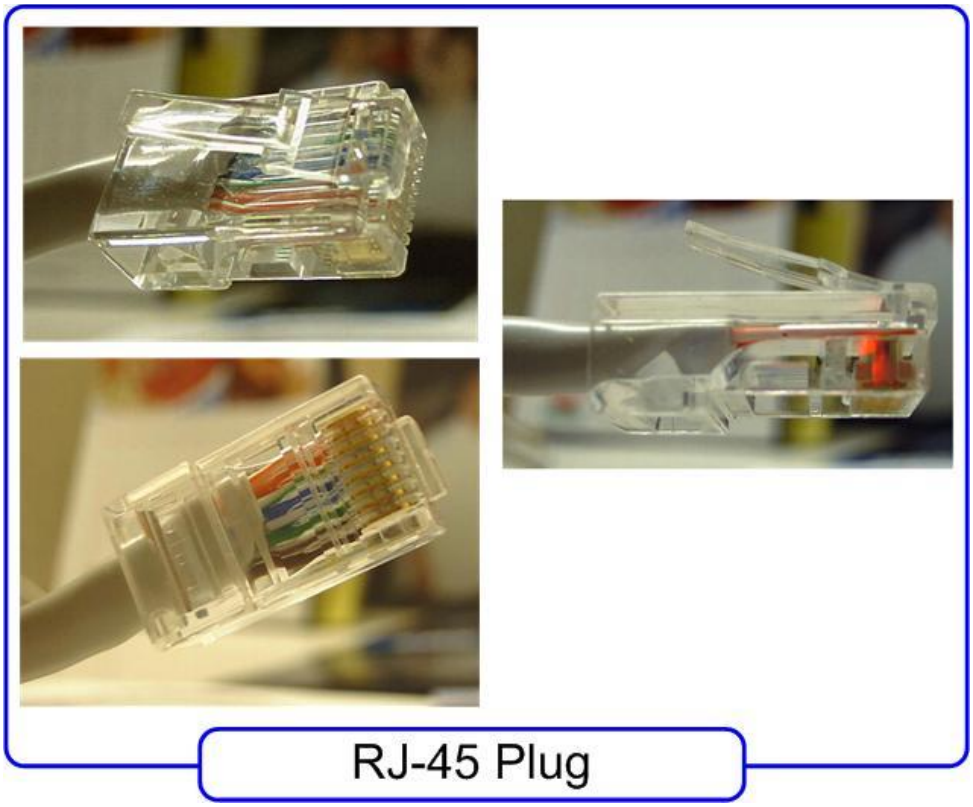
ცხრილი 4.1

"ხვეული წყვილის" კაბელის მახასიათებლები

კატეგორია	მახასიათებელი
1	სატელეფონო კაბელი ხმისა და მონაცემების გადასაცემად ანალოგური მოდემებით.
2	ძველი 2-წყვილიანი კაბელი. მონაცემების გადაცემის სიჩქარე - 4 მბიტი/წმ-მდე. მოიხმარება Token Ring და ARCNet ქსელებში. დღეს ზოგჯერ გამოიყენება სატელეფონო ქსელებში.
3	2-წყვილიანი კაბელი. მონაცემების გადაცემის სიჩქარე - 10 მბიტი/წმ-მდე. მოიხმარება Token Ring და 10BASE-T ქსელებში. გამოიყენება სატელეფონო ქსელებში.
4	4-წყვილიანი კაბელი. მოიხმარება Token Ring, 10BASE-T, 10BASE-T4 ქსელებში 16 მბიტი/წმ-მდე სიჩქარეებისათვის. დღეს პრაქტიკულად არ გამოიყენება.
5	ეს სწორედ ის 4-წყვილიანი კაბელია, რომელიც ჩვეულებრივ იგულისხმება "ხვეული წყვილის " ქვეშ. შეუძლია მონაცემების გადაცემა 100 მბიტი/წმ სიჩქარით ორი წყვილის გამოყენებით (Fast Ethernet) და 1000 მბიტი/წმ - ოთხივე წყვილის გამოყენებით (Gigabit Ethernet). ყველაზე გავრცელებულია თანამედროვე ლოკალურ ქსელებში. თუმცა ახალი ქსელების გაყვანისას უფრო ხშირად გამოიყენება *5e კატეგორიის* კაბელი, რომელიც უკეთესად ატარებს მაღალსიხშირიან სიგნალებს. გამოდის აგრეთვე ეკრანიანი ვარიანტი.
6	4-წყვილიანი კაბელი (ეკრანირებული და არაეკრანირებული). შეუძლია გადასცეს მონაცემები 10000 მბიტი/წმ (10 Gigabit Ethernet) 200 მჰც სიხშირეებზე. *6e კატეგორიის* კაბელებში გადაცემის ზღვრული სიხშირე გაზრდილია 500 მჰც-მდე. თანამედროვე ქსელების ნახევარზე მეტი იგება ამ კატეგორიის კაბელით.
7	4-წყვილიანი კაბელი. სპეციფიკაცია საბოლოოდ დადგენილი არ არის. მონაცემების გადაცემის სიჩქარე - 100000 მბიტი/წმ-მდე, გატარების სიხშირე - 600-700 მჰც. ცალკეული წყვილები და თავად კაბელი ეკრანირებულია.

სიიაფის, დაყენების სიმარტივისა და უნივერსალურობის გამო (შეიძლება გამოვიყენოთ ქსელური ტექნოლოგიების უმრავლესობაში), ამჟამად ლოკალური ქსელების აგებისას ყველაზე გავრცელებული ტიპის კაბელია არაეკრანირებული ხვეული წყვილი. მიუხედავად ხელშეშლების წინააღმდეგ მდგრადობისა, მონტაჟის სირთულის გამო (საჭიროა ზრუნვა დამიწებაზე), არაეკრანირებულ ხვეულ წყვილთან შედარებით, ეკრანირებული ხვეული წყვილი მეტი სიხისტის გამო არ არის ფართოდ გავრცელებული.

ხვეული წყვილი უერთდება კომპიუტერსა და სხვა მოწყობილობებს *რვაკონტაქტიანი* გასართით (კონექტორით) RJ-45 (Registered Jack 45). ეს კონექტორი (ნახ. 4.6) ჰგავს სატელეფონო ქსელებში გამოყენებად RJ-11 კონექტორს, ოღონდ მასზე ცოტათი მოზრდილია.



ნახ. 4.6. RJ-45 გასართი

4.2 ტაბულაში მოყვანილია RJ-45 კონექტორში ”ხვეული წყვილი” კაბელის ჩამაგრების ხერხები EIA/TIA 568A და EIA/TIA 568 B სტანდარტების შესაბამისად; ეს ოპერაცია სრულდება სპეციალური დასაწნეხი ინსტრუმენტით. (თუ გასართს განვალაგებთ კონტაქტებით ზემოთ და მივმართავთ ჩვენგან, მაშინ კონტაქტები უნდა დაინომროს მარცხნიდან მარჯვნივ 1-ნ 8-დე).

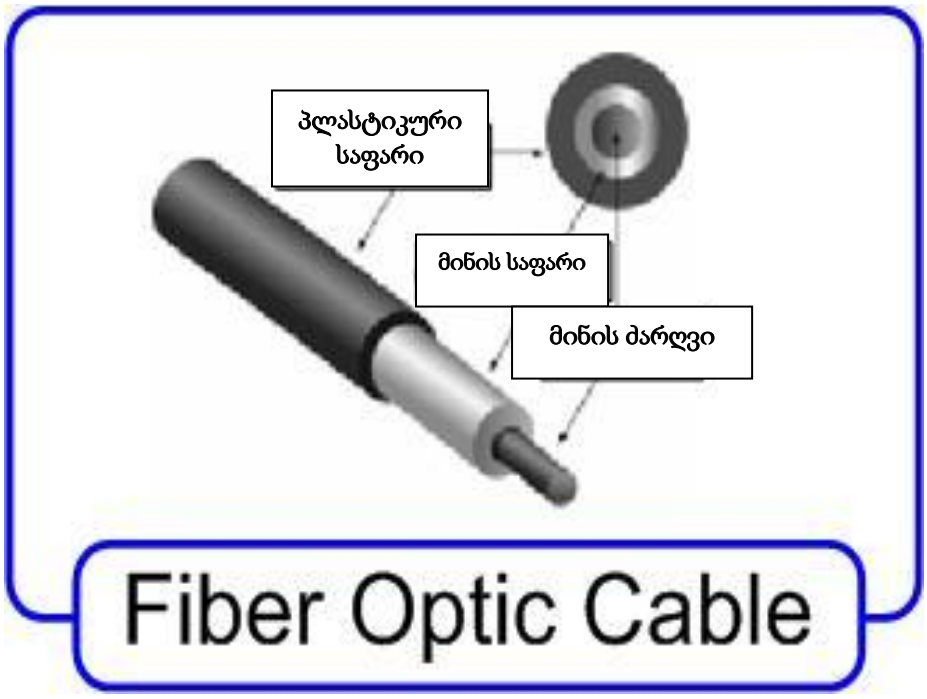
აღვნიშნოთ, რომ თუ კაბელებს ვიყენებთ კომპიუტერების კონცენტრატორებთან ან კომუტატორებთან მისაერთებლად, მაშინ კაბელი დაიწნეხება ორივე ბოლოდან ერთნაირად, ე. ი. ერთი და იგივე სტანდარტით და ამ შემთხვევაში კაბელს ჰქვია *პირდაპირი*. მაგრამ კომპიუტერების ქსელური ადაპტერების ერთმანეთთან უშუალოდ შეერთებისას ან კონცენტრატორებს ან კომუტატურებს შორის კავშირის დასამყარებლად გამოიყენება *ჯვარედინი კაბელი* (*”კროს-კაბელი”*). ასეთი კაბელების ერთი ბოლოდან გასართში ჩამაგრებისას ხვეულ

წყვილებს უცვლიან ადგილებს: თეთრი და მწვანე მავთული - თეთრი დე ვარდისფერის ნაცვლად, მწვანე კი - ვარდისფერის ადგილას, და პირიქით.

გამტარების გაყრა RJ-45 კონექტორებში

კონტაქტი	მავთულის წნულის ფერი	
	568A	568B
1	თეთრი და მწვანე	თეთრი და ვარდისფერი
2	მწვანე	ვარდისფერი
3	თეთრი და ვარდისფერი	თეთრი და მწვანე
4	ცისფერი	ცისფერი
5	თეთრი და ცისფერი	თეთრი და ცისფერი
6	ვარდისფერი	მწვანე
7	თეთრი და ყავისფერი	თეთრი და ყავისფერი
8	ყავისფერი	ყავისფერი

ბოჭკოვან–ოპტიკური კაბელი (ნახ. 4.7) განსხვავდება ქსელური გაყვანილობის სხვა სახეობებისაგან იმით, რომ აქ ინფორმაციის



ნახ. 4.7. ბოჭკოვან–ოპტიკური კაბელი

გადამტანი სინათლის იმპულსია და არა ელექტრული. ის ძალიან ჰგავს კოაქსიალურს, მაგრამ სპილენძის ან ალუმინის "ძარღვის" ნაცვლად გამოიყენება ოპტიკური ბოჭკო.

ამავდროულად შეიძლება გამოყენებულ იქნას ორი სახის ოპტიკურ-ბოჭკოვანი კაბელი: მრავალმოდიანი (multi-mode) და ერთმოდიანი (single mode).

შედარებით იაფ მრავალმოდიან ოპტიკურ-ბოჭკოვან კაბელში (ცენტრალური მინის ბოჭკოს დიამეტრია 50 ან 62,5 მკმ, ხოლო გარსის - 125 მკმ) სიგნალების გადასაცემად გამოიყენება ნაკლებად ძვირი, 850 ნმ ტალღის სიგრძის *შუქდიოდური ტრანსივერები.*

მაღალხარისხოვან (მაგრამ ძვირ) ერთმოდიან კაბელში მინის ბოჭკო უფრო წვრილია - დიამეტრით სულ 9-10 მკმ, მაგრამ მასში საგრძნობლად ნაკლებია სინათლის სიგნალის მილევა. გარდა ამისა, ერთმოდიანი კაბელით სიგნალების გადასაცემად გამოიყენება 1300 ნმ სინათლის ტალღის სიგრძის მქონე *ლაზერული ტრანსივერები.* შედეგად, ერთმოდიანი ოპტიკურ-ბოჭკოვანი კაბელებით სიგნალების გადაცემის მაქსიმალური მანძილი მრავალმოდიანთან შედარებით, არის გაცილებით მეტი.

ბოჭკოვან–ოპტიკური კაბელების მისაერთებლად გამოიყენება სპეციალური კონექტორები (ნახ. 4.8). FC და ST *კონექტორები* (დღეისათვის ითვლებიან მოძველებულად). უფრო ხშირად ახალ მოწყობილობებში გასართებად გამოიყენება SC *კონექტორები.* კონექტორების მონტაჟი

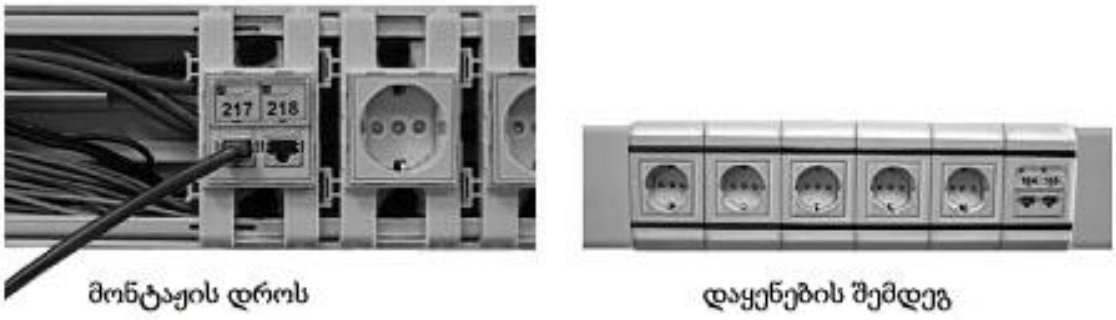
ნახ. 4.8. სხვადასხვა ტიპის ბოჭკოვან–ოპტიკური კონექტორები

(ოპტიკურ-ბოჭკოვანი კაბელების ჩამაგრება კონექტორში) საკმაოდ რთულია და მოითხოვს სპეციალურ მოწყობილობას. ბოლო დროს გამოჩნდა ინსტრუმენტების კრებულები, რომლებიც იძლევიან ოპტიკურ-ბოჭკოვანი კაბელების კონექტორში ჩამაგრების საშუალებას საშინაო პირობებში. ელექტრულ კაბელებთან შედარებით ოპტიკური ბოჭკო უზრუნველყოფს ხელშეშლებისაგან და მიტაცებისაგან დაცულობის საოცარ პარამეტრებს. გარდა ამისა, მისი გამოყენებისას მონაცემების გადაცემის მანძილი არის საგრძნობლად დიდი და თეორიულად შესაძლებელი სიჩქარეც გაცილებით მაღალია.

ბოჭკოვან–ოპტიკური კაბელების ნაკლოვანებებია: კაბელის მაღალი ღირებულება, კონექტორში ჩამაგრების სირთულე (საჭიროა მინის ბოჭკოს შედუღება) და დამატებითი ტრანსივერების საჭიროება, რომლებიც გარდაქმნიან სინათლის სიგნალებს ელექტრულში და პირიქით. ყოველივე ეს საგრძნობლად ზრდის ქსელის გაშლის საერთო ხარჯებს, ამიტომ დღემდე ოპტიკური ბოჭკო ლოკალურ ქსელებში უფრო იშვიათად გამოიყენება, ვიდრე ხვეული წყვილი.

მას შემდეგ, რაც შევარჩიეთ კაბელის საჭირო ტიპი, კომპიუტერების შევარებისათვის და დავადგინეთ კომუტაციისა და განაწილების ადგილები, შეიძლება დავიწყოთ *კაბელის გაყვანა*. შენობაში კაბელის ჩაგებისას, გაყვანილობას ჩვეულებრივ ჩაამაგრებენ კედელში, ათავსებენ სპეციალურ სივრცეებში ”ფალშიატაკის” ან ”დაკიდული ჭერის” შიგნით, და შემდეგ გამოყავთ გარეთ *კედლის ქსელური როზეტები*.

თუ კაბელის გაყვანა ვერ ხერხდება მითითებულ ადგილას, მაშინ იყენებენ კედლის (უფრო იშვიათად - იატაკის) *კაბელარხებს* (*კოლოფებს*). **კოლოფი** (box) - პლასტიკური, ჩვეულებრივად მართკუთხა, ასაწყობ-დასაშლელი ცარიელი მილი, რომელშიც გაჰყავთ ქსელური კაბელები, უფრო ხშირად ელექტრულთან ერთად (ნახ. 4.9).



ნახ. 4.9. კაბელების გასაყვანი პლასტიკური კოლოფი
(ჩაშენებული ქსელური და ელექტრული როზეტებით)

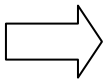
უკაბელო ქსელები

ყველა კაბელური ქსელის დამახასიათებელი ძირითადი პრობლემებია - დაბალი *მობილობა*, საკმაოდ დიდი კაპიტალ-დაბანდებები კაბელურ ინფრასტრუქტურაში და სიგნალის გადაცემის შედარებით მცირე მანძილი. უკაბელო ქსელებს ეს ნაკლებად ეხება, ამიტომ ისინი სულ უფრო მეტად შემოდიან ჩვენს ცხოვრებაში. იმისა მიუხედავად, რომ უკაბელო ქსელებში არ არსებობს ცნება "კაბელი", გადაცემის გარემო მაინც არის.

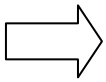
მონაცემების უკაბელო გადაცემისათვის იყენებენ რამო-დენიმე მეთოდს.

რადიოკავშირის ტექნოლოგიები მონაცემებს აგზავნიან რადიოსიხშირეებზე და პრაქტიკულად არა აქვთ შეზღუდვა სიშორის მხრივ. ისინი გამოიყენებიან როგორც ლოკალურ ქსელებში, ასევე დიდ მანძილებზე ქსელური შეერთე-ბებისათვის. რადგან რადიოსიგნალების მიტაცება ადვილია, საჭიროა მონაცემების აუცილებელი დაცვა კოდირებით და/ან დაშიფრვით.

მონაცემების გადაცემა *მიკროტალღურ დიაპაზონში* იყენებს უფრო მაღალ სიხშირეებს და გამოიყენება როგორც მოკლე მანძილებზე (სხვადასხვა შენობების ლოკალური ქსელების გაერთიანება), ასევე გლობალური კომუნიკაციებისას - თანამგზავრებისა და მიწისზედა *თანამგზავრული ანტენების* დახმარებით. ასეთი კავშირის მთავარი ნაკლია: გადამცემიც და მიმღებიც უნდა იყვნენ ერთმანეთის პირდაპირი ხედვის ზონაში.



ტექნოლოგიები, რომლებიც იყენებენ *ინფრაწითელ* (*იწ*) *გამოსხივებას*, ხშირად გამოიყენება ორმხრივი და ფართომაუწყებლური გადაცემებისათვის ახლო მანძილებზე. ჩვეულებრივად ინფრაწითელ გამოსხივებას იყენებენ საწყობებში და ოფისებში, ყველაზე ხშირად პორტატულ (მობილურ) მოწყობილობებთან ურთიერთქმედებისათვის. მიუხედავად იმისა, რომ ინფრაწითელი ქსელების სიჩქარეები და გამოყენების მოხერხებულობა ძალიან მიმზიდველია, წარმოიქმნება სიძნელეები სიგნალების 30 მეტრზე მეტ მანძილებზე გადაცემისას. ამასთან ხდება იწ-სიგნალების ბლოკირება ნებისმიერი საგნებით, და აგრეთვე განიცდიან ზემოქმედებას სინათლისა და სითბოს ძლიერი წყაროების მხრიდან, რომლებიც პრაქტიკულად ნებისმიერ შენობაშია.



უკაბელო ქსელებისათვის აგრეთვე იყენებენ *სინათლის გამოსხივებას ხილულ დიაპაზონში* (მაგალითად - ლაზერულს), თუმცა გადაცემის ეს ხერხი გამოიყენება იშვიათად. მაგრამ ის შეიძლება მოხერხებული აღმოჩნდეს მაღლივ შენობებს შორის კავშირისათვის.

”ხვეული წყვილი” 5e (ან უფრო მაღალი) კატეგორიის კაბელები დღეს ყველაზე უნივერსალური, საიმედო და გაფართოებადი გადაწყვეტილებებია ლოკალური ქსელებისადმი სტაციონარული მუშა სადგურებისა და სერვერების მისაერთებლად. სიგნალების გადასაცემად დიდ მანძილებზე, მაგალითად, ლოკალური ქსელების შეერთებისას, რომლებიც განლაგებულია სხვადასხვა შენობებში ან სხვადასხვა რაიონებში, ყველაზე ხშირად გამოიყენება ოპტიკურ-ბოჭკოვანი გაყვანილობა. მობილური მოწყობილობების (ნოუთბუკების, ტაბლეტურ კომპიუტერების ან ჯიპკ-ბის, კომუნიკატორების ან სმარტფონების) ქსელთან მიერთებას უზრუნველყოფენ რადიოსიგნალების გამოყენებით.

ქსელის აგებისათვის ჩატარებული სამუშაოების შედეგი მოცემულ ეტაპზე - გაყვანილი კაბელური ინფრასტრუქტურა და , თუ ეს საჭიროა, დაყენებული *ქსელთან უკაბელო შეღწევის წერტილები (Access Points)*.

კითხვები და დავალებები

1. რა როლს თამაშობს კოაქსიალურ კაბელში სპილენძის მავთულის ან ალუმინის ფოლგის წნული?
2. რომელ კატეგორიას მიეკუთვნება არაეკრანირებული ხვეული წყვილის კაბელი, რომელსაც შეუძლია მონაცემების გადაცემა 10 მბიტი/წმ სიჩქარით?
3. ელექტრული სიგნალის გადაცემას ესაჭიროება ორი გამტარი. სახელდობრ, რომელი გამტარები გამოიყენება კოაქსიალურ კაბელში? რისთვის გამოიყენება "ხვეული წყვილის" კაბელში გამტარების რამოდენიმე წყვილი (2 ან 4)?
4. რომელი გასართი გამოიყენება კომპიუტერთან "ხვეული წყვილის" კაბელის მისაერთებლად?
5. ლითონის კაბელებისათვის კონექტორების ძირითადი ამოცანაა - კაბელების მონაკვეთების შეერთებისას საიმედო ელექტრული კონტაქტის უზრუნველყოფა. როგორია კონექტორის ძირითადი ამოცანა ოპტიკურ-ბოჭკოვანი კაბელების შემთხვევაში?
6. რამ შეიძლება წარმოუქმნას ხელშეშლები უკაბელო ქსელის მუშაობას, თუ მასში გამოიყენება რადიოკავშირი? რამ შეიძლება წარმოუქმნას ხელშეშლები უკაბელო ქსელის მუშაობას, რომელიც ეყრდნობა ინფრაწითელი გამოსხივების გამოყენებას?
7. შეადგინეთ კაბელურ არხებში მეხუთე კატეგორიის "ხვეული წყვილის" კაბელის გაყვანის პროექტი განვითარებადი კომპანიისათვის ადრე შემუშავებული ქსელისათვის თქვენს მიერ არჩეული ტოპოლოგიის თანახმად.

თავი 5

ვაგებთ ქსელს: ქსელური არქიტექტურის არჩევა

ამ თავში
თქვენ ნახავთ პასუხებს
შემდეგ კოთხვებზე:

- როგორი ქსელური არქიტექტურები არსებობენ?
- როგორი პარამეტრებით ხასიათდება ქსელური არქიტექტურები?
- როგორი ქსელური არქიტექტურაა ყველაზე გავრცელებული?
- როგორი ტიპის გასართები (კონექტორები) არსებობენ?
- როგორ ავარჩიოთ არქიტექტურა ლოკალური ან საშინაო ქსელისათვის?

წინა თავში ჩვენ გავეცანით კაბელური შეერთებების ძირითად ტიპებს და ჩვენი ქსელისათვის ავირჩიეთ კაბელის ოპტიმალური სახეობა. მაგრამ ეს მხოლოდ დასაწყისია. ახლა უნდა ჩამოვყალიბდეთ *ქსელურ არქიტექტურაში* - ქვედა დონის სტანდარტების, ტოპოლოგიებისა და პროტოკოლების კრებულის არჩევაში, რომლებიც საჭიროა ქმედითუნარიანი ქსელის შექმნისათვის. შემდგომ ჩვენ განვიხილავთ ძირითად ქსელურ არქიტექტურებს, მათ უპირატესობებსა და ნაკლოვანებებს და ავირჩევთ მათგან საუკეთესოს: მაღალსიჩქარიანს, საიმედოდ ფუნქციონირებადს და გაფართოებადს.

ქსელური ტექნოლოგიების განვითარების მრავალი წლის განმავლობაში შემუშავდა საკმაოდ ბევრი სხვადასხვა ქსელური არქიტექტურა. ზოგი მათგანი უკვე გამოვიდა ხმარებიდან, მაშინ როცა ისეთი, როგორიცაა Ethernet, არა მხოლოდ აქტიურად გამოიყენება დღემდე, არამედ გამუდმებით უმჯობესდება.

Ethernet არქიტექტურა

Ethernet არქიტექტურა ფაქტობრივად აერთიანებს სტანდარტების მთელ კრებულს, რომელთაც აქვთ როგორც საერთო თვისებები, ასევე განსხვავებები. თავდაპირველად ის შეიქმნა ფირმა Xerox-ის მიერ 70-ან წლებში და მაშინ წარმოადგენდა 2.93 მბიტი/წმ-ში სიჩქარით გადაცემის სისტემას. საბოლოოდ დამუშავების შემდეგ Intel და DEC კომპანიების მონაწილეობით Ethernet არქიტექტურა გახდა 1985 წელს მიღებული IEEE 802.3 სტანდარტის საფუძველი, რომელიც განსაზღვრავდა შემდეგ პარამეტრებს:

- ტოპოლოგია - ”სალტე”;
- შეღწევის მეთოდი - CSMA/CD;
- გადაცემის სიჩქარე - 10 მბიტი/წმ;
- გადაცემის გარემო - კოაქსიალური კაბელი;
- ტერმინატორების გამოყენება - აუცილებელი;
- ქსელის სეგმენტის მაქსიმალური სიგრძე - 500 მ;

- ქსელის მაქსიმალური სიგრძე - 2.5კმ;
- ქსელში კომპიუტერების მაქსიმალური რაოდენობა სეგმენტზე - 100;
- ქსელში კომპიუტერების მაქსიმალური რაოდენობა - 1024;

Ethernet-ის თავდაპირველ ვერსიაში გათვალისწინებული იყო ორი სახის კოაქსიალური კაბელის გამოყენება - "სქელის" და "წვრილის" (10Base-5 და 10Base-2 სტანდარტები, შესაბამისად). მაგრამ, 90-იანი წლების დასაწყისში Ethernet ქსელების აგებისათვის გამოჩნდა სპეციფიკაციები ხვეული წყვილის (10Base-T) და ოპტიკურ-ბოჭკოვანი კაბელის (10Base-FL) გამოყენებით. მოგვიანებით, 1995 წელს გამოქვეყნდა სტანდარტი Fast Ethernet (IEEE 802.3u), რომელიც უზრუნველყოფდა მონაცემთა გადაცემის სიჩქარეებს 100 მბიტი/წმ-მდე, 1998 წელს - Gigabit Ethernet სტანდარტი (IEEE 802.3z და IEEE 802.3ab), ხოლო 2002 წელს - 10 Gigabit Ethernet სტანდარტი (IEEE 802.3ae).

5.1 ცხრილში მოყვანილია სხვადასხვა Ethernet სტანდარტების შედარება.

ცხრილი 5.1

რეალიზება	მონაცემთა გადაცემის სიჩქარე, მბიტი/წმ	ტოპოლოგია	გადაცემის გარემო	კაბელის მაქსიმალური სიგრძე, მ
Ethernet				
10Base-5	10	"სალტე"	მსხვილი კოაქსიალური კაბელი	500
10Base-2	10	"სალტე"	წვრილი კოაქსიალური კაბელი	185; რეალურად - 300-მდე
10Base-T	10	"ვარსკვლავი"	ხვეული წყვილი	100
10Base-FL	10	"ვარსკვლავი"	ოპტიკური ბოჭკო	500 (სადგური - კონცენტრატორი); 2000 (კონცენტრატორებს შორის)

რეალიზება	მონაცემთა გადაცემის სიჩქარე, მბიტი/წმ	ტოპოლოგია	გადაცემის გარემო	კაბელის მაქსიმალური სიგრძე, მ
Fast Ethernet				
100Base-TX	100	”ვარსკვლავი”	მე-5 კატეგორიის ხვეული წყვილი (გამოიყენება ორი წყვილი)	100
100Base-T4	100	”ვარსკვლავი”	მე-3, მე-4 ან მე-5 კატეგორიის ხვეული წყვილი (გამოიყენება ოთხი წყვილი)	100
100Base-FX	100	”ვარსკვლავი”	მრავალმოდიანი ან ერთმოდიანი ოპტიკური ბოჭკო	2000 (მრავალმოდიანი); 15000 (ერთმოდიანი); რეალურად - 40 კმ-მდე
Gigabit Ethernet				
1000Base-T	1000	”ვარსკვლავი”	მე-5 ან უფრო მაღალი კატეგორიის ხვეული წყვილი	100
1000Base-CX	1000	”ვარსკვლავი”	STP ტიპის სპეციალური კაბელი	25
1000Base-SX	1000	”ვარსკვლავი”	ოპტიკური ბოჭკო	220-550 (მრავალმოდიანი), ტიპის მიხედვით
1000Base-LX	1000	”ვარსკვლავი”	ოპტიკური ბოჭკო	550 (მრავალმოდიანი); 5000 (ერთმოდიანი); რეალურად - 80 კმ-მდე
10 Gigabit Ethernet				
10GBase-*x* (***x***-სტანდარტების კრებული	10000	”ვარსკვლავი”	ოპტიკური ბოჭკო	300-40000 (კაბელის ტიპისა და ლაზერის ტალღის სიგრძის მიხადვით)

აღვნიშნოთ, რომ Ethernet-ის თანამედროვე ვერსიებში ფიზიკური ტოპოლოგია "სალტე" უკვე აღარაა გათვალისწინებული. ახლა კოაქსიალურ კაბელზე აგებული ქსელების ნახვა საკმაოდ ძნელი საქმეა.

Ethernet ქსელების ძირითადი ნაკლი დაკავშირებულია CSMA/CD გარემოში შეღწევის მეთოდის გამოყენებასთან (შეგახსენებთ, ეს შემოკლება ნიშნავს: *მრავალჯერადი შეღწევა გადამტანის კონტროლითა და შეჯახებების თავიდან აცილებით*). კომპიუტერების რაოდენობის ზრდასთან ერთად იზრდება შეჯახებების რაოდენობა, რაც ამცირებს ქსელის გამტარუნარიანობას და ზრდის კადრების მიწოდების დროს. ამიტომ Ethernet ქსელებისათვის რეკომენდებულ დატვირთვად ითვლება მთელი გატარების ზოლის 30-40%-ნი დონე. აქვე აღვნიშნავთ, რომ თანამედროვე ქსელებში ეს ნაკლი ადვილად აცილებადია კონცენტრატორების *კომუტატორებით და ხიდებით* შეცვლით, რომლებსაც შეუძლიათ ორ კომპიუტერს შორის მონაცემების გადაცემის "იზოლირება" სხვებისაგან (ამ მოწყობილობების შესახებ მოგიყვებით შემდეგ თავში).

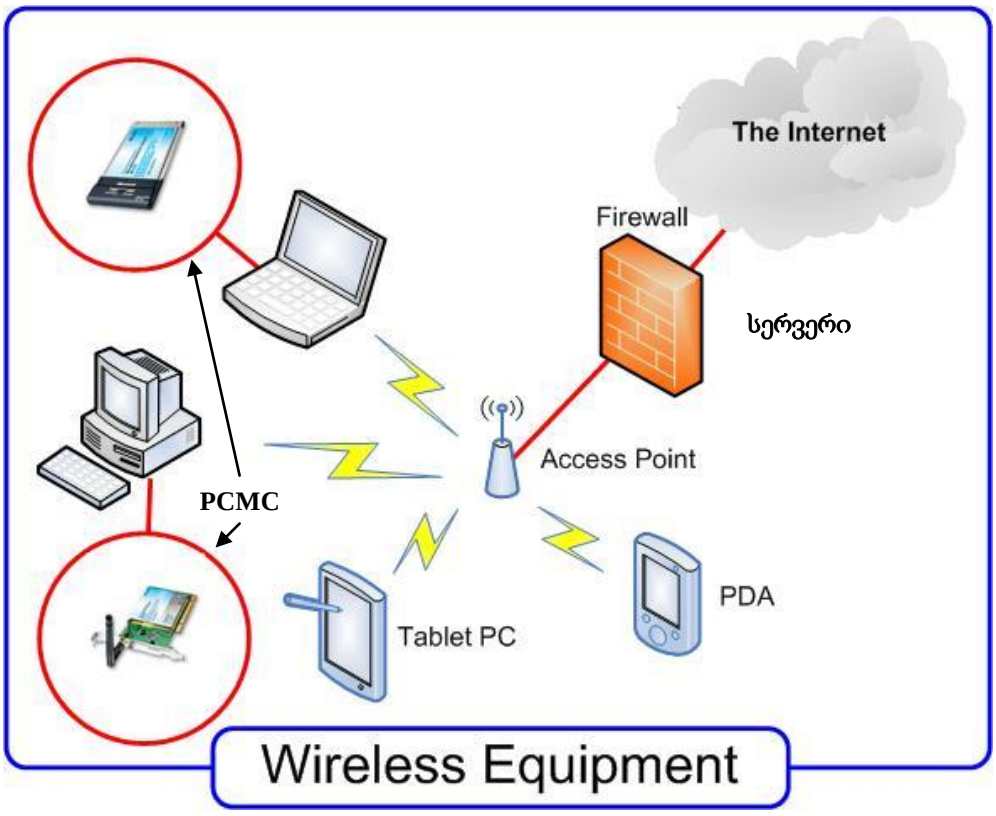
Ethernet არქიტექტურას საკმაოდ ბევრი უპირატესობა აქვს. პირველ რიგში, ეს ტექნოლოგია თავად საკმარისად მარტივია რეალიზაციაში. შესაბამისად, Ethernet-მოწყობილობები (ქსელური ადაპტერები, კონცენტრატორები, კომუტატორები და ა. შ.) სხვა ქსელური არქიტექტურების ანალოგიურ მოწყობილობებთან შედარებით გაცილებით იაფია. Ethernet ქსელებში შეიძლება პრაქტიკულად ნებისმიერი სახეების კაბელის გამოყენება, ხოლო ოპტიკურ-ბოჭკოვანი კაბელის გამოყენება ერთმანეთისგან დიდი მანძილებით დაშორებული ქსელების გაერთიანების საშუალებას იძლევა. ბოლოს, ძალიან მაღალია Ethernet ქსელების სხვადასხვა ვარიანტების თავსებადობა, რაც საშუალებას იძლევა არა მხოლოდ გავზარდოთ ქსელის სიმძლავრეები არსებული კაბელური ინფრასტრუქტურის გამოყენებით, არამედ ადვილია ქსელის გაფართოებაც, მიუერთებთ რა მას ახალ, სულ უფრო მაღალსიჩქარიან სეგმენტებს. დღეისათვის Ethernet არქიტექტურა გაბატონდა არა მხოლოდ ლოკალურ ქსელებში, არამედ გამოდევნა სხვა ტექნოლოგიები რეგიონალურ და გლობალურ ქსელებშიც.

უკაბელო ქსელები

გადავიდეთ ახლა უკაბელო ქსელურ გადაწყვეტილებებზე.

2010 წლის 11 ოქტომბერს ანონსირებულია ახალი ოპერაციული სისტემა Windows Phone 7 მობილური ტელეფონებისათვის (კლიენტური მოწყობილობებისათვის).

თქვენ შეგიძლიათ გამოიყენოთ უკაბელო მოწყობილობები მრავალნაირად და ნახოთ უკაბელო ტექნოლოგია ბევრ ადგილას. ნახავთ ადამიანებს, რომლებიც იყენებენ უკაბელო ტექნოლოგიას ნოუთბუკებში, პირად ციფრულ თანაშემწეებში (personal digital assistants, PDAs), დაფისებურ პერსონალურ კომპიუტერებში (Tablet PC ; ზოგიერთ ქვეყნებში პლანშეტურს უწოდებენ), მობილურ ტელეფონებში და ავტომობილებშიც კი. ნახ. 5.1 გვიჩვენებს დღეს პოპულარული უკაბელო მოწყობილობების ნაწილს. კლიენტური მოწყობილობები უკავშირდებიან შეღწევის წერტილს (Access Point) და მისი მეშვეობით ინტერნეტს, როგორც ჩაშენებული, ასევე სპეციალურ პორტში ჩადგმული ადაპტერებით - ქსელური ბარათებით (Personal Computer Memory Card, PCMC).



ნახ.5.1. უკაბელო აღჭურვილობა

ლოკალურ ქსელებში დღეს ყველაზე ხშირად გამოიყენება უკაბელო ტექნოლოგიები Wi-Fi და Bluetooth.

Wi-Fi (“Wireless Fidelity”-ს შემოკლებაა, ”უკაბელო სიზუსტე”) - მსოფლიოში პოპულარული და საქართველოში სწრაფად განვითარებადი უკაბელო 4G გადაწყვეტილება. სინამდვილეში ”Wi-Fi”-ს სახელწოდების ქვეშ იმალება უკაბელო ქსელებისათვის შემუშავებული რამოდენიმე სტანდარტი, რომლებიც გამოშვებულია ჯერ კიდევ 1997 წელს IEEE 802.11 სპეციფიკაციის საფუძველზე (ტაბულა 5.2).

ტაბულა 5.2

ყველაზე მნიშვნელოვანი IEEE 802.11x სტანდარტები

სტანდარტი	გადაცემის გარემო	გადაცემის სიჩქარე, მბიტი/წმ	შენიშვნა
IEEE 802.11	მიახლოებით 2.4 გჰც სიხშირის რადიოსიგნალი ან იწ-გამოსხივება	1 ან 2	საბაზო სტანდარტი, რომელიც განაპირობებს ურთიერთქმედებას OSI მოდელის საარხო და ფიზიკურ დონეებზე
IEEE 802.11a	მიახლოებით 5 გჰც სიხშირის რადიოსიგნალი	54-მდე	შეუთავსებადია IEEE 802.11b და g სტანდარტებთან
IEEE 802.11b	2.4-2.483 გჰც სიხშირის რადიოსიგნალი	11-მდე	აქვს შედარებით დაბალი სიჩქარე და დაცულობა (დაცვა WEPდაშიფრვის ტექნოლოგიით – Wireless Equivalent Privacy). სხვა სტანდარტებთან შედარებით უზრუნველყოფს მონაცემთა გადაცემის რამდენადმე დიდ მანძილს
IEEE 802.11g	2.4-2.483 გჰც სიხშირის რადიოსიგნალი	54-მდე	უზრუნველყოფს უკუთავსებადობას IEEE 802.11b სტანდარტთან, თუმცა ხასიათდება მეტი სიჩქარით და დაცულობით (გარდა WEP-სა, მხარდაჭერილია WPA დაცვის სტანდარტი – Wi-Fi Protected Access)
IEEE 802.11n	- || -	480-მდე	- || -

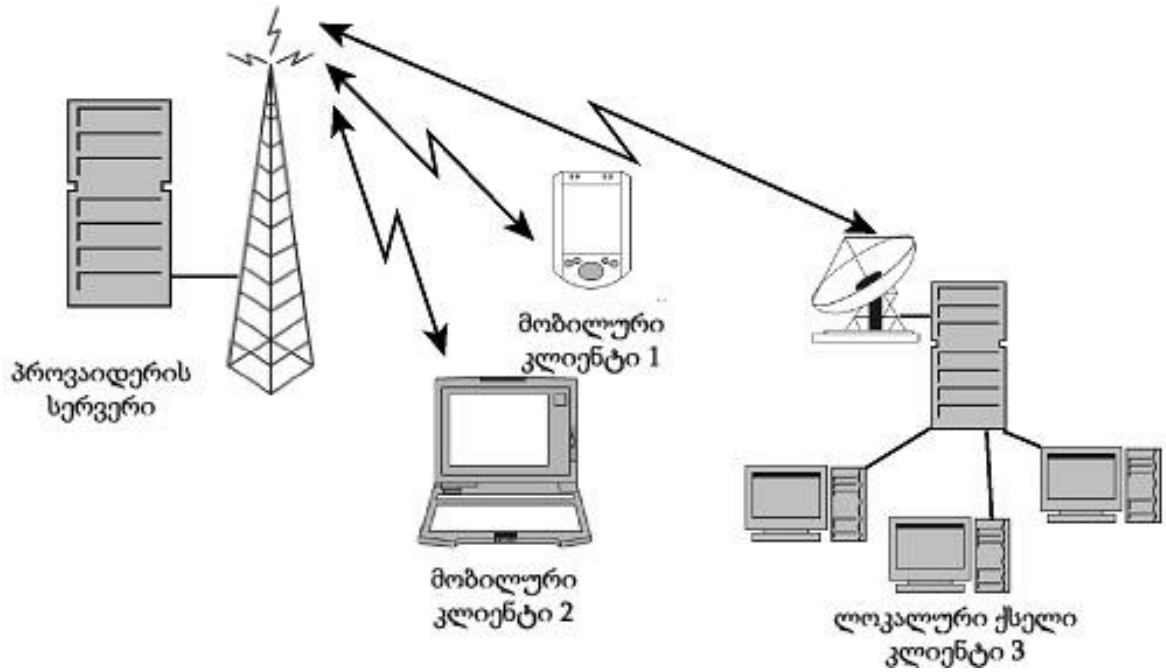
მნიშვნელოვანია აღინიშნოს, რომ 802.11 სტანდარტში გათვალისწინებულია მხოლოდ *ნახევრადდუპლექსური მიმღებ-გადამცემების* გამოყენება, რომლებსაც არ შეუძლიათ ერთდროულად ინფორმაციის გადაცემა და მიღება. ამის გამო 802.11 უკაბელო ქსელებში გადაცემისას სადგურს პრინციპულად არ შეუძლია შეჯახების აღმოჩენა, რადგან ამ დროს არ აქვს მონაცემების მიღების საშუალება. ამიტომ გარემოში შეღწევის

მეთოდად ყველა სტანდარტში გამოიყენება CSMA/CA მეთოდი (კოლიზიების თავიდან აცილებით), რომელიც საშუალებას იძლევა თავიდან ავიცილოთ შეჯახებები. ამას მივყავართ ურთიერთქმედებისას დამატებითი სირთულეებისაკენ და, შედეგად, მონაცემთა გადაცემის საგრძნობლად ნაკლები სიჩქარეებისაკენ, ვიდრე, მაგალითად, Ethernet ტექნოლოგიაში.

Wi-Fi ქსელების ძირითადი ნაკლი იყო მონაცემების გადაცემის მცირე სიშორე, რომელიც მოწყობილობათა უმრავლესობისათვის არ აღემატებოდა 150 მ (მაქსიმუმ 300 მ) ღია სივრცეში ან მხოლოდ რამოდენიმე ათეულ მეტრს - შენობაში.

დღეს უკვე არსებობს Wi-Fi IEEE 802.11n სტანდარტი, რომლითაც მონაცემების გადაცემის მაქსიმალური (თეორიული) სიჩქარეა 480 მბიტი/წმ, ხოლო გადაცემის სიშორე რამოდენიმე კილომეტრს აღწევს საშუალედო Access Point-ის ან მსგავსი მოწყობილობის გარეშე.

გარდა ამისა აღნიშნავია WiMAX (Worldwide Interoperability for Microwave Access) და LTE (Long Term Evolution) არქიტექტურები, რომლების სტანდარტები



ნახ. 5.2. WiMAX (LTE) უკაბელო 4G ქსელი

შემუშავებულია IEEE 802.16 და 3GPP (3G Partnership Program) მუშა ჯგუფების ფარგლებში, შესაბამისად. ამ ტექნოლოგიების რეალიზება, რომლებიც გადაცემის გარემოდ იყენებენ რადიოსიგნალებს, საშუალებას მისცემს მომხმარებლებს მიიღონ მაღალსიჩქარიანი უკაბელო შეღწევა ინტერნეტში რამოდენიმე ათეული კილომეტრის მანძილებზე (ნახ. 5.2). აღსანიშნავია, რომ LTE არის მობილური შეღწევის არქიტექტურა, ხოლო WiMAX არქიტექტურის სტანდარტებში მობილური ვერსიაა IEEE 802.16e,m.

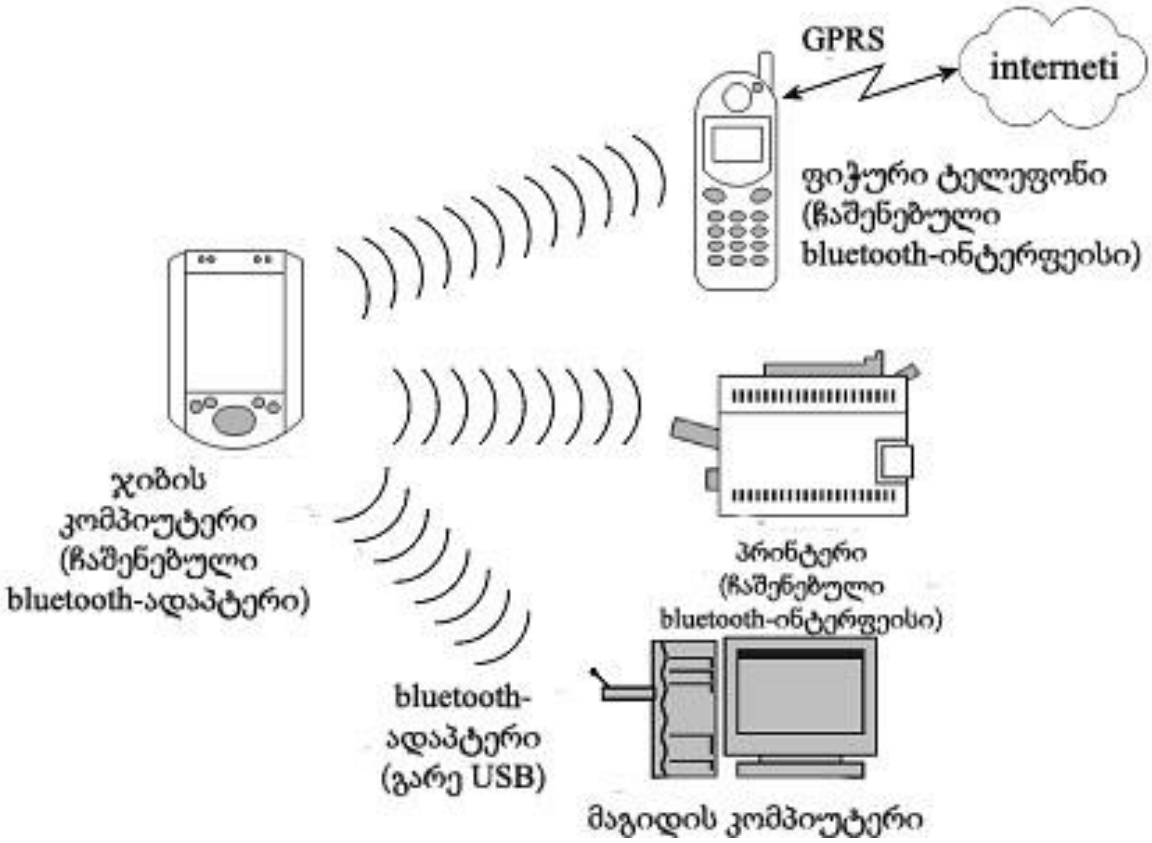
დაბოლოს, აღნიშვნის ღირსია პოპულარული უკაბელო არქიტექტურაა - **Bluetooth ტექნოლოგია** (IEEE 802.15.1 სტანდარტი) და აგრეთვე **ტექნოლოგია ZigBee.**

ისევე როგორც Wi-Fi-ში, Bluetooth-შიც გამოიყენება 2.4 გჰც სიხშირის რადიოსიგნალი, მაგრამ ეს სტანდარტები არ არიან ერთმანეთთან თავსებადი. Bluetooth-ი ხასიათდება საკმაოდ დაბალი ენერგომოხმარებით, რაც საშუალებას იძლევა წარმატებით გამოვიყენოთ იგი გადასატან მოწყობილობებში - ნოუთბუკებში, ჯიპკ-ში და მობილურ ტელეფონებში (ნახ. 5.3). ამასთან Bluetooth-სს პრაქტიკულად არ ესაჭიროება "აწყობა" - ეს სტანდარტი საშუალებას აძლევს მოწყობილობებს დაამყარონ ერთმანეთთან ურთიერთქმედება მომხმარებლის მინიმალური ჩარევით. მეორეს მხრივ, Bluetooth-ს აქვს დაბალი მაჩვენებლები გადაცემის სიშორისა და გატარების ზოლის მხრივ - არა უმეტეს 10 მეტრისა და 400-700 კბიტი/წმ, - რაც მკვეთრად ამცირებს ამ ტექნოლოგიის გამოყენების საშუალებას ლოკალურ ქსელებში.

ZigBee ტექნოლოგიის მაჩვენებლები, რომელიც ცოტა ხნის წინ გამოჩნდა რამდენიმე მსხვილი ტელეკომუნიკაციური კომპანიის ძალისხმევით (სტანდარტი IEEE 802.15.4), უფრო "მოკრძალებულია" - სპეციფიკაცია ითვალისწინებს მონაცემების დაცულ გადაცემას 10-75 მეტრის რადიუსში და 250 კბიტი/წმ-ში მაქსიმალური სიჩქარით. შეიძლება ვიფიქროთ, რა საჭიროა ასეთი ტექნოლოგია, თუ მასში გადაცემის სიჩქარეები უფრო ნაკლებია ვიდრე Bluetooth-ში? ZigBee მოწყობილობების "პეწი" მდგომარეობს ზედაბალ ენერგომოხმარებაში და "მიძინების" რეჟიმში გადასვლის შესაძლებლობაში, როდესაც მონაცემების გადაცემა არ არის საჭირო. ამიტომ ZigBee-მოწყობილობების გამოყენების ძირითადი სფერო გახდება არა ლოკალური ქსელები, არამედ აპარატურის მონიტორინგისა და კონტროლის სისტემები, მათ შორის საქსელო მოწყობილობებისაც.

Wireless USB – Bluetooth-ს ალტერნატივა

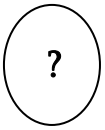
Wireless USB ტექნოლოგია ეფუძნება ულტრაფართოზოლიანი უკაბელო კავშირგაბმულობის გამოყენებას - UWB და უზრუნველყოფს მონაცემთა მოკლე მანძილებზე (10 მ-დე) გადაცემის ზესიჩქარიან (480 მბიტი/წმ, ხოლო პერსპექტივაში - 1გბიტი/წმ-დე). ის იძლევა პერიფერიული მოწყობილობების უკაბელო მიერთების საშუალებას, USB 2.0-ს ანალოგიურად. Wireless USB ადაპტერის პირველი სერიული ნიმუში წარმოდგენილი იყო შემმუშავებლებისათვის Intel-ის ფორუმზე (IDF 2005).



ნახ. 5.3. Bluetooth ქსელი

!

ძირითადი ტექნოლოგია, რომელიც დღეს გამოიყენება კაბელიან ქსელებში, არის Ethernet-ი. მნიშვნელოვანია მხოლოდ ქსელში გამოსაყენებელი კონკრეტული სტანდარტის ან სტანდარტების კრებულის დადგენა და საჭირო მოწყობილობების შეძენა. ამასთანავე რეკომენდაციები საკმარისად მარტივია: უნდა აირჩეს ჩქაროსნული და საიმედო მოწყობილობები, რომლებიც დამაკმაყოფილებელია ფასით. სასურველია, ეს მოწყობილობები იყოს მაქსიმალურად ფუნქციონალური და მართვადი, მაგრამ ეს კრიტერიუმები განსაკუთრებით მნიშვნელოვანია მსხვილი კორპორატიული ქსელების ქსელური ადმინისტრატორებისათვის. უკაბელო კლიენტების მიერთებისათვის საჭიროა Wi-Fi ტექნოლოგიერბი, თანაც უნდა აირჩეს მოწყობილობები, რომლებიც მხარს უჭერენ ბოლო IEEE 802.11n სტანდარტს, - მასში უზნველყოფილია მონაცემთა გადაცემის საკმარისი სიჩქარე და, რაც ყველაზე მთავარია, მათი საიმედო დაცვა.



კითხვები გამეორებისათვის

1. როგორი ქსელური არქიტექტურებია თქვენთვის ცნობილი? როგორია მათი უპირატესობები და ნაკლოვანებები?
2. რატომა არის დღეს ყველაზე მეტად გავრცელებული Ethernet არქიტექტურა?
3. Ethernet არქიტექტურის როგორი ნაირსახეობებია თქვენთვის ცნობილი?
4. როგორი უკაბელო არქიტექტურებია თქვენთვის ცნობილი?
5. როგორი ქსელური არქიტექტურების გამოყენებაა უკეთესი თქვენი აზრით:
   - ლოკალური ქსელის შექმნისას მსხვილ ოფისში?
   - საშინაო ქსელის გაშლისას ქალაქის ბინაში (ტელეფონით)?
   - საშინაო ქსელის გაშლისას სოფლის სახლში (არატელეფონიზირებულში)?
   - მობილური კომპიუტერების (ჯკპკ) ქსელში გაერთიანებისას სავაჭრო ცენტრის ან საწყობის ტერიტორიაზე?
   - მონაცემთა შეგროვების ორგანიზებისას საველე პირობებში დაბის ტერიტორიაზე ან სოფლის მიდამოებში?
6. იპოვეთ ინტერნეტში ყველაზე ახალი ინფორმაცია კაბელური და უკაბელო ქსელების შედარების შესახებ.

თავი 6

ვაგებთ ქსელს: კავშირგაბმულობის მოწყობილობების არჩევა

ამ თავში თქვენ ნახავთ პასუხებს შემდეგ კითხვებზე:

- **რა არის ქსელური ადაპტერი და რა ფუნქციებს ასრულებს ის?**
- **როგორი მოწყობილობებია პასუხისმგებელი კომპიუტერების ქსელთან კავშირისათვის?**
- **რა მსგავსება და განსხვავებაა ისეთ მოწყობილობებს შორის როგორებიცაა კონცენტრატორები, ხიდები, კომუტატორები და რაბები?**
- **როგორ ავირჩიოთ სწორად კავშირგაბმულობის მოწყობილობა?**

გავაანალიზეთ რა წინა თავში განხილული ქსელური არქიტექტურები, გადავწყვიტეთ ჩვენს ქსელში გამოგვეყენებინა Ethernet ტექნოლოგია (”ხვეული წყვილის” საფუძველზე) და Wi-Fi. ჩავთვალოთ, რომ კაბელური ინფრასტრუქტურა გვაქვს მზად - საჭირო ადგილებში გაყვანილია კაბელები, დამონტაჟებულია ქსელური მოწყობილობებისათვის როზეტები და პანელები. ახლა შევარჩიოთ მოწყობილობები, რომლებიც მოგვცემენ საშუალებას ერთ ქსელში გავაერთიანოთ კომპიუტერები (სტაციონარული კომპიუტერები და სერვერები, ნოუთბუქები, „დაფური“ („ტეიბლიტური“, „პლანშეტური“) კომპიუტერები, სმარტფონები და სხვა).

ვდგამთ ქსელურ ადაპტერს

დავიწყოთ კომპიუტერებით. ქსელთან ურთიერთქმედებისათვის კომპიუტერს ესაჭიროება რაიმე *ქსელური ადაპტერი* (კაბელიანი ან უკაბელო). ჩვეულებრივ აქ პრობლემები არ წარმოიქმნება - თანამედროვე კომპიუტერების აბსოლუტურ უმრავლესობაში ჩაშენებულია ქსელური Ethernet და Wi-Fi ადაპტერები, რომლებიც ინტეგრირებული არიან motherboard-ში (ხანდახან - რამოდენიმეც კი). არაუშავს, თუ თქვენს კომპიუტერში არ აღმოჩნდება საჭირო ქსელური ადაპტერი, - ის შეიძლება იოლად შეიძინოთ ნებისმიერ კომპიუტერულ მაღაზიაში და ჩააყენოთ კომპიუტერის გაფართოების სლოტში ან USB პორტში.

გარდა ამისა, უნდა დავაყენოთ *ქსელური ადაპტერის დრაივერი* - სპეციალური პროგრამული უზრუნველყოფა, რომელიც ოპერაციულ სისტემას (ოს) საშუალებას მისცემს იმუშაოს ამ მოწყობილობასთან. როგორც წესი, თანამედროვე ოს (მაგალითად Windows XP) თვითონ ამოიცნობს მოწყობილობას და აყენებს მისთვის საჭირო დრაივერს. თუ-კი ეს არ მოხდა (ან ავტომატურად დაყენებული დრაივერით ქსელი არ მუშაობს), მაშინ დრაივერი უნდა დავაყენოთ ხელით დისკეტიდან, რომელიც შედის ადაპტერის მოწოდების კომპლექტში.

ქსელური ადაპტერი და დრაივერი მუშაობენ OSI მოდელის *ფიზიკურ დონეზე* და *გარემოსადმი შეღწევის მართვის ქვედონეზე (MAC)* უზრუნველყოფენ რა ფიზიკური და ქსელური დონეების ურთიერთქმედებას.

შესაბამისად, ადაპტერს უნდა ჰქონდეს კონექტორის მისაერთებლად საჭირო გასართი (ჩვეულებრივად RJ-45), და აგრეთვე უნიკალური ფიზიკური (ანუ "MAC") მისამართი, რომელიც გამოიყენება *ქსელის მოცემულ სეგმენტში კომპიუტერის ცალსახა იდენტიფიკაციისათვის*. ჩვეულებრივ ამ მისამარს დანიშნავს მწარმოებელი ადაპტერის დამზადებისას, მაგრამ ადაპტერების ზოგიერთი მოდელის მიერ დაშვებულია MAC-მისამართის ხელით შეცვლა, მაგალითად ადაპტერის BIOS აწყობების მეშვეობით ან სპეციალური პროგრამის დახმარებით.

თუ კომპიუტერზე Windows 2000 ან XP ოპერაციული სისტემით დაყენებულია პროტოკოლი TCP/IP, მაშინ ამ კომპიუტერში დაყენებული MAC-მისამართები ადვილად შეგვიძლია დავადგინოთ მთელი რიგი INCONFIG, NBSTAT, ROUTE PRINT, NETSTAT, NET CONFIG უტილიტების დახმარებით. საკმარისია საბრძანებო მწკრივში გავცეთ ბრძანება

INCONFIG/ALL

და ეკრანზე გამოტანილ ტექსტში ყურადღება მივაქციოთ პარამეტრს "ფიზიკური მისამართი".

Windows XP ოპერაციულ სისტემაში ამის გაკეთება უფრო ადვილია - საკმარისია ორჯერ დავაწკაპუნოთ თაგვით მიერთების ღილაკს ფანჯარაში **ქსელური შეერთებები** (**Local Area Connection** - თუ პროგრამა ინგლისურენოვანია და **Подключение по локальной сети** თუ - რუსულენოვანია) - ორ ერთად მყოფ პატარა ეკრანს, და გახსნილ ადაპტერის მდგომარეობის ფანჯარაში ავირჩიოთ ჩასმა **მხარდაჭერა** (**Support** ან **Поддержка**) და მასში დავაჭიროთ ღილაკს **დაწვრილებები** (**Details** ან **Подробности**).

ვირჩევთ კავშირგაბმულობის მოწყობილობას

ადრე ჩვენ უკვე ვახსენეთ სხვადასხვა ტიპის მოწყობილობები, რომლებიც გამოიყენება ქსელებში კომპიუტერების დასაკავშირებლად. ახლა განვიხილოთ ისინი დაწვრილებით, რადგან ტელეკომუნიკაციური მოწყობილობების სწორ არჩევანზე დამოკიდებულია არა მხოლოდ ხარისხი და ქსელის მუშაობის სიჩქარე, არამედ მისი შემდგომი გაფართოების შესაძლებლობაც.

!

იმისათვის, რომ ქსელით გავაერთიანოთ *ორი* კომპიუტერი (მაგალითად, სახლის ქსელში), ტელეკომუნიკაციური მოწყობილობები საერთოდ არ არის საჭირო - საკმარისია ურთიერთთავსებადი ქსელური ადაპტერების არსებობა. Ethernet ქსელის გამოყენებისას ჩვენ დაგვჭირდება *ჯვარედინი კაბელი* (თუ როგორ დავამზადოთ ის, ნათქვამი იყო მე-4-ე თავში), რომელიც საკმარისია ჩაისვას ქსელური ადაპტერების RJ-45 გასართებში. Wi-Fi-ს გამოყენებისას უკაბელო ადაპტერები უნდა გადაირთოს Ad-Hoc სპეციალურ რეჟიმში, რომელიც უზრუნველყოფს კომპიუტერების ერთმანეთთან პირდაპირ ურთიერთქმედებას. აღვნიშნოთ, რომ ასეთი ხერხით უკაბელო ადაპტერებთან შეიძლება რამოდენიმე კომპიუტერის შეერთებაც, მაგრამ ასეთ ქსელში კომპიუტერების რიცხვის ზრდასთან ერთად მონაცემთა გადაცემის სიჩქარე დაიწყებს შემცირებას.

კონცენტრატორები (გამმეორებლები)

უმარტივესი მოწყობილობა, რომელიც უზრუნველყოფს კომპიუტერების ერთმანეთთან კავშირს, არის *კონცენტრატორი* ანუ "ჰაბი" (hub), ან *რეპიტერები* (*repeater*). ქსელებში, რომლებიც იყენებენ კოაქსიალურ კაბელს, მიღებულია რომ კონცენტრატორებს უწოდებენ გამმეორებლებს, ანუ *რეპიტერებს* (*repeater*).

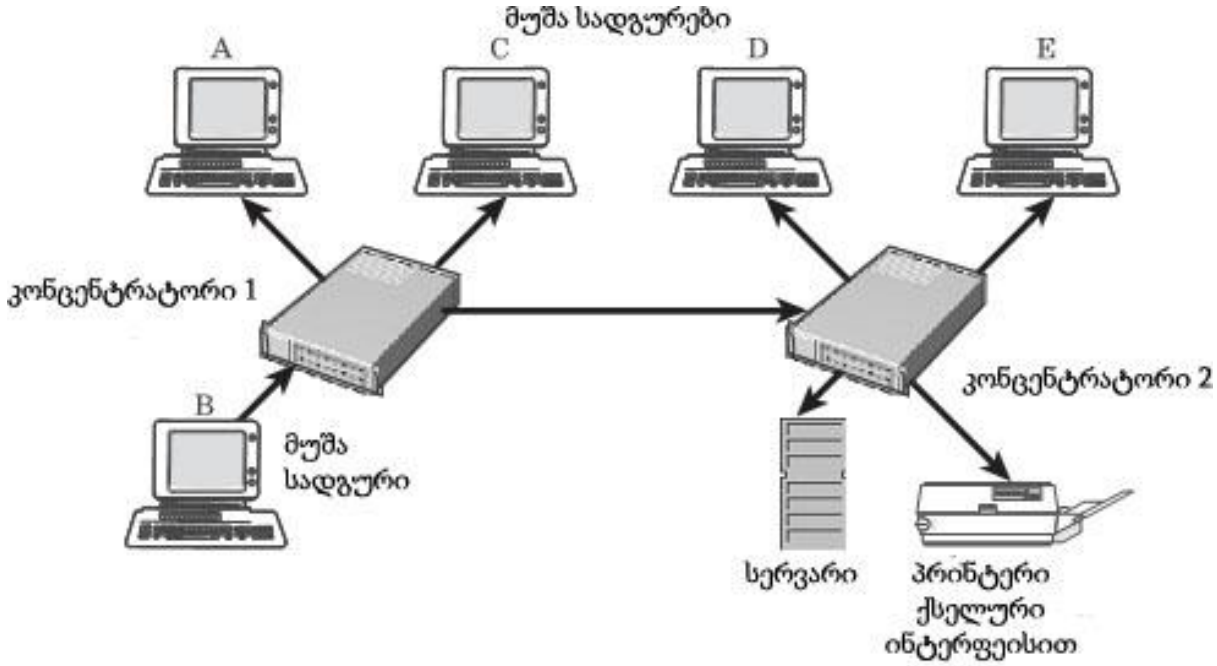
ჩვეულებრივ, კონცენტრატორს აქვს 4-დან 32-მდე ბუდე (*პორტი*) სხვადასხვა ტიპის კონექტორების მისაერთებლად. უმრავლეს შემთხვევებში, რათქმა უნდა, ეს იქნება ბუდეები RJ-45 კონექტორებისათვის, მაგრამ არსებობენ *ჰიბრიდული კონცენტრატორები* RJ-45 და BNC პორტებით, რომლებიც იძლევიან Ethernet 10Base-T და 10Base-2 სტანდარტების სეგმენტების გაერთიანების საშუალებას. პორტებს შეიძლება მივუერთოთ არა მხოლოდ კომპიუტერები, არამედ სხვა კონცენტრატორები. ასე ვაყალიბებთ *კონცენტრატორების ჯაჭვებს* (კასკადებს) ან უფრო რთულ, "ხის" ტიპის ტოპოლოგიებს.

!

10Base-5 და 10Base-2 სტანდარტებში კონცენტრატორების ასეთ კასკადირებაზე მოქმედებდა მკაცრი შეზღუდვები, რომლებიც აღიწერებოდა "5-4-3 წესით": ქსელში არ შეიძლებოდა ყოფილიყო 5 სეგმენტზე მეტი, შეერთებული 4 რეპიტერით, მხოლოდ 3 სეგმენტში დაიშვებოდა კომპიუტერების ჩართვა. 10Base-T სტანდარტის ქსელებში

დასაშვებია მაქსიმუმ 5 სეგმენტი. 100Base-T სტანდარტში ყველაფერი უფრო რთულად იყო - I კლასის კონცენტრატორების კასკადირება, რომლებიც მხარს უჭერდნენ ერთდროულად 100Base-T4, 100Base-TX100 და Base-FX მოწყობილობებთან მუშაობას, საერთოდ არ შეიძლებოდა, ხოლო II კლასის კონცენტრატორების გაერთიანება შესაძლებელია მხოლოდ წყვილ-წყვილად. ამაში მდგომარეობდა კონცენტრატორების საფუძველზე აგებული ქსელების პირველი პრობლემა - მსხვილი ქსელის აგება შეუძლებელია მხოლოდ კონცენტრატორებით.

კონცენტრატორები მუშაობენ OSI მოდელის ფიზიკურ დონეზე (იხ. ნახ. 6.4), არიან საკმარისად პრიმიტიული *აქტიური მოწყობილობები* (მოითხოვენ ელექტრულ ქსელთან მიერთებას). მათი ძირითადი ამოცანაა - ერთი კომპიუტერიდან წამოსული *ელექტრული სიგნალის მიღება, გაძლიერება და რეტრანსლირება* ყველა დანარჩენ აქტიურ პორტში (ნახ. 6.1). კონცენტრატორში სიგნალი არავითარ სხვა დამუშავებას არ განიცდის, არ ხდება მისი ბუფერიზაცია, კოლიზიები არ მუშავდება, მიუხედავად იმისა, რომ მრავალ მოდელზე არის შეჯახებების დონის ინდიკატორი. აქედან გამომდინარეობს



ნახ. 6.1. კონცენტრატორების მეშვეობით მონაცემების გადაცემის მაგალითი

მეორე ძირითადი პრობლემა, რომელსაც ადრე თუ გვიან წააწყდებიან ქსელების ადმინისტრატორები, რომლებიც იყენებენ მხოლოდ კონცენტრატორებს. წარმოიქმნება შეჯახებების ძალიან დიდი რაოდენობა, რომლებიც იზრდება ქსელში სეგმენტების და კომპიუტერების რაოდენობის ზრდასთან ერთად (გავიხსენოთ, რომ Ethernet ქსელში გამოიყენება შეღწევის CSMA/CD მეთოდი). ქსელის ასეთი ქცევა სპეციალური ტერმინითაც კი აღწერება: ამბობენ, რომ კონცენტრატორები *აყალიბებენ "შეჯახებების არეს"* (Collision Domain), ამიტომ დღეს ქსელებში კონცენტრატორები პრაქტიკულად არ გამოიყენება - ისინი გამოდევნეს ჯერ *ხიდებმა*, ხოლო შემდეგ *კომუტატორებმა*.

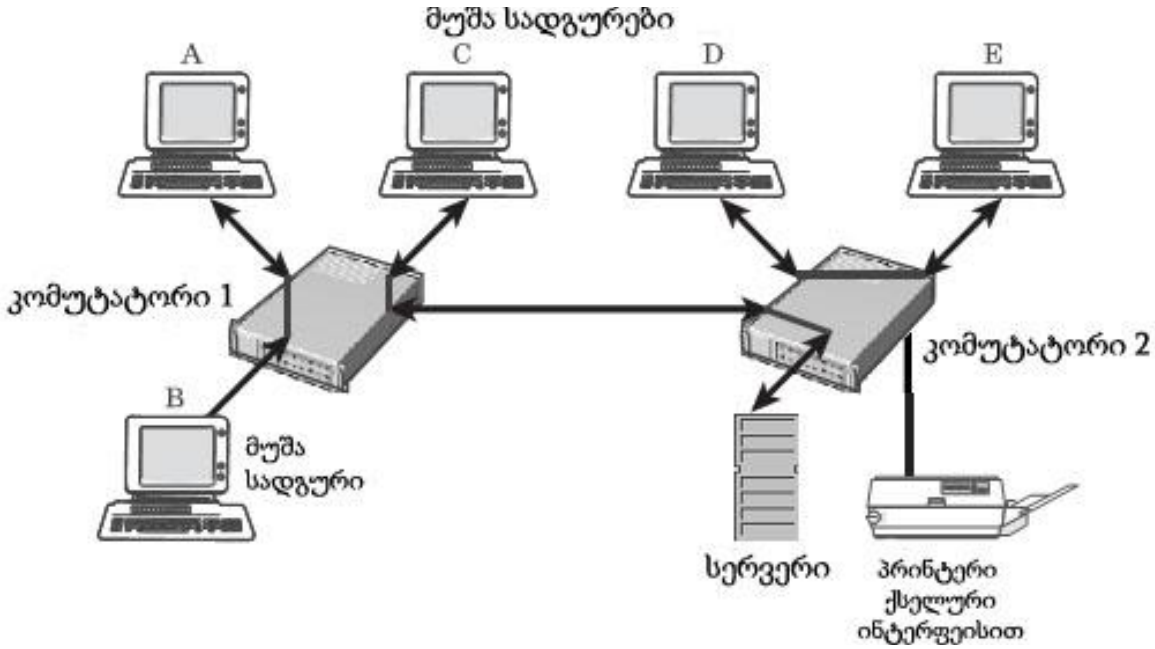
ხიდები და კომუტატორები

ხიდები (*bridge*), და შემდეგ *კომუტატორები* (*switch*) შემოიტანეს ქსელების გასაერთიანებლად და კოლიზიების დიდი რაოდენობის წარმოქმნის პრობლემების გადასაწყვეტად. ამ მოწყობილობების არსებითი განსხვავება კონცენტრატორებისაგან არის ის, რომ მათ შეუძლიათ სიგნალების წყაროსა და მიმღების MAC-მისამართების დადგენა, აგრეთვე *თავისი პორტებისა და ქსელში გამოყენებული MAC-მისამართების შესაბამისობისი ტაბულის* მხარდაჭერა. ასეთ ტაბულას ხიდი (ან კომუტატორი) აყალიბებს ჩართვისთანავე შემდეგი პრინციპით - ღებულობს თუ არა პორტი პასუხს გარკვეული ფიზიკური მისამართის მქონე მოწყობილობისაგან, ტაბულაში ჩნდება შესაბამისობის სტრიქონი: "MAC-მისამართი ↔ პორტი".

ამგვარად, ეს მოწყობილობები მუშაობენ OSI მოდელის *არა მარტო ფიზიკურ დონეზე, არამედ საარხოზეც*, - უფრო ზუსტად, *გარემოსთან შეღწევის მართვის ქვედონეზე* (*MAC*). მიიღებს რა კადრს და დაადგენს დანიშნულების მისამართს, ხიდი ან კომუტატორი ახდენს კადრის ტრანსლირებას მხოლოდ იმ პორტში, რომელთანაც ეს MAC-მისამართი არის მისადაგებული შესაბამისობების ტაბულაში. კადრებს, რომელთა გადაცემა ხდება ერთი სეგმენტის კომპიუტერებს შორის, კომუტატორი ღებულობს, მაგრამ მათ ტრანსლირებას არსად არ ახდენს (ნახ. 6.2).

ყველა პორტისათვის გადაცემული ერთადერთი სახის სიგნალები მხოლოდ მისამართებისათვის განკუთვნილი კადრებია, რომელთაც ჯერ არა აქვთ ჩანაწერი შესაბამისობების

ტაბულაში და *სპეციალური ფართომაუწყებლობის შეტყობინებები*, რომლებიც განკუთვნილია ლოკალური ქსელის ყველა კომპიუტერისათვის. ხიდებისა და კომუტატორების მუშაობის ამ თავისებურების აღსანიშნავად ამბობენ, რომ ისინი აყალიბებენ "*ფართომაუწყებლობის არეს*" (*Broadcast Domain*).



A და B *კომპიუტერებს შორის მონაცემთა გაცვლა* ***არანაირად არ მოქმედებს*** C *კომპიუტერის სერვერთან ურთიერთქმედებაზე, ისევე როგორც D და E კომპიუტერების ურთიერთკავშირზე.*

ნახ.6.2. კადრების გადაცემა კომუტატორების დახმარებით

ხიდებსა და კომუტატორებს შორის განსხვავება იმაში მდგომარეობს, რომ ხიდს დროის ყოველ მომენტში შეუძლია გადასცეს მხოლოდ ერთი კადრი (ემსახურება გადაცემას ერთი კომპიუტერიდან მეორესკენ), ამიტომ ხიდების პირველი მოდელები იყო ორპორტიანი. კომუტატორს კი შეუძლია პორტებს შორის დიდი რაოდენობის კავშირგაბმულობის ვირტუალური არხის ჩამოყალიბება (ე. ი. პორტების

კომუტირება ერთმანეთთან, აქედანაა მოწყობილობის სახელწოდებაც), აწარმოებს რა სხვადასხვა პორტებიდან შემოსული კადრების *პარალელურ დამუშავებას*. ბუნებრივია, რომ ქსელების წარმადობა, რომლებიც აგებულია კომუტატორების ბაზაზე, არსებითად დიდია.

ხაზი უნდა გაუსვათ იმას, რომ თანამედროვე ქსელების აბსოლუტური უმრავლესობა იგება სწორედ კომუტატორებზე, მაშინ როდესაც კონცენტრატორის ან ხიდის ნახვა საკმოდ ძნელია.

მარშრუტიზატორები

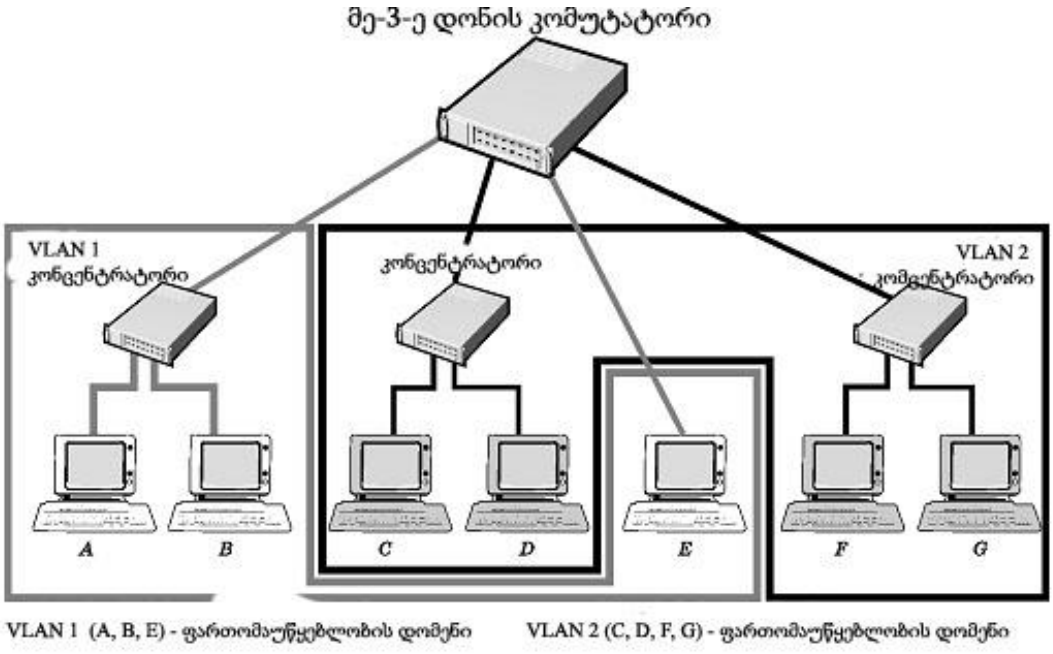
მარშრუტიზატორები მუშაობენ OSI მოდელის კიდევ უფრო მაღალ - *ქსელურ* დონეზე (იხ. ნახ. 6.4). მათ ამოცანაში შედის მისამართების ანალიზი, რომლებიც გამოიყენება ამ დონის პროტოკოლში (მაგალითად, IP-მისამართების) და დანიშნულების ადგილზე *მონაცემთა პაკეტის მიტანის საუკეთესო მარშრუტის* დადგენაში (მარშრუტიზაციის შესახებ უფრო დაწვრილებით მოთხრობილ იქნება შემდეგ თავებში). რათქმა უნდა, მარშრუტიზატორები მუშაობენ OSI მოდელის უფრო დაბალ დონეებზეც - ისინი, როგორც კონცენტრატორები აღადგენენ გადასაცემი სიგნალის დონესა და ფორმას, ხოლო როგორც ხიდები და კომუტატორები იძლევიან შეჯახებების თავიდან აცილების საშუალებას. მაგრამ, ზემოთჩამოთვლილი მოწყობილობებისაგან განსხვავებით, მარშრუტიზატორები *ცვლიან გადასაცემ Ethernet კადრებს* - უფრო ზუსტად, "შლიან" მათ ქსელურ დონემდე და შემდეგ გარკვეული წესების დაცვით აწყობენ თავიდან. სიტყვამ მოიტანა და, გარკვეული აწყობის გარეშე მარშრუტიზატორები არ გადასცემენ სხვა პორტებში ფართომაუწყებლობის პაკეტებსაც კი, და, ამგვარად, ქსელებში წარმოადგენენ *შეჯახებების და ფართომაუწყებლობების არეების საზღვრებს.*

OSI მოდელის უფრო მაღალი დონის პროგრამებთან ერთად, მარშრუტიზატორებს შეუძლიათ მთელი რიგი საკმარისად რთული მოქმედებების შესრულება, მაგალითად, აღმოაჩინონ ქსელში პრობლემები და შეატყობინონ მათ შესახებ, აწარმოონ მიღებული და გადაცემული მონაცემების სტატისტიკა, გაფილტრონ პაკეტები, ჩაატარონ მომხმარებლების ავტორიზაცია ინტერნეტში გასვლისას და ა. შ.

მძლავრი მარშრუტიზატორები არიან საკმაოდ რთული და ძვირი პროგრამულ-აპარატურული კომპლექსები, ამიტომ

თანამედროვე ქსელებში მათ ხშირად ცვლიან *მე-3 დონის კომუტატორებით* - მოწყობილობებით, რომლებსაც უჭირავთ საშუალედო საფეხური კომუტატორებსა და მარშრუტიზატორებს შორის. ჩვეულებრივი კომუტატორებისაგან იმით განსხვავდებიან, რომ შეუძლიათ შეასრულონ მარშრუტიზაციის უმარტივესი ფუნქციები, დარჩნენ მაღალმწარმოებლურები და არც ისე ძვირი.

გარდა ამისა, უნდა ვახსენოთ თანამედროვე კომუტატორების ისეთი ფუნქცია, როგორიცაა *ვირტუალური ლოკალური ქსელების (Virtual LAN)* აგების შესაძლებლობა, როდესაც ქსელის ერთ *ლოგიკურ* სეგმენტში ერთიანდებიან *ფიზიკურად* სხვადასხვა კომუტატორებთან მიერთებული კომპიუტერები (ნახ. 6.3). ასეთი გაერთიანების კრიტერიუმები შეიძლება იყოს სხვადასხვა, დაწყებული MAC- ან IP-მისამართებით და დამთავრებული კომპიუტერების სახელებით.



ნახ. 6.3. ვირტუალური ლოკალური ქსელის ფორმირების მაგალითი

რაბები

რაბის ქვეშ ზოგადად იგულისხმება ნებისმიერი მოწყობილობა ან პროგრამა, რომელიც იძლევა *სხვადასხვა სისტემების გაერთიანების* საშუალებას (მაგალითად, არსებობენ საფოსტო რაბები სხვადასხვა სისტემის ელექტრონული ფოსტის დასაკავშირებლად). მაგრამ, თუ ლაპარაკია ქსელებში ურთიერთქმედებაზე, მაშინ აქ რაბის ქვეშ უნდა ვიგულისხმოდ *სხვადასხვა ქსელური არქიტექტურების გამაერთიანებლი მოწყობილობა* (მაგალითად: რაბი Ethernet-დან TokenRing-ში). მნიშვნელოვანია, რომ რაბს უნდა ჰქონდეს არა მხოლოდ სხვადასხვაგვარი სისტემების მისაერთებელი ფიზიკური პორტები, არამედ უნდა "ხვდებოდეს" სხვადასხვაგვარ პროტოკოლებს, გამოდიოდეს რა მათთვის "თარჯიმნის" როლში.

რაბების ტიპიური მაგალითია თანამედროვე საშინაო ქსელებში ფართოდ გამოყენებადი ინტეგრირებული მოწყობილობები, რომლებშიც გაერთიანებულია ინტერნეტთან მისაერთებელი ADSL-მოდემი, IEEE 802.11b (ან g, n) სტანდარტით მომუშავე უკაბელო შეღწევის წერტილი და IEEE 802.3u სტანდარტის მხარდამჭერი Fast Ethernet კომუტატორი.

ჩამოვაყალიბოთ რამდენიმე რეკომენდაცია, რომლითაც შეიძლება ვიხელმძღვანელოთ ტელეკომუნიკაციური მოწყობილობების არჩევისას.

დღეს ქსელებში ყველაზე გავრცელებული ტელეკომუნიკაციური მოწყობილობაა Fast და Gigabit Ethernet კომუტატორიბი, ხოლო უკაბელო მოწყობილობების მიერთება ლოკალურ ქსელებთან ხორციელდება *რაბების* მეშვეობით, რომლებიც თავისთავში აერთიანებენ *კომუტატორისა* და *უკაბელო შეღწევის წერტილის* ფუნქციებს და მუშაობენ 802.11g,n სტანდარტებით.

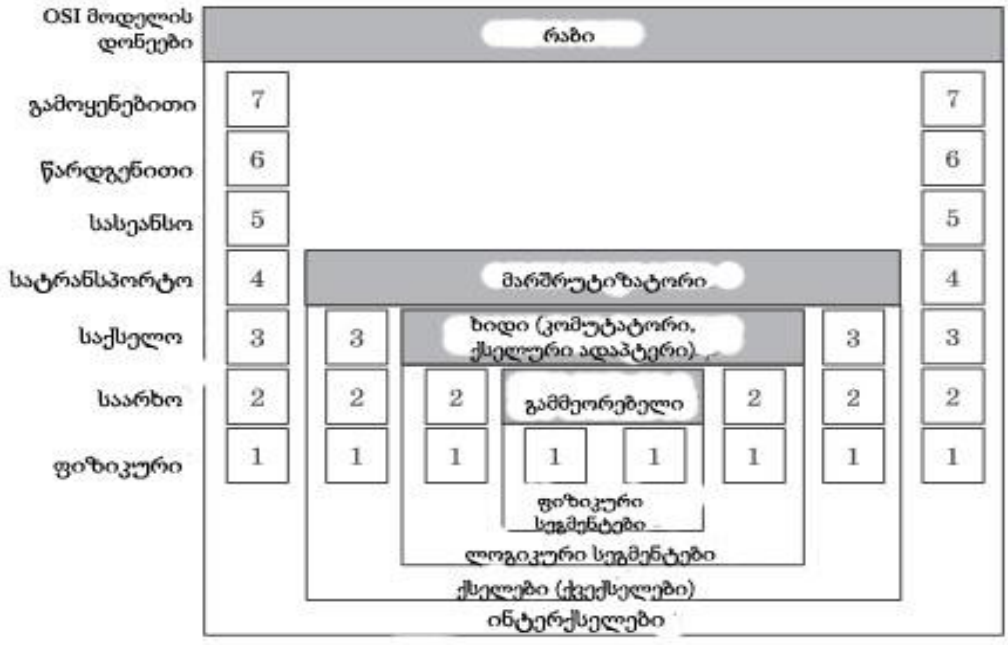
საშინაო და მცირე საოფისე ქსელებისათვის სავსებით გამოდგება არც თუ ძვირი 8- და 16-პორტიანი Fast Ethernet კომუტატორები - სასურველია პორტების მართვის ფუნქციით. თუ მონაცემთა დიდი მოცულობის გადაცემა არ იგეგმება, შეიძლება შევჩერდეთ უკაბელო შეღწევის წერტილებზე, მაგრამ ეს მობილური გადაწყვეტა უფრო ძვირია და ნაკლებად ჩქაროსნული.

მსხვილ ქსელებში საფუძველს წარმოადგენენ მძლავრი და საიმედო Gigabit Ethernet ან 10Gigabit Ethernet კომუტატორები, რომლებსაც უერთდებიან ქვეგანაყოფების (შენობების) კომუტატორები, მათთან კი, თავის მხრივ, - სართულების

(ოფისების) კომუტატორები. მსხვილ ქსელებში შეღწევის წერტილების განლაგება ზედმიწევნით გააზრებულად უნდა დაიგეგმოს, იმისათვის რომ მომხმარებელი საწარმოს ტერიტორიაზე გადაადგილებისას თანმიმდევრობით გადაერთოს ერთი შეღწევის წერტილიდან მეორეზე და ამავე დროს შეინარჩუნოს კავშირი ლოკალურ ქსელთან.

მარშრუტიზატორების გამოყენება მოითხოვება იქ, სადაც რთულ მარშრუტიზებად ქსელში საჭიროა IP-პაკეტების ნაკადების მკაფიო კონტროლი, და აგრეთვე პაკეტების მიწოდების სარეზერვო მარშრუტების უზრუნველსაყოფად, - მაგალითად, დაშორებულ ოფისთან ან ინტერნეტთან ურთიერთქმედებისას.

კომპიუტერისათვის *ქსელური ადაპტერის* შერჩევისას ყურადღება უნდა მივაქციოთ Ethernet ან Wi-Fi სტანდარტების მხარდაჭერის შესაძლებლობას. ყველაზე უკეთესია ავირჩიოთ რამდენადმე ძვირი, მაგრამ თანამედროვე ქსელური ადაპტერი, მაგალითად Gigabit Ethernet ან 802.11g,n სტანდარტების Wi-Fi. რადგან ეს სტანდარტები *უკუთავსებადია* წინამორბედებთან, ასეთი ადაპტერები სავსებით თავისუფლად შეძლებენ მუშაობას ძველ 10Base-T კონცენტრატორებთან და 802.11b შეღწევის წერტილებთან, მანამ სანამ არ შეიცვლება ხსენებული ტელეკომუნიკაციური მოწყობილობები.



ნახ. 6.4. ტელეკომუნიკაციური მოწყობილობების ფუნქციების შესაბამისობა OSI მოდელთან

კითხვები და დავალებები

1. რომელი მოწყობილობა უზრუნველყოფს ინტერფეისს კომპიუტერსა და ქსელურ კაბელს შორის?
2. რა იგულისხმება სახელწოდების ქვეშ ”ტელეკო-მუნიკაციური მოწყობილობა”?
3. რაშია მსგავსება და განსხვავება კონცენტრატორსა და გამმეორებელს შორის?
4. რა არის კასკადირება? რა უპირატესობებს უზრუნ-ველყოფს ის?
5. რა მსგავსება და განსხვავებაა ხიდებსა და კომუტატორებს შორის?
6. რა არის მარშრუტიზატორი? შეუძლია თუ არა მას შეცვალოს კონცენტრატორი, ხიდი ან კომუტატორი?
7. რა დანიშნულება აქვთ რაბებს?
8. რა არის ”უკაბელო შეღწევის წერტილი”? რა დანიშნულება აქვს მას?
9. OSI მოდელის რა დონეზე მუშაობს თქვენს მიერ შესწავლილი ტელეკომუნიკაციური მოწყობილობების ტიპები?
10. დააპროექტეთ (პრიმიტიული სტრუქტურული სქემის სახით) მსხვილი ფირმის ქსელი, რომელიც შედგება სამი ქვეგანაყოფისაგან:
    - ადმინისტრაციის ოფისი (ბათუმის ცენტრში შენობის მთელი სართული, 10 სამუშაო ადგილი; იხ. 3 და 4 თავების კითხვები და დავალებები);
    - საწყობი (ცალკე შენობა ქალაქგარეთ), აღჭურვილი 5 სტაციონარული სადგურით;
    - სავაჭრო ცენტრი (დიდი ფართობის საშენი მასალების ბაზრობა პლუს ავტოსადგომები მყიდველებისათვის), რომლის პერსონალი კლიენტებთან მუშაობისას მოიხმარს ჯპკ-ს, გადაადგილდება რა თავისუფლად სავაჭრო ცენტრისა და ავტოსადგომის ტერიტორიაზე 1.5-2 კმ-ს ფარგლებში.

    ამავდროულად ოფისისა და საწყობის ფარგლებში ქვექსელებს უნდა ჰქონდეთ ვარსკვლავისეული სტრუქტურა, ადმინისტრაციის ოფისისათვის საჭიროა ინტერნეტში გასვლის უზრუნველყოფა ADSL არხით, ხოლო ფირმის ქვედანაყოფებს შორის კავშირი განხორციელდეს ოპტიკურ-ბოჭკოვანი კაბელის დახმარებით. განმსაზღვრელად ჩაითვლება სიჩქარის პარამეტრები და ქსელის მუშაობის საიმედოობა, უგულველყავით მისი ღირებულება.
11. იპოვეთ ინტერნეტში დამატებითი ინფორმაცია კონცენტრატორის, ხიდის, კომუტატორის, რაბის, მარშრუტიზატორის მუშაობის პრინციპების შესახებ.

თავი 7

ვაწყობთ ურთიერთქმედებას კომპიუტერებს შორის: პროტოკოლების სტეკის შერჩევა

ამ თავში თქვენ ნახავთ პასუხებს შემდეგ კოთხვებზე:

- რა არის პროტოკოლთა სტეკი?
- როგორი პროტოკოლთა სტეკები არსებობენ?
- პროტოკოლთა რომელი სტეკია ყველაზე გავრცელებული?
- სხვადასხვა დონეების რომელი პროტოკოლები გამოიყენება TCP/IP-ში?

წინა თავებში ჩვენ გავიგეთ, როგორ ერთიანდებიან კომპიუტერები ქსელში, ავირჩიეთ ქსელური ტოპოლოგია და არქიტექტურა, შევაერთეთ კომპიუტერები კომუტატორების (ან სხვა ტელეკომუნიკაციური მოწყობილობების) დახმარებით. მაგრამ, კომპიუტერებს რომ შეეძლოთ ქსელში მუშაობა, ყოველივე ეს არ არის საკმარისი. ახლა უნდა ვასწავლოთ ქსელურ გამოყენებებს ერთმანეთთან "ლაპარაკი" - გაცვალონ მონაცემები პროტოკოლების დახმარებით უფრო მაღალ დონეებზე, ვიდრე საარხოა. ასეთი დონე რამოდენიმეა, ამიტომ ჩვენ დაგვჭირდება არა ერთი, არამედ რამოდენიმე პროტოკოლი, გაერთიანებული ერთ კრებულად, ანუ, როგორც ამბობენ, *სტეკში*.

ამ თავში ჩვენ შევისწავლით ქსელებში ყველაზე ხშირად გამოყენებად ზოგიერთ *პროტოკოლთა სტეკს*, მათ შორის დღეისათვის ყველაზე გავრცელებულ კრებულს - TCP/IP *სტეკს*.

NetBEUI

მოთხოვნილი პროგრამული უზრუნველყოფის მოცულობით არც ისე დიდი პროტოკოლი, ახორციალებს OSI მოდელის ქსელურ, სატრანსპორტო და სასეანსო დონეების მხარდაჭერას. გამართვაში მეტად მარტივია (პრაქტიკულად არ საჭიროებს), მუშაობს ეფექტურად და სწრაფად ზომებით მცირე და საშუალო ქსელებში (200 კომპიუტერამდე). თანამედროვე საზომით, NetBEUI პროტოკოლის სერიოზული ნაკლია: შეზღუდვები დიდი რაოდენობის კომპიუტერების ქსელებში მუშაობისას და, ყველაზე მთავარი, მარშრუტიზაციის მხარდაჭერის არარსებობა - ქსელური ადრესაციისა და ქსელებს შორის პაკეტების გადაგზავნის ფუნქციები მასში უბრალოდ არა რეალიზებული. შესაბამისად, მისი გამოყენება არ შეიძლება მარშრუტიზატორით გაერთიანებულ დიდ ქსელებში, და ინტერნეტთან მუშაობისას. NetBEUI პროტოკოლის მიწოდება ხორციელდებოდა Windows ყველა ოპერაციული სისტემის შემადგენლობაში უშუალოდ Windows 2000-დე, მაგრამ ბოლო ვერსიებში მისი მხარდაჭერა შეწყვეტილია.

i

აბრევიატურა NetBEUI განიშიფრება როგორც "NetBIOS Extended User Interface" – "NetBIOS პროტოკოლის გაუმჯობესებული ვერსია".

IPX/SPX

NWLink – Microsoft კომპანიის IPX/SPX სტეკის რეალიზება, რომელიც მიეწოდება Windows-ს ყველა ვერსიაში.

IPX/SPX პროტოკოლების სტეკი შემუშავდა ფირმა Novell-ის მიერ 80-იანი წლების დასაწყისში თავისი ქსელური ოპერაციული სისტემის NetWare-სათვის. სტეკის საფუძველი - IPX (Internetwork Packet eXchange) და SPX (Sequenced Packet eXchange) პროტოკოლებია, რომლებიც ახორციელებენ OSI მოდელის *ქსელურ* და *სატრანსპორტო დონეების* ფუნქციებს, შესაბამისად. ისევე როგორც NetBEUI, პროტოკოლი IPS/SPX არის არც ისე დიდი (მისი პროგრამული მხარდაჭერა შეიძლება ადვილად მოვათავსოდ ჩვეულებრივ 1.44 მბ დისკეტაზე DOS-ს ერთად) და სწრაფი, რაც განსაკუთრებით მნიშვნელოვანი იყო მცირე ოპერატიული მეხსიერების მქონე (640 კბაიტი) პირველი თაობის IBM-თავსებადი კომპიუტერების ეპოქაში. გარდა ამისა, IPX/SPX სტეკში მხარდაჭერილია მარშრუტიზაცია. ამ ორივე ფაქტორმა, Novel Netware-ის იმ წლების ოპერაციული სისტემის ბაზაზე სერვერების საიმედოობასთან ერთად, ხელი შეუწყვეს IPX/SPX სტეკის ფართო გავრცელებას 80-იანი და 90-იანი წლების ლოკალურ ქსელებში. პროტოკოლთა ამ სტეკის ნაკლოვან მხარეებს უნდა მივაკუთვნოთ ფართომაუწყებლური შეტყობინებების ინტენსიური გამოყენება, რაც სერიოზულად ტვირთავს ქსელს, განსაკუთრებით ნელი გლობალური არხებით მუშაობისას. ამ გარემოებამ, და აგრეთვე იმან, რომ IPX/SPX სტეკი ეკუთვნის ფირმა Novel-ს და მისი რეალიზაციისათვის ოპერაციული სისტემების სხვა მწარმოებლებს უხდებოდათ ლიცენზიის ყიდვა, საბოლოოდ გამოიწვია IPX/SPX-ის გამოდევნა საყოველთაოდ ხელმისაწვდომი TCP/IP სტეკით. მნიშვნელოვანი იყო 90-იან წლებში სულ უფრო მეტი ორგანიზაციების მიერთება ინტერნეტთან, რომელშიც გამოიყენებოდა TCP/IP სტეკი, ხოლო ქსელში პროტოკოლთა ორი სტეკის მხარდაჭერა - ზედმეტი "თავის ტკივილია" ქსელური ადმინისტრატორებისათვის.

TCP/IP

TCP/IP სტეკის (ისევე როგორც ინტერნეტის) განვითარების ისტორია დაიწყო გასული, XX საუკუნის 60-ანი წლებიდან ARPANet პროექტით - აშშ-ს თავდაცვის სამინისტროს პერსპექტიული საკვლევო პროექტების სააგენტოს ქსელით (Advanced Research Project Agency Network). რადგან სამხედროებისათვის "ცივი ომის" დროს განსაკუთრებით მნიშვნელოვანი იყო მონაცემების გადაცემის შესაძლებლობა ატომური დაბომბვის პირობებშიც კი, ARPANet-ი იყო მაღალი საიმედოობის ქსელი, რომელიც აერთიანებდა სამხედრო, სახელმწიფო და სამეცნიერო დაწესებულებებს. შედეგად, მიღებული ქსელი და მოგვიანებით (70-ნ წლებში) შემუშავებული TCP/IP პროტოკოლთა სტეკი აღმოჩნდა იმდენად კარგი, რომ თავდაცვის სამინისტროს მიერ ARPANet

პროექტის ფინანსირების შეწყვეტის შემდეგაც გააგრძელა არსებობა და წარმატებული განვითარება. შეიქმნა თანამედროვე ინტერნეტის საფუძვლები.

TCP/IP პროტოკოლთა სტეკის ძირითადი უპირატესობები სხვებთან შედარებით (მაგალითად, IPX/SPX სტეკთან) - *ქსელური ადრესაციის* უფრო მოხერხებული სისტემა, *პაკეტების ფრაგმენტაციის* შესაძლებლობა და ძალიან მცირე რაოდენობის ფართომაუწყებლობის შეტყობინებები. ეს უპირატესობები გადამწყვეტია არა მხოლოდ გლობალური ქსელების აგებისას, რომლებიც აერთიანებენ სხვადასხვა არქიტექტურის ქსელებს, არამედ მსხვილი კორპორატიული ქსელების შექმნისას. შედეგად, TCP/IP სტეკმა პრაქტიკულად გამოდევნა ყველა დანარჩენი - გამოიყენება მცირე საშინაო ქსელებშიც და გლობალურ ინტერნეტ ქსელშიც.

!

რადგან TCP/IP სტეკი არის *საყოველთაოდ ხელმისაწვდომი*, მისი სტანდარტები (და აგრეთვე უბრალოდ საინფორმაციო მასალები) ქვეყნდება ინტერნეტში სპეციალური დოკუმენტების სახით "RFC"-ს ("Request for Comments", "კომენტარების მოთხოვნა") სახელწოდებით, თანმიმდევრულად ზრდადი ნომრით. მაგალითისათვის, IP პროტოკოლის სპეციფიკაცია გამოქვეყნდა RFC 791-ში, ხოლო 1.1 ვერსიის HTTP პროტოკოლის - RFC 2616-ში. RFC პირველი დოკუმენტი წარმოდგენილი იყო ჯერ კიდევ 1969 წლის აპრილში, ახლა RFC-ს მიმდინარე ნომრებმა გადალახა 4 ათასი.

TCP/IP სტეკი, განსხვავებით შვიდდონიანი OSI მოდელისაგან, მიღებულია აღიწეროს ოთხი დონის ჩარჩოებში (ნახ. 7.1).

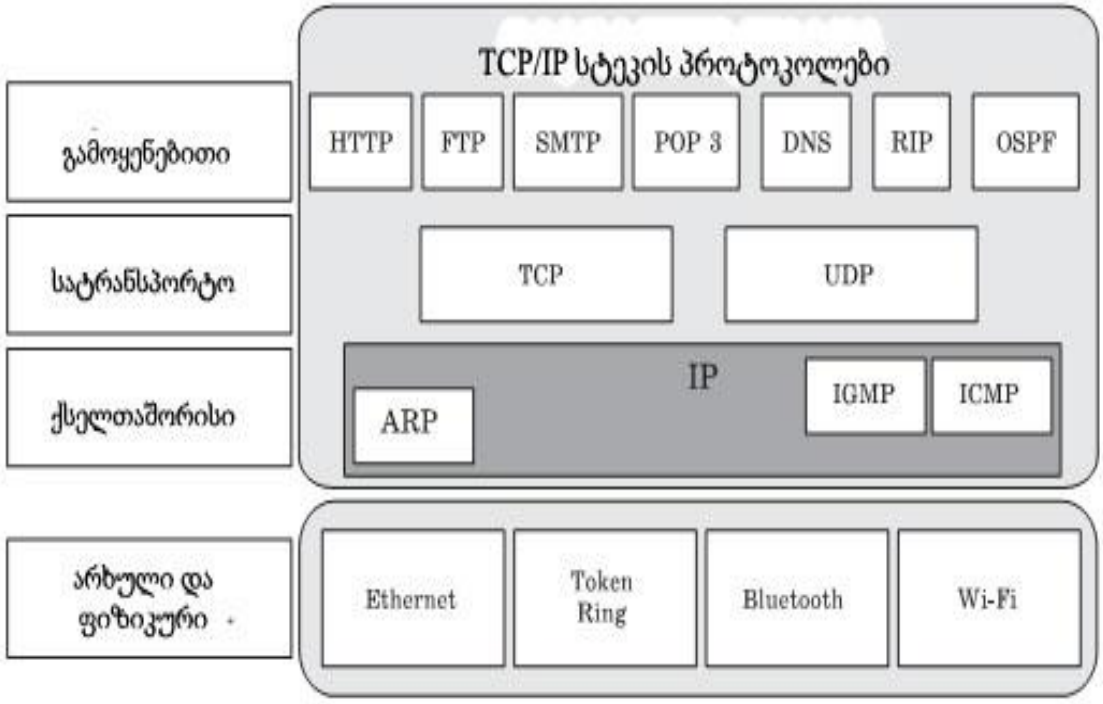
i

ფიზიკურ დონეზე TCP/IP მხარს უჭერს მუშაობას ლოკალური ქსელების ძირითად ტექნოლოგიებთან Ethernet, Token Ring, Wi-Fi, Bluetooth - და ა. შ.

ქსელურ დონეზე თავსდება რამოდენიმე პროტოკოლი:

- *პროტოკოლი ARP* (*Address Resolution Protocol*) არის რგოლი, რომელიც აკავშირებს ქსელურ დონეს ფიზიკურთან. ის პასუხისმგებელია ქსელური IP-მისამართების გარდაქმნაზე აპარატულ MAC-მისამართებად;

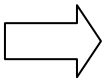
იმის შემოწმება - ბოლო დროს თქვენი ქსელის რომელი კომპიუტერის IP-მისამართი გარდაიქმნა შესაბამის MAC-მისამართებად, შეიძლება ARP-A ბრძანებით.



ნახ. 7.1. **TCP/IP** სტეკის ძირითადი პროტოკოლები

- *პროტოკოლი RARP* (*Reverse Address Resolution Protocol*) - ახორციელებს MAC-მისამართების უკუგარდაქმნას IP-მისამართებად (Windows ოპერაციულ სისტემებში RARP პროტოკოლის მხარდაჭერა არ არის გათვალისწინებული);
- *პროტოკოლი ICMP (Internet Control Message Protocol)* - გამოიყენება შეცდომების შესახებ შეტყობინებების გადასაცემად, ქსელური კვანძისა და პაკეტების მიწოდების მარშრუტის ხელმისაწვდომობის დიაგნოსტირებისათვის (სახელდობრ, მას იყენებენ ისეთი პოპულარული უტილიტები, როგორიცაა PING და TRACERT)

- *პროტოკოლი IGMP (Internet Group Management Protocol)* - გამოიყენება კომპიუტერთა ჯგუფის მართვისათვის, მაგალითად, ქსელში ნაკადური ვიდეო და ხმის გადაცემისას. ამ დროს ქსელზე დატვირთვის შემცირებისათვის პაკეტი ერთდროულად ეგზავნება სპეციალური მისამართით რამდენიმე კომპიუტერს (*მრავალმისამართიანი გაგზავნა*);
- *პროტოკოლი IP* (*Internet Protocol*) - ერთ-ერთი ყველაზე მნიშვნელოვანია TCP/IP სტეკში. სახელწოდებიდან გამომდინარე (”IP” ითარგმნება - ”ქსელთაშორისი პროტოკოლი”), ის პასუხისმგებელია *IP-დეიტაგრამების* (ასე ეწოდება პაკეტებს IP პროტოკოლის დონეზე) მიწოდებაზე, უზრუნველყოფს რა პაკეტის გადაცემას ერთი ქსელიდან მეორეში. თუ როგორ ხდება ეს, დაწვრილებით იქნება მოგითხრობთ ქვემოთ.



სატრანსპორტო დონეზე მუშაობს ორი პროტოკოლი:

- *პროტოკოლი TCP* (*Transmission Control Protocol, გადაცემის მართვის პროტოკოლი*) - სატრანსპორტო დონის ძირითადი პროტოკოლია. უზრუნველყოფს *შეერთების დამყარებას* გამგზავნსა და მიმღებს შორის, *ინფორმაციის* დიდი ბლოკის *დანაწევრებას* (მაგალითად, ფაილის) *მცირე ზომის TCP-პაკეტებად* და მათ *გარანტირებულ მიწოდებას* მიმღებისათვის (საჭირო წესრიგითა და უშეცდომოდ). შესაბამისად, TCP პროტოკოლი გამოიყენება იმ გამოყენებებში, სადაც მნიშვნელოვანია მთლიანობის უზრუნველყოფა მონაცემების გადაცემისას;
- *პროტოკოლი UDP* (*User Datagram Protocol*), TCP-გან განსხვავებით, არ ამყარებს შეერთებას ინფორმაციის გადაცემის წინ და არ უზრუნველყოფს მონაცემების საიმედო მიწოდებას, თუმცა მუშაობს უფრო სწრაფად ვიდრე TCP. მას იყენებენ იქ, სადაც გადაცემის სიჩქარესთან შედარებით ინფორმაციის მიწოდების უზრუნველყოფა არც ისე მნიშვნელოვანია (კონტროლი მონაცემთა დაცულობაზე ამ დროს გადატანილია გამოყენებაზე, რომელიც იყენებს UDP პროტოკოლს).

იმისათვის, რომ უკეთესად წარმოვიდგინოთ TCP და UDP პროტოკოლების მუშაობა, დავუბრუნდეთ ჩვენს ანალოგიას ფოსტასთან. ვთქვათ, თქვენ უნდა გადააგზავნოთ გამომცემლობაში მთლიანი რომანი, მაგრამ წერილში ნებადართულია ტექსტის მხოლოდ რამდენიმე ფურცელის ჩადება. იმისათვის, რომ გადაგზავნისას არაფერი დავკარგოთ და ხელნაწერის დასაბეჭდად მიღებისას არაფერი აირიოს, კარგი იქნებოდა მოლაპარაკება გამომცემლობასთან აღნიშვნების სისტემაზე თქვენი რომანისათვის (სხვა ავტორებიც ხომ არსებობს!) და შეტყობინებების ნუმერაციის შესახებ. ამისათვის უნდა გაუგზავნოთ წერილი გამომცემლობას, რომ თქვენ აპირებთ რომანის გაგზავნას და იქვე მიუთითოთ თქვენი შემდეგი შეტყობინების ამოსავალი ნომერიც. გამომცემლობა დაადასტურებს თქვენი შეტყობინების მიღებას და საპასუხო წერილში გაცნობებთ თავის ამოსავალ და შემომავალ ნომრებს, თქვენ დაუდასტურებთ ამ ნომრების მიღებას. ამგვარად, ორივე მხარე შეათანხმებენ შეტყობინებების ნომრებს, რომლებსაც მოგვიანებით ელოდებიან ერთმანეთისაგან. ეს კავშირის დამყარებას ნიშნავს. ახლა ისღა დაგრჩენიათ, დაყოთ რომანი მცირე ნაწილებად და გაუგზავნოთ თითოეული ნაწილი ცალკე წერილით, ხოლო გამომცემლობას - მიღებული ნაწილების დადასტურება. ფოსტის მუშაობის შეცდომები (თუ რომელიმე შეტყობინება ვერ მიაღწევს რედაქციამდე წერილის დაკარგვის, დაზიანების, ან რიგგარეშე მისვლის შემთხვევაში) ადვილად შეიძლება დაადგინოთ შემომავალი და გამავალი ნომრებით, რომ მიიღოთ შესაბამისი ზომები - ხელახლა გადაუგზავნოთ დაკარგული ნაწილი ან შეკრიბოთ რომანის გვერდები საჭირო თანმიმდევრობით.

დაახლოებით ასევე მუშაობს TCP:

- ამყარებს კავშირს კომპიუტერებს შორის გარკვეული პორტებით;
- კომპიუტერ-გამგზავნზე ანაწევრებს ინფორმაციას პაკეტებად, ნომრავს მათ და IP პროტოკოლის დახმარებით გადასცემს მიმღებს;
- კომპიუტერ-მიმღებზე ამოწმებს, მიღებულია თუ არა ყველა პაკეტი, და თუ პაკეტი გამოტოვებულია ან დაზიანებული, მოითხოვს გამომგზავნისგან ხელახალ გადაგზავნას;
- ყველა პაკეტის მიღების შემდეგ ხურავს შეერთებას, კრებს პაკეტებს საჭირო წესითა და რიგით და გადასცემს მიღებულ მონაცემებს უფრო მაღალი დონის გამოყენებას.

UDP პროტოკოლი ამ ანალოგიაში შეიძლება შევადაროთ სარეკლამო შეტყობინებების გაგზავნა-განაწილებას. არავითარი

კავშირის დამყარების და კორესპონდენციის მიღების დადასტურება აქ არ არის - წერილებს სარეკლამო ინფორმაციით უბრალოდ აგდებენ თქვენს საფოსტო ყუთში. ამასთანავე, არც გამგზავნს, არც მიმღებს ინფორმაციის მიწოდების საიმედოობა ან მისი დაუზიანებლობა, სხვათაშორის რომ ვთქვაქთ, მაინცადამაინც არ აწუხებს.

ცხადია, საფოსტო გზავნილები ამ ორივე მაგალითში არის IP პაკეტების ანალოგიები, ხოლო ფოსტალიონები ასრულებენ IP პროტოკოლის ფუნქციებს.

პორტი TCP-ში ან UDP-ში - არის ლოგიკური არხი გარკვეული ნომრით (0-ნ 2^{16}=65536-დე), რომელიც უზრუნველყოფს მიმდინარე ურთიერთქმედებას გამგზავნსა და მიმღებს შორის. ერთი IP-მისამართის მქონე კომპიუტერს პორტები აძლევენ საშუალებას პარალელურად აწარმოოს მონაცემების გაცვლა მრავალ, სხვა კომპიუტერთან. პორტების ზოგიერთი ნომრები (ეგრეთწოდებული "კარგად ცნობილი", ანუ "well-known", პორტები ნომრებით 0-ნ 2^{10}=1024-დე) მიბმულნი არიან გარკვეულ სამსახურებზე და გამოყენებებზე, რაც კლიენტებს საშუალებას აძლევს ადვილად მიმართონ მათთვის საჭირო ქსელურ სერვისებს.

ბოლოს, პროტოკოლების კრებულის მიხედვით ყველაზე მდიდარია TCP/IP სტეკის *გამოყენებითი დონე* . ქვევით, ტაბ. 7.1-ში მოყვანილია ყველაზე პოპულარული პროტოკოლები და აგრეთვე მათთვის რეზერვირებული პორტები. აღვნიშნოთ, რომ, მართალია ჩვეულებრივად რეზერვირდება პორტების ერთნაირი ნომრები TCP-თვისაც და UDP-თვისაც, ტაბულაში მოყვანილია სატრანსპორტო დონის ყველაზე ხშირად გამოყენებადი პროტოკოლის (TCP ან UDP) პორტები.

იმისათვის რომ ვნახოთ, რომელი პორტები გამოიყენება თქვენს კომპიუტერზე ან ელოდებიან მიერთებას, საკმარისია შევასრულოთ ბრძანება NETSTAT-AN.

მიუხედავად პროტოკოლების კრებულების დიდი რაოდენობისა, დღეს ძირითადად გვევლინება საყოველთაოდ ხელმისაწვდომი TCP/IP სტეკი. ის გამოიყენება პრაქტიკულად ყველგან, დაწყებული პატარა საშინაო ქსელებიდან, დამთავრებული უმსხვილესი ქსელით - ინტერნეტით.

ფიზიკურ დონეზე TCP/IP სტეკი მხარს უჭერს ყველა ძირითად ლოკალურ და გლობალურ ქსელურ ტექნოლოგიებთან მუშაობას, ქსელურზე - უზრუნველყოფს ადრესაციის და ეფექტური ქსელთაშორისი მარშრუტიზაციის ლოგიკურ სქემას, სატრანსპორტო დონეზე - პროტოკოლებს როგორც გარანტირებული, ასევე მონაცემების სწრაფი

მიწოდებით, გამოყენებების დონეზე - სხვადასხვა პროტოკოლების მთელს გამას.

ამიტომ, გთავაზობთ გამოიყენოთ ქსელში სწორედ TCP/IP სტეკი.

ტაბულა 7.1

TCP/IP სტეკის გამოყენებითი დონის პროტოკოლები

პროტოკოლი	დანიშნულება	პორტის ნომერი
NTP (Network Time Protocol)	ქსელური დროის პროტოკოლი, გამოიყენება ქსელებში კომპიუტერების სისტემური საათების სინქრონიზაციისათვის	123 (UDP)
DNS (Domain Name System, ან Service)	დომენური სახელების სამსახური, გამოიყენება კომპიტერების ადამიანებისთვის გასაგები სახელების IP-მისამართებად გარდასაქმნელად (მაგალითად, www.microsoft.com ტიპის სახელების)	53 (TCP და UDP)
NetBIOS name service და WINS (Windows Internet Naming Service)	NetBIOS სახელების სამსახური და Windows ქსელთაშორისი სახელების სამსახური, გამოიყენება კომპიუტერების NetBIOS-სახელების IP-მისამართებად გარდასაქმნელად (მაგალითად, SERVER ტიპის სახელების)	137 და 138 (UDP)
NetBIOS session service	NetBIOS სეანსების სამსახური, გამოიყენება კომპიუტერებს შორის სეანსების დამყარებისათვის	139 (TCP)
LDAP (Lightweight Directory Access Protocol)	კატალოგისადმი შეღწევის მარტივი პროტოკოლი, გამოიყენება სხვადასხვა ქსელურ კატალოგებთან მუშაობისათვის (მაგალითად Active Directory სამსახურთან დომენებში Windows Server 2003-ის საფუძველზე)	389 (TCP)
RPC (Remote Procedure Call)	დაშორებული პროცედურის გამოძახება, გამოიყენება Microsoft-ქსელებში მრავალ ქსელურ სამსახურებთან სამუშაოდ	135 (TCP)
Telnet	პროტოკოლი დაშორებულ კომპიუტერებთან ტერმინალური შეღწევისათვის	23 (TCP)
FTP (File Transfer Protocol)	ფაილების გადაცემის პროტოკოლი, ინტერნეტის ერთერთი ”უძველესი” პროტოკოლი; გამოიყენება ფაილების ეფექტური და საიმედო გადაცემისათვის კლიენტსა და FTP სერვერს შორის	20 და 21 (TCP)
TFTP (Trivial File Transfer Protocol)	FTP პროტოკოლის გამარტივებული ვარიანტი, არ აქვს ისეთი ფუნქციები, როგორიცაა მომხმარებლის შემოწმება შემოსასვლელზე, სერვერის კატალოგებისა და ფაილების დათვალიერება; გამოიყენება მხოლოდ ფაილების ჩაწერისა და წაკითხვისათვის	69 (UDP)

პროტოკოლი	დანიშნულება	პორტის ნომერი
Gopher	პროტოკოლი Gopher (”ზაზუნა”), გამოიყენება დაშორებულ სერვერზე ტექსტური საინფორმაცო რესურსებში შეღწევისათვის	70 (TCP)
HTTP (HyperText Transfer Protocol)	ჰიპერტექსტის გადაცემის პროტოკოლი, დღეს ყველაზე პოპულარულია და გამოიყენება მსოფლიო აბლაბუდაში (World Wide Web); აღწერს, როგორი ხერხით უნდა წარვადგინოთ მონაცემები (ტექსტური, აუდიო-, ვიდეო- და ა. შ.) ვებ-სერვერებზე, როგორ მივმართოთ მათ ვებ-ბრაუზერის დახმარებით (მაგალითად, Internet Explorer პროგრამები) და როგორ გადავცეთ ეს მონაცემები	80 (TCP)
NNTP (Network News Transfer Protocol)	ქსელური სიახლეების გადაცემის პროტოკოლი, გამოიყენება შეტყობინებების გაცვლისათვის ტელეკონფერენციების სისტემებში	119 (TCP)
SMTP (Simple Mail Transfer Protocol)	ფოსტის გადაცემის მარტივი პროტოკოლი, გამოიყენება საფოსტო სერვერის მიერ ელექტრონული შეტყობინებების გაცვლისათვის (ავტორის მიერ საფოსტო შეტყობინების გაგზავნის ეტაპზე)	25 (TCP)
POP3 (Post Office Protocol)	”საფოსტო განყოფილების პროტოკოლი”, საკმაოდ მარტივია, გამოიყენება საფოსტო კლიენტის მიერ (მაგალითად Outlook Express პროგრამის მიერ) სერვერზე თავის საფოსტო ყუთთან მისაერთებლად და შეტყობინიბების ამოსაკითხავად (საფოსტო შეტყობინების ადრესატისადმი მიწოდების ეტაპზე)	110 (TCP)
IMAP4 (Internet Message Access Protocol)	ელექტრონული შეტყობინებებისადმი შეღწევის პროტოკოლი - უფრო ფუნქციონალური, ვიდრე POP3, კლიენტური პროტოკოლი საფოსტო სერვერთან შეღწევისათვის	143 (TCP)
SSL (Secure Sockets Layer)	პროტოკოლი, რომელიც უზრუნველყოფს ალგორითმების ურთიერთშეთანხმებასა და დაშიფრვის გასაღებების გაცვლას. გამოიყენება ქსელებით გადაგზავნისას მონაცემების დაცვისათვის	25 (SMTP) 995 (POP3S) 993 (IMAPS) 443 (HTTPS) (TCP)

?

კითხვები გამეორებისთვის

1. რა არის პროტოკოლების კრებული (სტეკი)? რაში მდგომარეობს ”სტეკ”-ის აზრი?
2. პროტოკოლების როგორი კრებულები იცით? რით განსხვავდებიან ისინი?
3. პროტოკოლების რომელი სტეკია დღეს ყველაზე მეტად პოპულარული? რატომ?
4. OSI მოდელის რომელი დონეებია მხარდაჭერილი TCP/IP პროტოკოლთა სტეკში?
5. რაშია მსგავსება და განსხვავება TCP და UDP პროტოკოლებს შორის? ამ პროტოკოლებიდან რომელი და როდის არის რეკომენდებული გამოყენებისათვის?
6. ჩამოთვალეთ TCP/IP სტეკის თქვენთვის ცნობილი პროტოკოლები. რისთვის არის განკუთვნილი თითოეული მათგანი?
7. რა არის ”პორტი” TCP/IP-ში? რისთვის არის საჭირო პორტები?
8. TCP/IP სტეკის სატრანსპორტო პროტოკოლებიდან თქვენ რომელს გამოიყენებდით:
   - ინტერნეტის ქსელით საარქივო ფაილების გადაგზავნისათვის?
   - IP-ტელეფონიის რეალიზებისათვის (ხმოვანი შეტყობინებების რეალურ დროში) ორ მობილურ ჯპკ-ს მომხმარებლებს შორის უკაბელო Wi-Fi არხით?
9. გაარკვიეთ, რომელი პროტოკოლებია დაყენებული თქვენ პკ-ზე.

თავი 8

ვაწყობთ ურთიერთქმედებას კომპიუტერებს შორის: IP-ადრესაციისა და მარშრუტიზაციის აწყობა

ამ თავში
თქვენ ნახავთ პასუხებს შემდეგ კითხვებზე:

- **რა არის IP-მისამართი, ქვექსელის ნიღაბი (mask), ძირითადი რაბი?**
- **როგორ მუშაობს IP-მარშრუტიზაცია? როგორ "წავიკითხოთ" მარშრუტიზაციის ტაბულა?**
- **როგორ ცვლიან ერთმანეთში მარშრუტიზაციის ტაბულებს მარშრუტიზატორები?**
- **როგორ დაუნიშნოთ IP-მისამართები ქსელის კომპიუტერებს?**
- **როგორ შევამოწმოთ IP პროტოკოლის ქმედითუნარიანობა?**

ამგვარად, ჩვენ ავირჩიეთ TCP/IP პროტოკოლების კრებული და დავაყენეთ ის (დავაინსტალირეთ შესაბამისი პროგრამული უზრუნველყოფა). აღვნიშნოთ, რომ თანამედროვე ოპერაციულ სისტემებში ამ პროტოკოლის არსებობა იგულისხმება; მეტიც, მისი წაშლა, მაგალითად Windows XP ან Windows Server 2003-დან ჩვეულებრივი ხერხით შეუძლებელია (ღილაკი **Delete** ქსელური მიერთებების თვისებებში არ არის გააქტიურებული).

სამწუხაროდ, TCP/IP პროტოკოლის მხოლოდ დაყენება არაა საკმარისი. სტეკი არ ამუშავდება მანამ, სანამ თქვენს ქსელში არ იქნება სწორად აწყობილი *IP-ადრესაცია და მარშრუტიზაცია.* (ქსელის მუშაობა ისევ შევადაროთ ფოსტის მუშაობას: როგორ მიუტანს წერილს ფოსტალიონი ადრესატს თუ გზები და ტრანსპორტი, მართალია მუშაობენ, მაგრამ სახლები არ არის დანომრილი, ხოლო საფოსტო განყოფილებებმა არ იციან როგორ გადააგზავნონ წერილი ერთი ქალაქიდან მეორეში?).

ამიტომ უნდა გავიგოთ, თუ რა არის *IP-მისამართი და ქვექსელის ნიღაბი (mask),* გავარკვიოთ, როგორ გამოიყენება ეს ორივე პარამეტრი *ლოკალური* და *დაშორებული IP- ქსელების* დასადგენად და კონკრეტული მაგალითებით გავეცნოთ, როგორ *მიაქვთ IP-პაკეტები* კომპიუტერებს და მარშრუტიზატორებს ერთი ქსელიდან მეორეში.

IP-ადრესაციის საფუძვლები

ნებისმიერი კომპიუტერის TCP/IP პროტოკოლის თვისებებში მისი IP-მისამართი არის უპირველესი და აუცილებელი პარამეტრი.

IP-მისამართი - არის უნიკალური 32-თანრიგიანი ორეული ციფრების თანმიმდევრობა, რომლის დახმარებითაც კომპიუტერი ერთმნიშვნელოვნად იდენტიფიცირდება IP-ქსელში. (შეგახსენებთ, რომ საარხო დონეზე კომპიუტერების ასეთივე უნიკალური მისამართების როლში გამოდიან ქსელური ადაპტერების MAC-მისამართები, რომელთა დამთხვევის შეუძლებლობა კონტროლირდება დამამზადებლის მიერ წარმოების სტადიაზე.)

ამ თავში განხილული იქნება IP პროტოკოლის ყველაზე გავრცელებული ვერსია 4, ანუ IP v4. მაგრამ უკვე შექმნილია შემდეგი - *IP ვერსია 6 (IP v6)*, რომელშიც IP-მისამართი წარმოდგენილია 128-ბიტიანი ორეული ციფრების თანმიმდევრობით. IP პროტოკოლის ამ ვერსიამ ჯერ ვერ ჰპოვა ფართო გავრცელება, მიუხედავად იმისა, რომ მხარდაჭერილია თანამედროვე მარშრუტიზატორებისა და ოპერაციული ბის მიერ (მაგალითად,Windows XP ან Windows Server 2003).

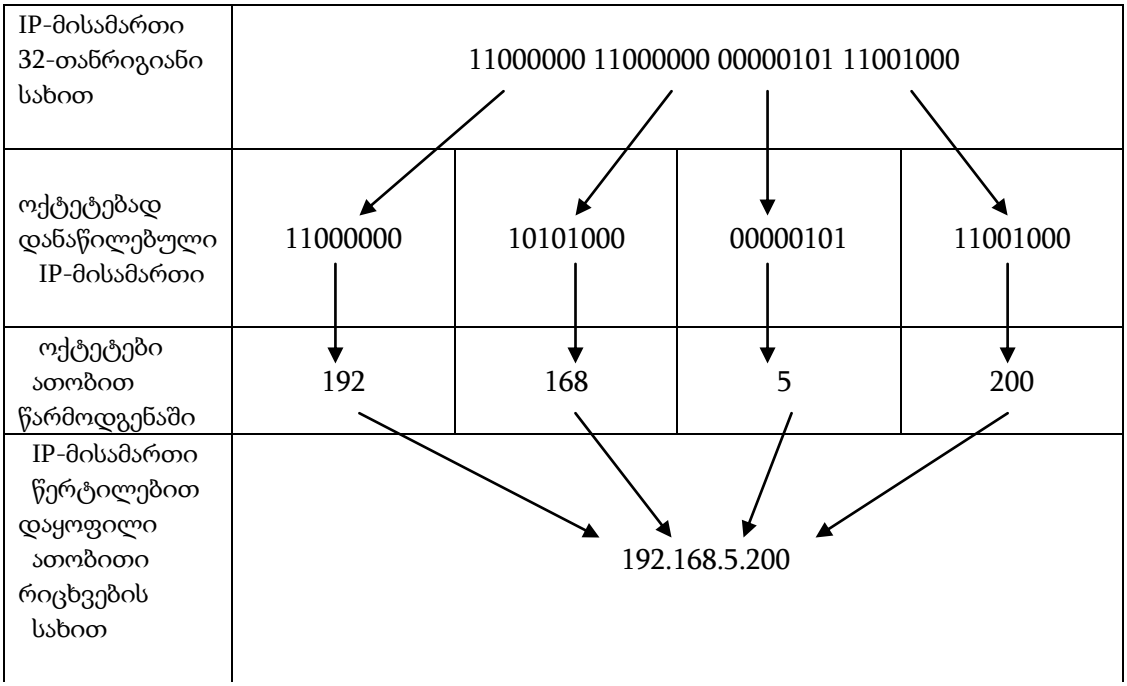
IP-მისამართებთან მუშაობის მოხერხებულობისათვის 32-თანრიგიან თანმიმდევრობას ყოფენ 4 ნაწილად, 8 ბიტით თითოში (*ოქტეტებად*), თითოეული ოქტეტი გადაჰყავთ ათობით რიცხვებში და ჩაწერისას ამ რიცხვებს განაცალკევებენ წერტილებით. ასეთი სახით (ამ წარმოდგენას ეწოდება "წერტილებიანი ათეული რიცხვები ", ან, ინგლისურად, "*dotted-decimal notation*") IP-მისამართები იკავებენ გაცილებით ნაკლებ ადგილს და გაცილებით ადვილად დასამახსოვრებელია (ტაბ. 8.1).

IP v6

ტექნიკური მიმართულებით აქტიურად განვითარებადი ქვეყნები (ჩინეთი, იაპონია, კორეა და სხვა) იწყებენ მწვავე დეფიციტის განცდას IP-მისამართების გამო, რომლებიც ახდენენ არა მხოლოდ კომპიუტერების, არამედ სხვა, ინტერნეტში შეღწევის ფუნქციების მქონე მოწყობილობების იდენტიფიცირებას. ამჟამად მიღებული 32-ბიტიანი სტანდარტი უზრუნველყოფს IP-მისამართების რაოდენობას, რომელიც თითქმის 4.3 მილიარდს უდრის, მაგრამ მათი უმრავლესობა მიმაგრებულია აშშ-ზე (დაახლოებით 70%), კანადაზე და ევროპულ ქვეყნებზე, მაგრამ, მაგალითად, ჩინ. სახ. რესპ.-მ მიიღო მხოლოდ 22 მილიონი. ახალი 128-თანრიგიანი IP პროტოკოლის IP v6 ვერსია საშუალებას მოგვცემს IP-მისამართების რაოდენობა გაიზარდოს უზარმაზარ სიდიდემდე - $3.4x10^{36}$.

ტაბულა 8.1

IP-მისამართის სხვადასხვა წარმოდგენები



ასეთი გარდაქმნის სწრაფად და ზეპირად განვახორციელებისათვის (რაც ქსელურ ადმინისტრატორებს ესაჭიროებათ არც თუ იშვიათად, ხოლო კალკულატორი ყოველთვის ხელთ არააქვთ), სასარგებლოა შემდეგი ტაბულის დამახსოვრება. მასში მოყვანილია რიცხვი 2-ის ხარისხის ათობითი მნიშვნელობები, რომლის მაჩვენებელი უდრის ბიტის რიგით ნომერს ოქტეტში (შეგახსენებთ - ბიტების ნუმერაცია წარმოებს მარჯვნიდან მარცხნივ, დაწყებული ნულიდან):

ბიტის რიგითი ნომერი ოქტეტში	7	6	5	4	3	2	1	0
2 ხარისხში - შესაბამისად ბიტის ნომრისა	128	64	32	16	8	4	2	1

თუ ასეთ ტაბულას დავიმახსოვრებთ, არ იქნება რთული ზეპირად ოქტეტების გადაყვანა ათობით რიცხვებში და პირიქით.

ათობითი რიცხვი *ოქტეტში არანულოვანი ბიტების შესაბამისი რიცხვთა ჯამის ტოლია*, მაგალითად:

$$10101101 \rightarrow 128\cdot 1+64\cdot 0+32\cdot 1+16\cdot 0+8\cdot 1+$$

$$+4\cdot 1+2\cdot 0+1\cdot 1=173$$

შედარებით რთულია ათობითი წარმოდგენის გადაყვანა ორობითში, მაგრამ გავარჯიშებით არც ეს იქნება პრობლემა. მაგალითად

$$201=128\cdot 1+64\cdot 1+32\cdot 0+16\cdot 0+8\cdot 1+$$

$$+4\cdot 0+2\cdot 0+1\cdot 1\rightarrow 11001001$$

კომპიუტერისათვის TCP/IP ქსელში სამუშაოდ მხოლოდ IP-მისამართი არ არის საკმარისი. სხვა აუცილებელი პარამეტრი, რომლის გარეშეც TCP/IP პროტოკოლი არ იმუშავებს, არის *ქვექსელის ნიღაბი (mask).*

ქვექსელის ნიღაბი - 32-თანრიგიანი რიცხვი, რომელიც შედგება თავდაპირველი ერთიანებისაგან და მერე - ნულებისაგან, მაგალითად (ათობით წარმოდგენაში) 255.255.255.0 ან 255.255.240.0.

ქვექსელის ნიღაბი თამაშობს განსაკუთრებულად მნიშვნელოვან როლს IP-ადრესაციასა და მარშრუტიზაციაში. რომ გავიგოთ ამ პარამეტრის მნიშვნელობა, გავიხსენოთ ქსელი ARPANet-ის აგება როგორც ერთმანეთთან შეერთებული ჰეტეროგენული ქსელების კრებული. ასეთ რთულ ქსელში სწორი ურთიერთქმედებისათვის ყველა მონაწილეს უნდა შეეძლოს დადგენა, რომელი IP-მისამართები ეკუთვნის მის *ლოკალურ* ქსელს და რომელი - *დაშორებულ* ქსელებს.

სწორედ ქვექსელის ნიღაბის გამოიყენებით, ხდება *ნებისმიერი IP-მისამართის გაყოფა* ორ ნაწილად: *ქსელის იდენტიფიკატორად (Net ID)* და *კვანძის იდენტიფიკატორად (Host ID).* ასეთი გაყოფა ძალიან მარტივია: იქ სადაც ნიღაბში არის ერთიანები, იმყოფება ქსელის იდენტიფიკატორი, ხოლო სადაც ნულებია - კვანძის იდენტიფიკატორი.

პროტოკოლი IP v6 – Windows XP-ში

IP v6 პროტოკოლის გამოყენებისათვის Windows XP-ში არის საჭირო პროგრამული უზრუნველყოფა, რომელიც, დუმილით არ არის გააქტიურებული. ახალი პროტოკოლის საბრძანებო სტრიქონში (მენიუში) გასაშვებად საკმარისია შევიყვანოთ და გავუშვათ შესრულებაზე ბრძანება Ip v6 install. IP v6 პროტოკოლთან მუშაობის შესახებ საჭირო ცნობების მიღება (მისი ინსტალირების შემდეგ) შეიძლება ბრძანებით IP v6/?.

მაგალითად, 192.168.100.55 IP-მისამართში 255.255.255.0 ქვექსელის ნიღაბის გამოყენებისას, ქსელის იდენტიფიკატორი იქნება რიცხვი 192168.100.0, ხოლო რიცხვი 55 - კვანძის იდენტიფიკატორი. საკმარისია შევცვალოთ ქვექსელის ნიღაბი, ვთქვათ, რიცხვზე 255.255.0.0, რომ კვანძის იდენტიფიკატორი და ქსელის იდენტიფიკატორი შეიცვლებიან 192.168.0.0-ითა და 100. 55-ით, შესაბამისად, ამიტომ, როგორც შემდგომ ვნახავთ, სხვანაირად მოიქცევა კომპიუტერი IP-პაკეტების გაგზავნისას.

ქსელებისა და კვანძების IP-მისამართების დანიშვნის წესები

ახლა, როცა ჩვენ ვიცით, რა არის IP-მისამართი, ქვექსელის ნიღაბი, ქსელისა და კვანძის იდენტიფიკატორები, სასარგებლოა დავიმახსოვროთ **წესები, რომლებიც უნდა გამოვიყენოთ ამ პარამეტრების დანიშნვისას:**

1. ქსელის იდენტიფიკატორი არ შეიძლება შეიცავდეს მხოლოდ ორობითი ნულებს ან ერთიანებს. მაგალითად, მისამართი 0.0.0.0 არ შეიძლება იყოს ქსელის იდენტიფიკატორი;
2. კვანძის იდენტიფიკატორი ასევე არ შეიძლება შეიცავდეს მხოლოდ ორობით ნულებს ან მხოლოდ ერთიანებს - ასეთი მისამართები რეზერვირებულია სპეციალური მიზნებისათვის:

    - კვანძის იდენტიფიკატორში ყველა ნული ნიშნავს, რომ ეს მისამართი არის *ქსელის მისამართი*. მაგალითად, 192.168.100.0 არის ქსელის სწორი მისამართი 255.255.255.0 ნიღაბის გამოყენებისას და არ შეიძლება გამოვიყენოთ კომპიუტერების ადრესაციის დროს,
    - კვანძის იდენტიფიკატორში ყველა ერთიანი ნიშნავს, რომ ეს მისამართი არის მოცემული ქსელის *ფართომაუწყებლობის მისამართი*. მაგალითად, 192.168.100.255 არის ფართომაუწყებლობის მისამართი 192.168.100.0 ქსელში 255.255.255.0 ნიღაბის გამოყენებისას და მისი გამოყენება არ შეიძლება კომპიუტერების ადრესაციისათვის;

ტაბულა 8.2

მისამართების კლასები IP-ადრესაციის თავდაპირველ სქემაში

კლასი	პირველი ბიტები ოქტეტში	პირველი ოქტეტის შესაძლო მნიშვნელობები	ქსელების შესაძლო რაოდენობა	ქსელში კვანძების შესაძლო რაოდენობა
A	0	1-126	126	16777214
B	10	128-191	16384	65534
C	110	192-223	2097152	254
D	1110	224-239	გამოიყენება მრავალმისამართიანი გაგზავნისათვის (multicast)	
E	1111	240-254	რეზერვირებულია როგორც ექსპერიმენტალური	

3. კვანძის იდენტიფიკატორი ერთი და იგივე ქსელის ფარგლებში უნდა იყოს უნიკალური;
4. მისამართების დიაპაზონი 127.0.0.1-ნ 127.255.255.254-დე არ შეიძლება გამოვიყენოთ კომპიუტერების IP-მისამართებად. მთელი 127.0.0.1 ქსელი 255.0.0.0 ნიღაბზე რეზერვირებულია ე. წ. ”დახშობის მისამართის” (loopback) ქვეშ, და IP-ში გამოიყენება იმისათვის, რომ კომპიუტერმა მიმართოს საკუთარ თავს.

ამის შემოწმება ადვილია: საკმარისია ნებისმიერ კომპიუტერზე, რომელზედაც დაყენებულია TCP/IP პროტოკოლი შევასრულოთ ბრძანება

PING 127.12.34.56

და, თუ TCP/IP პროტოკოლი მუშაობს, თქვენ ნახავთ, როგორ უპასუხებს თქვენი კომპიუტერი საკუთარ მოთხოვნებს.

კლასობრივი და უკლასო IP-ადრესაცია

მსოფლიოში IP-მისამართების განაწილებით დაკავებულია კერძო არაკომერციული კორპორაცია ICANN (Internet Corporation for Assigned Names and Numbers), უფრო ზუსტად, მისი პატრონაჟის ქვეშ მომუშავე ორგანიზაცია IANA (Internet Assigned Numbers Authority).

თავდაპირველი IP-ადრესაცია ინტერნეტში გამოიყურებოდა შემდეგნაირად. IP-მისამართების მთელი სივრცე (ეს კი ოთხ მილიარდზე მეტია, უფრო ზუსტად - 4 294 967 296 მისამართი) დაყოფილი იყო ხუთ კლასად, IP-მისამართის მიკუთვნება გარკვეულ კლასისზე ამასთან დგინდებოდა პირველი ოქტეტის რამოდენიმე ბიტით (ტაბ. 8.2). აღვნიშნოთ, რომ ქსელებისა და კვანძების ადრესაციისათვის იყენებდენ მხოლოდ **A, B** და **C** კლასებს. გარდა ამისა, ამ ქსელებისათვის დუმილით იყო განკუთვნილი ქვექსელების ფიქსირებული ნიღბები, რომლებიც, შესაბამისად, 255.0.0.0, 255.255.0.0 და 255.255.255. 0 ტოლი არიან, ისინი არა მარტო მკაცრად განსაზღვრავენ კვანძების IP-მისამართებს ასეთ ქსელებში, არამედ მათი მარშრუტიზაციის მექანიზმსაც.

კვანძების მაქსიმალური რაოდენობს გამოანგარიშებისათვის ნებისმიერ IP-ქსელში, საკმარისია ვიცოდეთ რამდენი ბიტია კვანძის იდენტიფიკატორში, ან, სხვანაირად, რამდენი ნულია ქვექსელის ნიღაბში. ეს რიცხვი გამოიყენება ორიანის ხარისხის მაჩვენებლად, შემდეგ, შედეგს გამოვაკლებთ ორ რეზერვირებულ მისამართს (ქსელისა და ფართომაუწყებლობის). ანალოგიური ხერხით ადვილად შეიძლება გამოვიანგარიშოთ **A, B** ან **C** კლასების ქსელების რაოდენობა, თუ გავითვალისწინებთ, რომ ოქტეტში პირველი ბიტები უკვე რეზერვირებულია და **A** კლასში ქსელის ადრესაციისათვის არ შეიძლება გამოვიყენოთ 0.0.0.0. და 127.0.0.0 IP-მისამართები.

IP-მისამართების საჭირო დიაპაზონის მისაღებად ორგანიზაციებს სთავაზობდნენ სპეციალური სარეგისტრაციო ფორმის შევსებას, სადაც მითითებული იყო კომპიუტერების მიმდინარე რაოდენობა და კომპიუტერული პარკის დაგეგმილი ზრდა ორი წლის განმავლობაში.

თავდაპირველად მოცემული სქემა კარგად მუშაობდა, რადგან ქსელების რაოდენობა არ იყო დიდი. მაგრამ ინტერნეტის განვითარებასთან ერთად IP-მისამართების განაწილებისადმი ასეთმა მიდგომამ წარმოქმნა პრობლემები, განსაკუთრებით

მწვავე - **B** კლასის ქსელებისათვის. მართლაც, ორგანიზაციებს, რომელთა კომპიუტერების რიცხვი არ აღემატებოდა რამდენიმე ასეულს (ვთქვათ, 500), უხდებოდათ დაერეგისტრირებიათ თავისთვის **B** კლასის მთელი ქსელი. ამიტომ, **B** კლასის ხელმისაწვდომი ქსელების რაოდენობა "დნებოდა" თვალსა და ხელს შუა, ამავე დროს, IP-მისამართების უზარმაზარი დიაპაზონი უქმად იკარგებოდა.

პრობლემის გადასაწყვეტად შემუშავებულ იქნა *IP-ადრესაციის უკლასო სქემა* (*Classless InterDomain Routing, CIDR*), რომელშიც გარდა იმისა რტომ არ არის IP-მისამართის მიბმა ქსელის კლასისადმი და ქვექსელის ნიღაბისადმი, დაშვებულია ეგრეთწოდებული *ცვლადი სიგრძის ქვექსელის ნიღბების* გამოყენება (*Variable Length Subnet Mask, VLSM*). მაგალითად, თუ ზემოთ მითითებული 500 კომპიუტერიანი ორგანიზაციისათვის ქსელის გამოყოფისას 255.255.0.0 ფიქსირებული ნიღაბის გამოყოფის ნაცვლად გამოვიყენებთ ნიღაბს 255.255.254.0, მაშინ 512 შესაძლო IP-მისამართისაგან მიღებული დიაპაზონი იქნება სავსებით საკმარისი.

ასეთი მიდგომა საშუალებას იძლევა უფრო ეფექტურად გამოვყოთ ორგანიზაციებისათვის მათთვის საჭირო IP-მისამართების დიაპაზონები, და IP-მისამართების ნაკლებობის პრობლემა ნაკლებად მწვავე ხდება.

IP-მისამართები ლოკალური ქსელებისათვის

როგორც უკვე ვთქვით, ინტერნეტში გამოყენებული ყველა მისამართი უნდა დარეგისტრირდეს IANA-ში, რაც მათი უნიკალურობის გარანტიას იძლევა მთელი პლანეტის მასშტაბით. ასეთ მისამართებს ეძახიან *რეალურს*, ანუ *საჯარო* (*public*) IP-მისამართებს.

ინტერნეტთან მიუერთებელი ლოკალური ქსელებისათვის, ბუნებრივია, IP-მისამართების რეგისტრაცია არ არის საჭირო და შეიძლება გამოვიყენოთ ნებისმიერი შესაძლო მისამართი. ასეთი ქსელის ინტერნეტთან შემდგომი მიერთებისას რომ შესაძლო კონფლიქტების წარმოქმნა არ დავუშვათ, RFS 1918 იძლევა რეკომენდაციას, ლოკალურ ქსელებში გამოყენებულ იქნას *IP-მისამართების* ე. წ. *კერძო* (*private*), შემდეგი დიაპაზონები (ინტერნეტში ასეთი მისამართები არ არსებობენ და მათი გამოყენების საშუალებაც არ არსებობს):

- 10.0.0.0 – 10.255.255.255;
- 172.16.0.0 – 172.31.255.255;
- 192.168.0.0 – 192.168.255.255.

IP-მარშრუტიზაციის საფუძვლები

სხვა კომპიუტერებთან და ქსელებთან სწორად ურთიერთქმედებისათვის, როგორც უკვე ვთქვით, თითოეული კომპიუტერი ადგენს, რომელი IP-მისამართი ეკუთვნის მის ლოკალურ ქსელს და რომელი - დაშორებულ ქსელებს. თუ გაირკვა, რომ დანიშნულების კომპიუტერის IP-მისამართი ეკუთვნის ლოკალურ ქსელს, მაშინ პაკეტი ეგზავნება უშუალოდ დანიშნულების კომპიუტერს, ხოლო თუ ეს არის დაშორებული ქსელის მისამართი, მაშინ პაკეტი იგზავნება ძირითადი რაბის მისამართზე.

განვიხილოთ პროცესი დაწვრილებით. ავიღოთ კომპიუტერი IP პროტოკოლის შემდეგი პარამეტრებით:

- IP-მისამართი - 192.168.100.55;
- ქვექსელის ნიღაბი - 255.255.255.0;
- ძირითადი რაბი - 192.168.100.1.

IP პროტოკოლის გაშვებისას კომპიუტერზე სრულდება *ლოგიკური* „and“-ის *ოპერაცია მის საკუთარ IP-მისამართსა და ქვექსელის ნიღაბს* შორის, რის შედეგად IP-მისამართის ყველა ბიტი, რომლებიც შეესაბამებიან ქვექსელის ნიღაბის ნულოვან ბიტებს, აგრეთვე ხდებიან ნულოვანები:

- **IP-მისამართი 32-თანრიგიანი სახით** - 11000000 10101000 01100100 00110111;
  ქვექსელის ნიღაბი -
- 11111111 11111111 11111111 00000000;
  ქსელის იდენტიფიკატორი -
- 11000000 10101000 01100100 00000000.

ეს მარტივი ოპერაცია კომპიუტერს საშუალებას აძლევს დაადგინოს *საკუთარი ქსელის იდენტიფიკატორი* (ჩვენს მაგალითში - 192.168.100.0).

დავუშვათ კომპიუტერს უნდა გააგზავნოს IP-პაკეტი მისამართზე 192.168.100.15. ამისათვის კომპიუტერი ასრულებს *ლოგიკური* „and"-ის *ოპერაციას დანიშნულების კომპიუტერის IP-მისამართთან და საკუთარი ქვექსელის ნიღაბთან.* იოლი გასაგებია, რომ შედეგად მიღებული *დანიშნულების ქსელის იდენტიფიკატორი* დაემთხვევა კომპიუტერ-გამგზავნის საკუთარი ქსელის იდენტიფიკატორს. ასე ადგენს ჩვენი კომპიუტერი, რომ დანიშნულების კომპიუტერი იმყოფემა მასთან ერთად ერთ ქსელში და ასრულებს შემდეგ ოპერაციებს:

- ARP პროტოკოლის დახმარებით დადგენილ იქნება ფიზიკური MAC-მისამართი, რომელიც შეესაბამება დანიშნულების კომპიუტერის IP-მისამართს;
- საარხო და ფიზიკური დონეების პროტოკოლების დახმარებით ამ MAC-მისამართით გაიგზავნება საჭირო ინფორმაცია.

ახლა ვნახოთ, რა შეიცვლება, თუ პაკეტი უნდა გაიგზავნოს 192.168.10.20 მისამართზე. კომპიუტერი შეასრულებს დანიშ-ნულების ქსელის იდენტიფიკატორის დადგენის ანალოგიურ პროცედურას. შედეგად მიიღება მისამართი 192.168.10.0, რომელიც არ ემთხვევა კომპიუტერ-გამგზავნის ქსელის იდენტიფიკატორს. ასე დადგინდება, რომ დანიშნულების კომპიუტერი იმყოფება დაშორებულ ქსელში და კომპიუტერ-გამგზავნის მოქმედების ალგორითმი შეიცვლება:

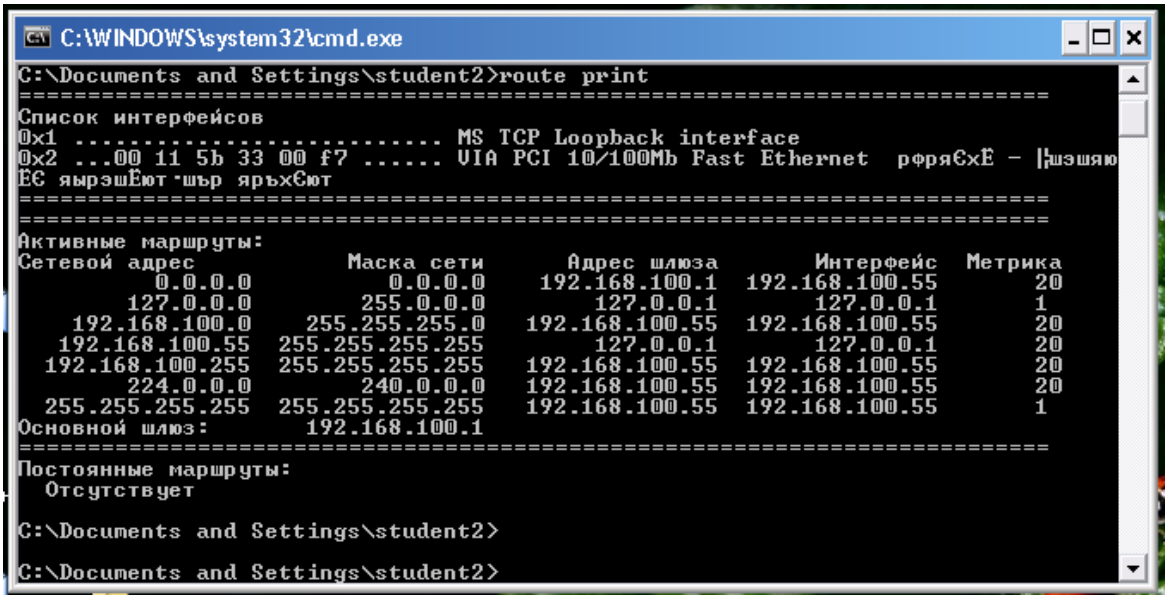
- დადგენილ იქნება არა დანიშნულების კომპიუტერის, არამედ მარშრუტიზატორის MAC-მისამართი;
- საარხო და ფიზიკური დონეების პროტოკოლების დახმარებით MAC-მისამართით მარშრუტიზატორი-სთვის გაიგზავნება საჭირო ინფორმაცია.

მიუხედავად იმისა, რომ ამ შემთხვევაში IP-პაკეტი არ მიეწოდება უშუალოდ დანიშნულებისამებრ, IP პროტოკოლი კომპიუტერ-გამგზავნზე თავის მისიას თვლის შესრულებულად (გაიხსენეთ, წერილის გაგზავნისას მხოლოდ ვაგდებთ მას საფოსტო ყუთში). IP-პაკეტის შემდგომი ბედი დამოკიდებულია

მარშრუტიზატორის სწორ აწყობაზე, რომელიც აერთიანებს 192.168.100.0 და 192.168.10.0 ქსელებს.

ამასთან, მოცემულ მაგალითში ადვილად შეიძლება იმის დემონსტრირება, თუ რამდენად მნიშვნელოვანია ქვექსელის ნიღაბის სწორი გამართვა IP-ადრესაციის პარამეტრებში. ვთქვათ, ჩვენ შეცდომით მივუთითეთ 192.168.100.200 კომპიუტერისათვის ქვექსელის ნიღაბი, რომელიც ტოლია 255.255.0.0. ამ შემთხვევაში, 192.168.10.20 მისამართზე პაკეტის გაგზავნის მცდელობისას ჩვენი კომპიუტერი ჩათვლის, რომ დანიშნულების კომპიუტერი იმყოფება მის საკუთარ ქსელში (ასეთი ნიღაბისას ქსელების იდენტიფიკატორები ერთმანეთს ემთხვევიან!), და ეცდება გააგზავნოს პაკეტი დამოუკიდებლად. შედეგად ეს პაკეტი ვერ მოხვდება მარშრუტიზატორში და ვერ იქნება დანიშნულებისამებრ მიტანილი.

იმისათვის, რომ გავიგოთ როგორ მუშაობენ მარშრუტიზატორები, ჯერ გავაანალიზოთ *მარშრუტების ცხრილი*, რომელსაც ამწკრივებს ჩვეულებრივი კომპიუტერი IP პროტოკოლის ჩატვირთვისას, მაგალითად, Windows XP ოპერაციული სისტემით (ნახ.8.1). ამისათვის მენიუ **"გაშვება"**-ში (**Start, *пуск***) ავირჩიოთ პუნქტი **შესრულება** (**Run, Выполнить** ...), შევიყვანოთ მოწოდებულ ველში ბრძანება **cmd** და დავაწკაპუნოთ თაგვით ღილაკზე **OK** (**Do it**), შემდეგ, გამოსულ DOS-გამოყენების ფანჯარაში გამოჩენილ დაპატიჟების სტრიქონში (მოციმციმე ტირე) შევიყვანოთ ბრძანება **route print** და დავაჭიროთ ღილაკს **Enter**.



ნახ. 8.1. მარშრუტების ცხრილა Windows XP ო ს-ით

ადვილი დასანახია, რომ ტაბულაში განსაზღვრულია რამდენიმე მარშრუტი განსხვავებული პარამეტრებით. მარშრუტების ტაბულაში თითოეული ჩანაწერის წაკითხვა საჭიროა შემდეგნაირად:

რომ მივაწოდოთ პაკეტი ქსელს მისამართით ველიდან ***ქსელური მისამართი (Netvork Destination, Сетевой адрес)*** *და ნიღაბით ველიდან* ***ქსელის ნიღაბი (Netmask, Маска сети),*** *საჭიროა ინტერფეისიდან IP-მისამართით ველიდან* ***ინტერფეისი (Interface, Интерфейс),*** *გავაგზავნოთ პაკეტი IP-მისამართზე ველიდან* ***რაბის მისამართი (Gateway, Адрес шлюза),*** *ხოლო ასეთი მიწოდების "ღირებულება" ტოლი იქნება რიცხვის ველიდან* ***მეტრიკა (Metric, Метрика).***

პარამეტრები **ქსელური მისამართი** და **ქსელის ნიღაბი** ერთად იძლევიან მოცემულ ქსელში ყველა ნებადართული IP-მისამართების დიაპაზონს. მაგალითად, 127.0.0.0 და 127.255.255.254, როგორც უკვე ვთქვით, ნიშნავს ნებისმიერ IP-მისამართს 127.0.0.0-დან 127.255.255.254-დე. გავიხსენოთ აგრეთვე, რომ IP-მისამართს 127.0.0.1 ეწოდება "დახშობის მისამართი" - ამ მისამართზე გაგზავნილი პაკეტები უნდა დამუშავდეს თავად კომპიუტერით. გარდა ამისა, ნიღაბი 255.255.255.255 ნიშნავს ქსელს ერთადერთი IP-მისამართით, ხოლო კომბინაცია 0.0.0.0 - ნებისმიერ განუსაზღვრელ მისამართს ან ქვექსელის ნიღაბს. მაშინ მარშრუტების ტაბულის პირველი სტრიქონი ნიშნავს იმას, რასაც აკეთებს კომპიუტერი, როდესაც აუცილებელია პაკეტის გაგზავნა დაშორებულ, ე. ი. მარშრუტიზაციის ტაბულიდან მისთვის უცნობ ქსელში - თავისი ინტერფეისიდან პაკეტი იგზავნება მარშრუტიზატორის IP-მისამართზე.

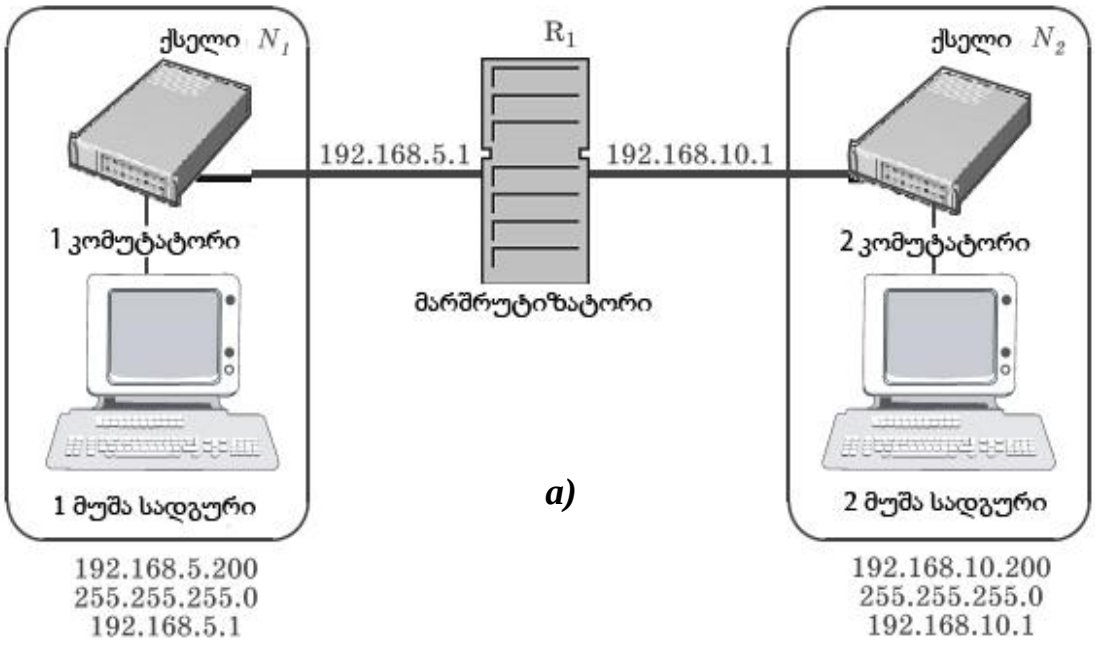
ტაბულის მეორე სტრიქონი აიძულებს კომპიუტერს გაუგზავნოს თავის თავს ყველა პაკეტი (და პასუხი გასცეს მათზე), რომელიც გაგზავნილია ნებისმიერ IP-მისამართზე 127.0.0.1 - 127.255.255.254 დიაპაზონიდან.

მესამე სტრიქონში განსაზღვრულია, როგორ უნდა გაეგზავნოს პაკეტი ლოკალური ქსელის კომპიუტერებს (მისამართებზე დიაპაზონიდან 192.168.100.1 - 192.168.100.254). მკაფიოდ ჩანს, რომ ეს უნდა შეასრულოს თავად კომპიუტერმა - რაბის მისამართი არის მისი საკუთარი IP-მისამართი 192.168.100.55.

ანალოგიურად (ტაბულის მეხუთე, მეექვსე და მეშვიდე სტრიქონები) უნდა მოვიქცეთ იმ შემთხვევაშიც, როდესაც პაკეტები მიიმართება ქვექსელის დაგაგზავნის მისამართზე (192.168.100.255), მრავალმისამართიანი დაგაგზავნის მისამართებზე (224.0.0.0) ან ლოკალური ფართომაუწყებლური დაგზავნის მისამართებზე (255.255.255.255).

მეოთხე სტრიქონი ნიშნავს, რომ 192.168.100.55 IP-მისამართით გაგზავნილი პაკეტები (მიაქციეთ ყურადღება ნიღაბს!), უნდა მუშავდებოდეს თავად კომპიუტერის მიერ.

რამდენადმე რთული სახე ექნება მარშრუტიზაციის ტაბულას კომპიუტერისათვის ორი ქსელური ადაპტერით, რომელსაც გამოვიყენებთ მარშრუტიზატორად არც თუ ისე დიდი ქსელის ორი სეგმენტის გასაერთიანებლად (ნახ. 8.2).



a)

b)

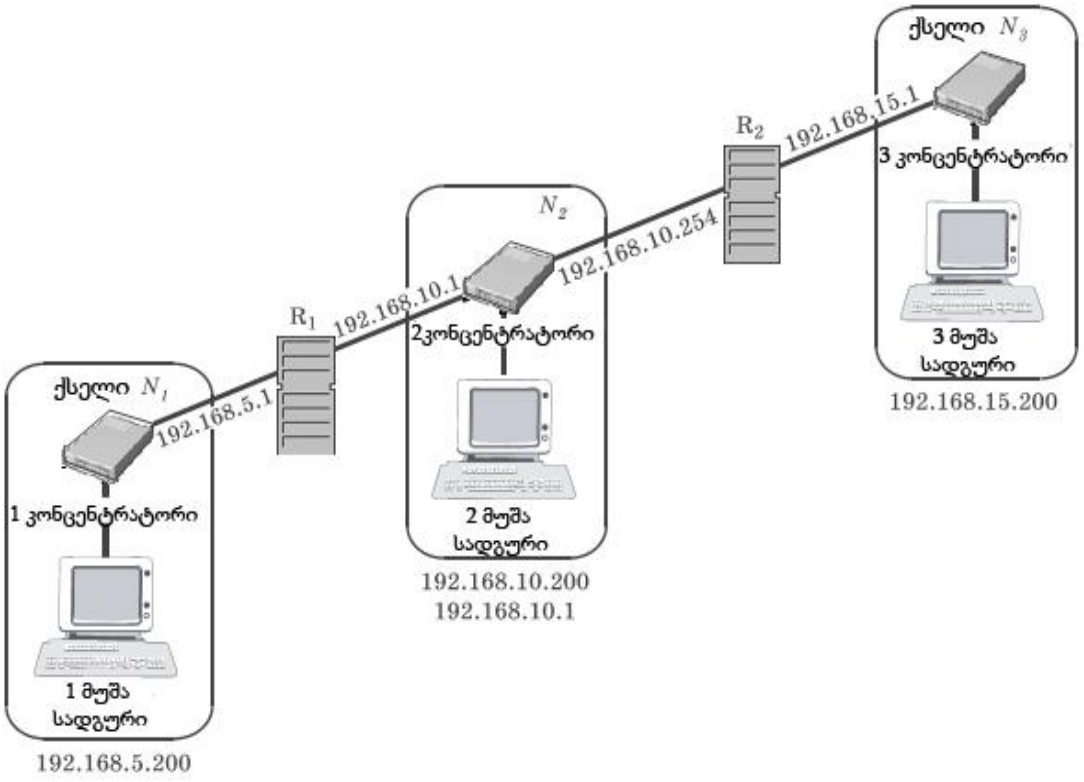
```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
        192.168.5.0  255.255.255.0      192.168.5.1     192.168.5.1      20
        192.168.5.1  255.255.255.255      127.0.0.1       127.0.0.1      20
      192.168.5.255  255.255.255.255    192.168.5.1     192.168.5.1      20
       192.168.10.0  255.255.255.0      192.168.10.1    192.168.10.1     20
       192.168.10.1  255.255.255.255      127.0.0.1       127.0.0.1      20
     192.168.10.255  255.255.255.255    192.168.10.1    192.168.10.1     20
          224.0.0.0        240.0.0.0      192.168.5.1     192.168.5.1      20
          224.0.0.0        240.0.0.0      192.168.10.1    192.168.10.1     20
    255.255.255.255  255.255.255.255      192.168.5.1     192.168.5.1      1
    255.255.255.255  255.255.255.255      192.168.10.1    192.168.10.1     1
```

ნახ. 8.2. ქსელის გაერთიანება მარშრუტიზატორის დახმარებით (*a*) და R_1 კომპიუტერის მარშრუტიზაციის ტაბულა (*b*)

ამ ცხრილში ჩანს რამდენიმე დამატებითი სტრიქონი, რომელიც აღნიშნავს მარშრუტიზაციას უკვე ორ ქსელში - 192.168.5.0 და 192.168.10.0. აღვნიშნოთ, რომ ყველა მარშრუტი იქნება აგებული ავტომატურად.

ქსელებს შორის IP-პაკეტებით ურთიერთგაცვლის გასამართავად, უნდა შევასრულოთ შემდეგი მოქმედებები:

- ჩავრთოთ მარშრუტიზაცია R_1 კომპიუტერზე - ეს შესაძლებელია თუ გავმართავთ, მაგალითად, მარშრუტიზაციისა და დაშორებული შეღწევის სამსახურს, რომელიც შედის Windows Server 2003 ოპერაციული სისტემის შემადგენლობაში;



ნახ. 8.3. ქსელი ორი მარშრუტიზატორით

- N_1 ქსელის ყველა კომპიუტერზე პარამეტრი **ძირითადი რაზი** უნდა დავაყენოთ ამ ქსელში ჩართული მარშრუტიზატორის ინტერფეისის IP-მისამართის ტოლი, ე. ი. 192.168.5.1-ს ტოლი, ხოლო N_2 ქსელის კომპიუტერებზე - 192.168.10.1-ს ტოლი.

ამგვარად, მარშრუტიზატორი - პროგრამულ- აპარატურული მოწყობილობაა, რამდენიმე ქსელური ინტერფეისით, რომელზედაც მუშაობს *მაშრუტიზაციის სამსახური.*

გავართულოთ ჩვენი ქსელი - დავამატოთ მეორე მარშრუტეზატორი და N_3 ქსელი, რომლის მისამართია 192.168.15.0 (ნახ. 8.3).

ასეთ ქსელში მარშრუტიზაციის აწყობა რთულდება. მიუხედავად იმისა, რომ R_1 მარშრუტიზატორმა იცის როგორ უნდა გააგზავნოს პაკეტები N_1 და N_2 ქსელებში, მარშრუტი N_3 ქსელში მას არა აქვს. თავის მხრივ R_2 მარშრუტიზატორს არა აქვს მარშრუტი N_1 ქსელში. ე. ი. IP-პაკეტებით გაცვლა N_1 და N_3 ქსელებს შორის იქნება შეუძლებელი.

ამ პრობლემის გადაწყვეტა პატარა ქსელში საკმაოდ მარტივია - უბრალოდ უნდა დავამატოთ საჭირო ჩანაწერები R_1 და R_2 მარშრუტიზატორების ტაბულებში. ამისათვის R_1 მარშრუტიზატორზე საკმარისია შევასრულოთ ბრძანება დანიშნულებით - ყველი პაკეტი განკუთვნილი 192.168.15.0 ქსელისათვის, მიმართულ იქნას 192.168.10.254 მისამართისკენ (ე. ი. მეორე მარშრუტიზატორისათვის, რომელიც უკვე შეძლებს მიაწოდოს ეს პაკეტები დანიშნულების ადგილს; გასაღები P გამოიყენება, რომ მარშრუტი გახდეს მუდმივი):

```
ROUTE – P ADD 192168.5.0
        MASK 255.255.255.0 192.168.10.254
```

მარშრიტაზატორის IP-მისამართად მიღებულია ან პირველი, ან ბოლო შესაძლო მისამართის არჩევა მოცემული IP-ქსელის მისამართებიდან.

ანალოგიური ბრძანება R_2 მარშრუტიზატორზე უნდა გამოიყურებოდეს ასე:

```
ROUTE – P ADD 192.168.15.0
        MASK 255.255.255.0 192.168.10.1
```

ამის შემდეგ ურთიერთქმედება თქვენს ქსელში იქნება გამართული.

მსხვილ ქსელებში, რომლებიც შეიცავენ ერთმანეთთან შეერთებულ დიდი რაოდენობის ქვექსელებს, მექანიკურად, ხელით პაკეტების მიწოდების მარშრუტების გაწერა ყველა მარშრუტიზატორზე საკმაოდ დამქანცველია. ამასთან, ასეთი მარშრუტები *სტატიკურია*, ე. ი., ქსელის კონფიგურაციის ყოველი ცვლილებისას საჭირო იქნება დიდი სამუშაოს შესრულება IP-მარშრუტიზაციის სისტემის შესაცვლელად.

ამის თავიდან ასაცილებლად, საკმარისია მარშრუტიზატორები გავმართოთ ისე, რომ მათ *მარშრუტების შესახებ ინფორმაცია ცვალონ ერთმანეთთან*. ამისათვის ლოკალურ ქსელებში იყენებენ პროტოკოლებს *RIP* (*Routing Information Protocol*) და *OSPF* (*Open Shortest Path First*). პროტოკოლი RIP უფრო მარტივია გამართვაში, ვიდრე OSPF, მაგრამ ინფორმაციის გაცვლისათვის მასში გამოიყენება ფართომაუწყებლური შეტყობინებები, რომლებიც საგრძნობლად ტვირთავენ ქსელს. ამიტომ RIP-ს ჩვეულებრივ იყენებენ პატარა ქსელებში. პროტოკოლი OSPF მუშაობს უფრო ეფექტურად, მაგრამ მეტად რთულად გასამართია, თუმცა გამოყენება რეკომენდებულია მსხვილი კორპორატიული ქსელებისათვის.

IP-მისამართების დანიშნვა და TCP/IP-ს ქმედითუნარიანობის შემოწმება

ჩვენ უკვე ვნახეთ, რამდენად მნიშვნელოვანია IP პროტოკოლის გამართვა TCP/IP ქსელში კომპიუტერების ურთიერთქმედებისათვის. მნიშვნელოვანია განვიხილოთ, როგორი ხერხებით შეიძლება IP პარამეტრების გამართვა კომპიუტერებზე და სწრაფად როგორ შევამოწმოთ IP-ადრესაციისა და მარშრუტიზაციის ქმედითუნარიანობა.

IP პროტოკოლის პარამეტრების გამართვის ყველაზე მარტივი ხერხია - მათი ხელით დანიშვნა. მეთოდის უპირატესობა განპირობებულია იმით, რომ ქსელური ადმინისტრატო–

რები მთლიანად აკონტროლებენ ქსელის ყველა კომპიუტერის IP-მისამართს, რაც მნიშვნელოვანი შეიძლება იყოს მონაცემების დაცვის ან ინტერნეტთან ურთიერთქმედების თვალსაზრისით. ამ მეთოდს აქვს ბევრი ნაკლი. უპირველეს ყოვლისა, ადვილად შეიძლება შეცდომის დაშვება და ნიღაბის ან რაბის არასწორი პარამეტრების შეყვანა ან, უფრო უარესი, ქსელში განმეორებადი IP-მისამართის დანიშვნა. მეორედ, ქსელში IP-ადრესაციის პარამეტრების ცვლილებისას (მაგალითად, მარშრუტიზატორის IP-მისამართის შეცვლისას) მოგვიწევს ყველა კომპიუტერის ხელახალი გამართვა. გამართვის ასეთი ხერხისას პრაქტიკულად შეუძლებელია მუშაობა მსხვილ კორპორატიულ ქსელებში ნოუთბუქებით ან ჯპკ-ს ტიპის მობილური მოწყობილობებით, რომლებიც ხშირად გადაადგილდებიან ქსელის ერთი სეგმენტიდან მეორეში.

ორგანიზაციებში უფრო ხშირად იყენებენ სპეციალურ სერვერებს, რომლებიც მხარს უჭერენ *კვანძების დინამიკური კონფიგურირების პროტოკოლს* (*Dynamic Host Configuration Protocol, DHCP*). მათი ამოცანა მდგომარეობს IP-მისამართის ან სხვა ინფორმაციის მიღებისათვის კლიენტის მოთხოვნების მომსახურებაში, რაც აუცილებელია ქსელის სწორი მუშაობისათვის. სწორედ ამიტომ კომპიუტერები Windows ოპერაციული სისტემით დუმილით არიან გამართული IP-მისამართის ავტომატურ მიღებაზე.

თუ DHCP სერვერი არ არის ხელმისაწვდომი (არ არის ან არ მუშაობს), მაშინ Windows 98 ვერსიიდან დაწყებული კომპიუტერები თავად ინიშნავენ IP-მისამართს. ამ დროს გამოიყენება *პირადი IP-ადრესაციის ავტომატური* მექანიზმი (*Automatic Private IP Addressing*), რისთვისაც კორპორაცია Microsoft-ს მიერ IANA-ში დარეგისტრირებულ იქნა მისამართების დიაპაზონი 169.254.0.0 - 169.254.255.255.

დაბოლოს, განვიხილოთ, როგორი ნაბიჯები უნდა გადავდგათ *IP პროტოკოლის პარამეტრებისა და ქმედითუნარიანობის შესამოწმებლად.*

შეგახსნებთ, IPCONFIG და PING უტილიტებთან სამუშაოდ საჭიროა DOS-რეჟიმის ფანჯრის გახსნა, ავირჩიოთ მენიუ **გაშვებაში** (Start ან Пуск) პუნქტი **შესრულება** (Run ან Выполнить), შევიყვანოთ ბრძანება **cmd** და დავაწკაპუნოთ თაგვით ღილაკზე **OK**.

1. **შეასრულეთ ბრძანება IPCONFIG/ALL**

   თუ ეკრანზე გამოტანილი ინფორმაცია არ შეიცავს არავითარ პარამეტრს, გამოდის, რომ თქვენ არ გაქვთ აქტიური ინტერფეისები.

   თუ გამოტანილ ინფორმაციაში არის დიაგნოსტიკური შეტყობინება "ქსელი გათიშულია", მაშინ, თქვენ გაქვთ პრობლემები ფიზიკურ დონესთან - შეამოწმეთ კონექტორის შეერთება ქსელური ადაპტერის გასართთან და/ან კომუტატორების შრომისუნარიანობა.

   თუ თქვენი IP-მისამართის და ქვექსელის ნიღბის პარამეტრები 0.0.0.0-ს ტოლია, ეს ნიშნავს, რომ თქვენ მოიხმართ სტატიკურ IP-მისამართს, რომელიც კონფლიქტშია ქსელის სხვა კვანძთან.

   თუ თქვენი IP-მისამართი იმყოფება 169.254.*x.x* დიაპაზონში, მაშინ, DHCP-სერვერი არ არის ხელმისაწვდომი და ქსელში მუშაობას თქვენ შეძლებთ მხოლოდ იმ კომპიუტერებთან, რომლებმაც დამოუკიდებლად დაინიშნეს თავისთვის მისამართი.

   ნორმალურ სიტუაციაში, IP-მისამართის DHCP-სერვერისგან მიღებისას ან ხელით სწორად გამართვით, ეკრანზე გამოტანილ ინფორმაციაში თქვენ უნდა დაინახოთ ისეთი პარამეტრები, როგორიცაა კომპიუტერის IP-მისამართი, ქვექსელის ნიღაბი, ძირითადი რაბი, DNS-სერვერი, DHCP-სერვერი (და აგრეთვე, შესაძლოა, სხვა პარამეტრები).

2. **შეასრულეთ ბრძანება PING 127.0.0.1**

   თუ პასუხი არ არის მიღებული, ეს ადასტურებს TCP/IP პროტოკოლების სტეკის არასწორ გამართვას; მოგვიწევს შესაბამისი პროგრამული მხარდაჭერის გადაყენება.

   თუ პასუხი მიღებულია, ეს მიშნავს, რომ TCP/IP პროტოკოლთა სტეკი მუშაობს გამართულად.

3. **შეასრულეთ ბრძანება PING w.x.y.z, სადაც w.x.y.z არის მეზობელი კომპიუტერის IP-მისამართი.**

   ასე მოწმდება ლოკალური ქსელის ქმედითუნარიანობა.

4. **შეასრულეთ ბრძანება PING w.x.y.z, სადაც w.x.y.z არის ძირითადი რაბის IP-მისამართი.**

   ასე მოწმდება რაბის ხელმისაწვდომობა და ქმედითუნარიანობა.

5. **შეასრულეთ ბრძანება PING w.x.y.z, სადაც w.x.y.z არის ნებისმიერი დაშორებული კომპიუტერის IP-მისამართი.**

ასე მოწმდება თქვენი კორპორატიული ქსელის ან ინტერნეტთან მიერთების მარშრუტიზაციის მთელი სისტემის ქმედითუნარიანობა.

ბევრ თანამედროვე ქსელებში ICMP პროტოკოლის პაკეტები, რომლითაც PING უტილიტა უკეთებს ტესტირებას ქსელურ ურთიერთქმედებას, აკრძალულია უსაფრთხოების სამსახურების მოთხოვნით. ოპერაციული სისტემა (ოს) Windows XP SP2, ჩართული ქსელთაშორისი ეკრანით, ასევე ბლოკირებას უკეთებს ICMP-პაკეტებს. ამიტომ, თუ PING უტილიტა არ გვიჩვენებს პასუხებს, არ იჩქაროთ ”გაჩერების” მიზეზების ძებნა საკუთარ კომპიუტერზე. ჯერ გაარკვიეთ ქსელურ ადმინისტრატორთან (ან საკუთარი Windows XP ოს გაწყობაში), ნებადართულია თუ არა თქვენს ქსელში ICMP-ს გამოყენება.

ბოლოს მოვიყვანთ მოკლე წესების კრებულს, რომლებიც დაგეხმარებათ არ შეცდეთ IP-ადრესაციისა და მარშრუტიზაციის გამართვისას TCP/IP ქსელებში:

1) TCP/IP ქსელში ურთიერთქმედებისათვის, ყველა კომპიუტერს უნდა ჰქონდეს IP-მისამართი;
2) კომპიუტერებს, რომლებიც იმყოფებიან ქსელის ერთსა და იგივე ფიზიკურ სეგმენტში (შეერთებულები კონცენტრატორებით ან კომუტატორებით), უნდა ეკუთვნოდნენ ერთი დაიგივე IP-ქსელს, მაგრამ ჰქონდეთ უნიკალური IP-მისამართები;
3) ლოკალური ქსელის ან დაშორებული ქსელის იდენტიფიკატორების დასადგენად გამოიყენება ქვექსელის ნიღაბი;
4) დაშორებულ ქსელებთან ურთიერთქმედებისათვის, კომპიუტერებს ესაჭიროებათ ძირითადი რაბის მისამართი, რომელიც უნდა ემთხვევოდეს თქვენი და სხვა ქსელების შემაერთებელი მარშრუტიზატორის მისამართს;
5) მარშრუტიზატორი არის კომპიუტერი რამდენიმე ქსელური ინტერფეისით, შეუძლია IP-პაკეტების გადაცემა ერთი ქსელიდან მეორეში მარშრუტიზაციის საკუთარი ტაბულების შესაბამისად;
6) მარშრუტიზატორს ყოველთვის აქვს მარშრუტები ყველა მასთან უშუალოდ მიერთებულ ქსელში; მარშრუტები სხვა ქსელებში უნდა გაიმართოს;
7) მარშრუტიზაციის ტაბულები შეიძლება გაიმართოს ხელით ან გამოვიყენოთ მარშრუტიზაციის შესახებ ინფორმაციის გაცვლის დინამიური პროტოკოლები.

?

კითხვები და დავალებები

1. რომელი პარამეტრები და გაწყობა-გამართვებია აუცილებელი TCP/IP პროტოკოლთა სტეკის მუშაობისათვის?
2. რა არის IP-მისამართი? როგორია მისი სტრუქტურა? IP-მისამართის წარმოდგენის როგორი ხერხებია შესაძლებელი?
3. რით განსხვავდება IP პროტოკოლის 4 და 6 ვერსიები? რა უპირატესობებს უზრუნველყოფს IP პროტოკოლის ვერსია 6? რატომ წარმოიქმნა IP პროტოკოლის ვერსია 6-ზე გადასვლის აუცილებლობა?
4. რა არის ქვექსელის ნიღაბი? რისთვის არის საჭირო ის?
5. რაში მდგომარეობს IP-მისამართის გაყოფა ქსელისა და კვანძის იდენტიფიკატორებად? რისთვის არის ეს საჭირო?
6. რომელი IP-მისამართები და ნიღბებია დასაშვები და რომელი არა? რატომ?
7. რაშია განსხვავება კლასობრივ და უკლასო IP-მისამართებს შორის? როგორია მათი უპირატესობები და ნაკლოვანი მხარეები?
8. რა არის IP-მისამართების კლასები? რა წესებით ხდება მათი განსაზღვრა?
9. როგორ დავნიშნოთ IP-მისამართი ლოკალურ ქსელში (ინტერნეტში გასვლის გარეშე)?
10. როგორია პაკეტების მარშრუტიზაციის ძირითადი პრინციპები ლოკალურ და დაშორებულ ქსელებში?
11. რა არის მარშრუტების ტაბულა (მარშრუტიზაციის ტაბულა)? ახსენით მისი ყოველი სვეტის არსი.
12. როგორ გავუფორმოთ "ჩაწერა" მარშრუტიზაციის ტაბულაში იქ არარსებულ ახალ მარშრუტს?
13. რა არის კვანძის დინამიური კონფიგურაცია? რისთვის არის ის საჭირო?
14. რაში მდგომარეობს ავტომატური პირადი IP-ადრესაციის ტექნოლოგია?
15. როგორია IP პროტოკოლის ქმედითუნარიანობის შემოწმების ტიპიური ალგორითმი?
16. იპოვეთ ინტერნეტში დამატებითი ინფორმაცია IP-მისამართების განაწილების პრინციპების შესახებ.

თავი 9

ვაწყობთ მუშაობას ქსელში: ქსელური სამსახურები, კლიენტები, სერვერები, რესურსები. დაცვა ქსელში მუშაობისას

ამ თავში
თქვენ ნახავთ პასუხებს შემდეგ კითხვებზე:

- რისთვის არის საჭირო ქსელური ოპერაციული სისტემა?
- როგორ ფუნქციებს ასრულებენ კლიენტური და სერვერული ოპერაციული სისტემები (ოს)?
- როგორი სამსახურები უზრუნველყოფენ ურთიერთქმედებას კლიენტურ და სერვერულ ოს-ს შორის Microsoft ქსელებში?
- სერვერის როგორი ტიპები არსებობენ?
- როგორ იგება უსაფრთხოების სისტემა თანამედროვე ქსელურ ოს-ში?
- დაცვის როგორი ზომების მიღებაა რეკომენდებული ქსელში მუშაობისას?

ამგვარად, ჩვენი ქსელი ამუშავდა. კომპიუტერები გაერთიანებულია კომუტატორების, შეღწევის წერტილებისა და, შესაძლოა, მარშრუტიზატორების დახმარებით, ყველგან დაყენებულია TCP/IP პროტოკოლი და კორექტულადაა გამართული IP პარამეტრები.

ახლა უნდა ვისწავლოთ ქსელში მუშაობის წესები. ამისათვის ჩვენ დაგვჭირდება *ქსელური ოპერაციული სისტემები (ოს)*, რომელთა დახმარებით მომხმარებლები შეძლებენ ინფორმაციის გაცვლას ერთმანეთში, ერთობლივად იმუშაონ მონაცემებთან, გამოიყენონ საერთო რესურსები და ა. შ.

ქსელური ოს შეიძლება გავყოთ *კლიენტურებზე* - Windows 2000 Professional, Windows XP Home Edition ან Windows XP Professional, და *სერვერულებზე* - Windows Server 2003.

კლიენტური ქსელური ოს-ს ძირითადი ფუნქციაა - მიაწოდოს მომხმარებელს მოხერხებული ინტერფეისი ქსელურ გამოყენებებთან და სამსახურებთან მუშაობისათვის, ამავე დროს უნდა უზრუნველყოს კომპიუტერის მაქსიმალური დაცვა და უსაფრთხოება მონაცემებთან და რესურსებთან შეღწევისას. სერვერები ასრულებენ სერვისულ ფუნქციებს, აწვდიან რა თავის მონაცემებსა და რესურსებს ერთობლივი მოხმარებისათვის, აგრეთვე ემსახურებიან სხვადასხვა კლიენტურ მოთხოვნებს.

მაინც როგორ სერვისებს იყენებენ ოპერაციული სისტემები ქსელში მუშაობისათვის? დავიწყოთ კლიენტური ოპერაციული სისტემებით. თუ გადავხედავთ კომპონენტების სიას Windows 2000 Professional ოს-ს ქსელური მიერთებებით (გარდა TCP/IP პროტოკოლისა), რომელიც უზრუნველყოფს ქსელთაშორის სატრანსპორტო ფუნქციებს, შეიძლება დავინახოთ კიდევ ორი სერვისი: *Microsoft ქსელების ფაილებთან და პრინტერებთან შეღწევის სამსახური* და *კლიენტი Microsoft ქსელებისათვის*. ეს ორი სამსახური განუყრელად არის დაკავშირებული ერთმანეთთან: პირველი გამოიყენება კატალოგებისა და პრინტერების მიწოდებისათვის საერთო შეღწევისას, მეორე - მათთან

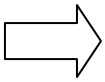
ქსელებით მისაერთებლად.

Windows XP ოპერაციული სისტემის მიერ დამატებით მიეწოდება *QoS (Quality of Service) პაკეტების დამგეგმველი* - სამსახური, რომელიც იძლევა გატარების საერთო ზოლის რაღაც ნაწილის *რეზერვირების* საშუალებას, ხოლო შემდეგ გამოყოფს მას ისეთი გამოყენებებისათვის, სადაც შეყოვნებები დაუშვებელია (მაგალითად, ქსელით ვიდეოგამოსახულებისა და საუბრის გადაცემისას ვიდეოკონფერენცკავშირისას).

ამგვარად, კლიენტურ ოს-შიც დუმილით არის გათვალისწინებული ფაილებთან და პრინტერებთან შეღწევის სერვისული სამსახური. ეს სამსახური საშუალებას იძლევა საშინაო და საოფისე პატარა ქსელებში თავი ავარიდოთ სერვერის გამოყენებას (ასეთ ქსელებს, შაგახსენებთ, ეწოდება *ერთრანგიანი*, ან *მუშა ჯგუფები*). კომპიუტერების რაოდენიბა მათში ჩვეულებრივად არ აღემატება 10-ს (სიტყვამ მოიტანა, სწორედ ამდენი მიერთებაა გათვალისწინებული Windows კლიენტურ ოს-ში). ერთრანგიან ქსელებში კლიენტები ჩვეულებრივ უერთებიან ერთ კონცენტრატორს ან კომუტატორს და მარშრუტიზატორები არ გამოიყენება. იმისათვის, რომ აღმოაჩინონ „მეზობლები“, კომპიუტერები იყენებენ ფართომაუწყებლურ შეტყობინებებს, და ამ დროს IP-მისამართებად სახელების გარდაქმნის არავითარი სისტემებს არ საჭიროებენ.

მსხვილ ქსელებში სერვერების გარეშე უკვე შეუძლებელია. უფრო მეტიც, კორპორატიული მომხმარებლების მუდამ მზრდადი მოთხოვნების დასაკმაყოფილებლად, გამუდმებით უხდებათ სერვერების რაოდენობის და ფუნქციონალურობის გაზრდა, მათი აპარატურული შესაძლებლობების გაფართოება. ბევრი სერვერის გამოშვება *სპეციალიზირებული* სახით ხდება - განკუთვნილია კონკრეტული სამსახურებისა და გამოყენებების მხარდასაჭერად. სხვა, არც თუ რთული სერვისები, შეიძლება პირიქით, *გავაერთიანოთ* (*გავხადოთ კონსოლიდირებული*) ერთი მძლავრი აპარატული სერვერის ჩარჩოებში.

განვიხილოთ სერვერების ძირითადი ტიპები



სერვერები, რომლებიც უზრუნველყოფენ TCP/IP ქსელში მუშაობას, ანუ ქსელური ინფრასტრუქტურის სერვერები. მათ რიცხვს შეიძლება მივაკუთვნოთ DHCP-, DNS-, WINS-სერვერები; ჩვეულებრივად მსხვილ ქსელებში მუშაობის აწყობა-გამართვას იწყებენ სწორედ მათგან:

- *DHCP-სერვერები* უკვე ვახსენეთ წინა თავში. ისინი

საჭიროა, რომ *DHCP-კლიენტის* მოთხოვნით (კომპიუტერის, რომლის TCP/IP-აწყობებში ჩართულია IP-მისამართის ავტომატური მიღების რეჟიმი) გაიცეს პარამეტრები: უნიკალური IP-მისამართი და ქვექსელის ნიღაბი. გარდა ამათისა, კლიენტმა DHCP-სერვერისგან შეიძლება მიიღოს დამატებითი პარამეტრების რიგი, რომლებიც მნიშვნელოვანია სხვა ქსელებთან ურთიერთქმედებისათვის და მოხერხებულია ქსელში მუშაობისათვის, მაგალითად, ძირითადი რაბის მისამართი, DNS- და WINS-სერვერების მისამართები, დომენის დასახელება, რომელშიც შედის ეს კომპიუტერი და ზოგიერთი სხვა;

სერვერის ქვეშ სხვადასხვა შემთხვევებში შეიძლება იგულისხმებოდეს როგორც თავად კომპიუტერი, ასევე მასზე დაყენებული სპეციალიზებული პროგრამული უზრუნველყოფა, ან მთელი ეს პროგრამულ-აპარატურული კომპლექსი მთლიანობაში.

- DNS-სერვერები ასრულებენ ძალზე მნიშვნელოვან ფუნქციას - *გარდაქმნიან* (*განარჩევენ*) *კვანძების სახელებს* (*host names*) *მათ შესაბამის IP-მისამართებად*. შეგახსენებთ: DNS (Domain Name System) ნიშნავს ”დომენურ სახელების სისტემას (სამსახურის)”. DNS სამსახური რეალიზებულ იქნა ინტერნეტში 1981 წელს, ხოლო 2000 წლიდან (Windows 2000 ოს-ს გამოსვლასთან ერთად) ის გახდა Microsoft ქსელებში სახელების გარდაქმნის ძირითადი სამსახური;

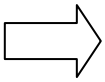
- *WINS-სერვერები* NetBIOS-ქსელებში არეგისტრირებენ კომპიუტერების სახელებს და მათ IP-მისამართებს, ხოლო შემდეგ *WINS--კლიენტების* მოთხოვნით გარდაქმნიან მათ IP-მისამართებად. სახელწოდება WINS (Windows Internet Name Service) ითარგმნება როგორც ”ქსელთაშორისი სახელების Windows სამსახური”; ეს სამსახური შემუშავდა იმისათვის, რომ მხარი დაუჭიროს NetBIOS-გამოყენებების მუშაობას ქსელებში TCP/IP პროტოკოლის ბაზაზე. ამჟამად გამოიყენება იმისათვის, რომ ქსელში კორექტულად იმუშაონ ისეთმა მოძველებულმა ოს-ებმა, როგორიცაა Windows 9*x* და Windows NT.

შეგახსენებთ, რომ კომპიუტერები ერთმანეთთან ურთიერთქმედებისათვის იყენებენ IP-მისამართებს. ჩვენთვის, კი რიცხვით IP-მისამართებთან მუშაობა მოუხერხებელია, ამიტომ ქსელებში მუშაობისას ხშირად გამოიყენება კომპიუტერების სიტყვიერი სახელები. (თუმცა, გამოყენებების აბსოლუტურ უმრავლესობაში შეიძლება უშუალოდ IP-მისამართების გამოყენებაც; ხანდახან ეს ძალიან მოსახერხებელია

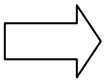
გამოყენებების შესამოწმებლად, განსაკუთრებით თუ სახელების განრჩევის სისტემები მოცემულ ქსელში არ მუშაობენ).

ამასთან შესაძლოა კომპიუტერის ორი ტიპის სახელები:

- *კვანძების სახელები* - შედგებიან წერტილებით გაყოფილი ასოების, ციფრებისა და დეფისის ნიშნის კომბინაციისაგან. ეს შეიძლება იყოს კომპიუტერების სახელები, როგორც ინტერნეტში (მაგალითად: www. microsoft.com), ასევე ლოკალურ ქსელში (server.domain.local);
- NetBIOS-სახელები - კომპიუტერების "საკუთარი" სახელები, რომლებიც შეიცავენ არაუმეტეს 15 ნებისმიერი სიმბოლოსი (მაგალითად, SERVER1).



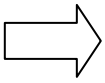
ფაილების სერვერები (ფაილ-სერვერები) საჭიროა მონაცემთა დიდი მოცულობის შენახვისათვის და მათთვის მომხმარებლების შეღწევის მიწოდების მიზნით. ფაილების ერთ სერვერს შეუძლია ერთდროულად მხარი დაუჭიროს ასობით და ათასობით მომხმარებლის მუშაობას. ინფორმაციის საიმედო შენახვის უზრუნველსაყოფად ფაილ-სერვერები, როგორც წესი, აღჭურვლები არიან მყარი დისკოების დაზიანებისადმი მდგრადი კრებულებითა (მასივებით) და მაგნიტურ ფირზე ან სხვა მატარებელზე სარეზერვო კოპირების სისტემებით.



ბეჭდვის სერვერები (პრინტ-სერვერები) განკუთვნილია ერთ ან რამდენიმე საერთო პრინტერთან მომხმარებლის მისაწვდომობის უზრუნველსაყოფად. ისინი ქსელით ღებულობენ მომხმარებლური გამოყენებებისაგან შემოსულ ბეჭდვის დავალებებს და ემსახურებიან რა, ჩვეულებრივ, რამოდენიმე პრინტერს, მართავენ *ბეჭდვაზე დავალებების რიგებს.*

მსგავს ფუნქციებს ასრულებენ **ფაქს-სერვერები**, რომლებიც ემსახურებიან კლიენტურ დავალებებს ფაქსის გაგზავნაზე. ისინი, გარდა ამისა, პასუხისმგებელნი არიან ფაქსის მიღებასა და მომხმარებლისათვის მიწოდებაზე.

ფაილ-სერვერები და ბეჭდვის სერვერები - ერთ-ერთი ყველაზე გავრცელებული სერვერებია.



გამოყენებების სერვერები მომხმარებლის მოთხოვნების მომსახურების ამოცანებს ასრულებენ რაიმე ინფორმაციის ამორჩევასთან ან დამუშავებასთან დაკავშირებით; მათ ხშირად

აერთიანებენ **მონაცემთა ბაზების სერვერებთან**. მნიშვნელოვანია, რომ გამოყენებებისა და მონაცემთა ბაზების სერვერებთან ერთად შეიძლება იმუშაოს მომხმარებელთა დიდმა რიცხვმა, ამასთან კლიენტური მოთხოვნების შესრულება სპეციალიზირებულ მრავალპროცესორიან სერვერზე ხორციელდება გაცილებით სწრაფად, ვიდრე მომხმარებელთა კომპიუტერებზე.

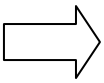
დაშორებული შეღწევის სერვერები და VPN სერვერები (Virtual Private Network – "ვირტუალური კერძო ქსელი") უზრუნველყოფენ ლოკალურ ქსელთან მოდემით ან ინტერნეტით დაშორებულ მიერთებას. ეს საშუალებას აძლევს მომხმარებელს იმუშაოს საწარმოს, ოფისის ან სასწავლო დაწესებულების ლოკალური ქსელის რესურსებთან სახლიდან ან ნებისმიერი ინტერნეტთან მიერთებული ადგილიდან, მაგალითად ინტერნეტ-კაფედან.

ტერმინალური სერვერები იძლევიან სხვა სერვერებთან მუშაობის საშუალებას სპეციალური პროგრამების - *ტერმინალური კლიენტების* მეშვეობით. ამ პროგრამების დახმარებით ადმინისტრატორები თითქოს იმყოფებიან სერვერის მოწყობილობაში და შეუძლიათ მართონ ის სრულად ლოკალური ქსელისაგან შორს, ხოლო მომხმარებლებს შეუძლიათ დაშორებულად იმუშაონ სერვერზე არსებულ გამოყენებებთან.

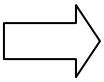
ქსელთაშორისი ეკრანები (Windows Firewall, Брандмауер Windows) გამოიყენებიან ინტერნეტთან მიერთებისას შიგა ქსელის ბოროტი ქმედებებისაგან ან თავდასხმისგან დასაცავად. **პროქსი-სერვერები (შუამავალი სერვერები)** ასრულებენ მომხმარებლების ინტერნეტში შეღწევის კონტროლის და ხშირად მოთხოვნადი ვებ-გვერდების ქეშირების ფუნქციებს (რაც საშუალებას მოგვცემს შევამციროთ ინტერნეტით სარგებლობის ხარჯები). ორივე სერვერი განკუთვნილია ინტერნეტთან ლოკალური ქსელს დამაკავშირებელ კომპიუტერზე დასაყენებლად. მათ ხშირად აერთიანებენ ერთ პროგრამულ-აპარატურულ სისტემად.

ელექტრონული ფოსტის სერვერები (საფოსტო სერვერები, mail-სერვერები), ემსახურებიან მომხმარებლების საფოსტო ყუთებს მოცემულ ორგანიზაციაში, უზრუნველყოფენ მათთან *საფოსტო კლიენტების* მიერთებას, ამუშავებენ ყველა შემავალ და გამომავალ შეტყობინებებს. ისინი შეიძლება გამოვიყენოთ

აგრეთვე სამისამართო წიგნების, საერთო საქაღალდეებისა და ელექტრონული დოკუმენტბრუნვის სისტემების შემოღებისათვის.



ვებ- და FTP-სერვერები აძლევენ შეღწევას გარე მომხმარებლებს (და ხშირად - შიგასაც) მოცემულ ქსელში განთავსებულ ვებ- და FTP-რესურსებისადმი.



დომენის მაკონტროლებლები უზრუნველყოფენ Microsoft ქსელებში *აქტიური კატალოგის* (Active Directory) სამსახურის მუშაობას და მხარს უჭერენ *დომენში* რეგისტრირებულ ყველა მომხმარებლის, კომპიუტერის, ჯგუფისა და რესურსის მონაცემების ბაზებს. მონაცემთა ასეთი ბაზის არსებობა საშუალებას აძლევს ადმინისტრატორს ცენტრალიზებულად მართოს ქსელური ობიექტები და რესურსები. მომხმარებლები კი ღებულობენ ქსელში შესვლის საშუალებას დომენის კუთვნილი ნებისმიერი კომპიუტერიდან და შემდეგ "გამჭვირვალედ" (სახელისა და პაროლის შეყვანის გარეშე) მიუერთდებიან სხვა კომპიუტერებს და იმუშავებენ მათი რესურსებით.

არსებობენ სხვა ტიპის სერვერებიც, მაგრამ ზემოთჩამოთვლილი ნაირსახეობა (ჩამონათვალი შორსაა სისრულესაგან) შეიძლება ვნახოთ პრაქტიკულად ნებისმიერ კორპორატიულ ქსელში.

უსაფრთხოების საფუძვლები ქსელებში მუშაობისას

იმ დროს, როცა კომპიუტერები არ იყვნენ გაერთიანებული ქსელებში ან მიერთებული ინტერნეტთან, მონაცემთა დაცულობა შეგვეძლო დიდად საზრუნავი არ იყო. საკმარისად ითვლებოდა კომპიუტერის *ფიზიკური დაცვის* უზრუნველყოფა და უცხო მომხმარებლების შეღწევის კონტროლი ჩამწერ მოწყობილობებთან (მაგალითად, დისკმიმღებებთან).

კომპიუტერების ქსელში გაერთიანების შემდეგ ყველაფერი შეიცვალა - სერიოზული დაცვის გარეშე ყოფნა შეუძლებელი გახდა. ოპერაციული სისტემაც, და კომპიუტერზე შენახული ან ქსელით გადაცემადი მონაცემები დაცვის გარეშე შეიძლება გახდეს ბოროტმოქმედთა იოლი ნადავლი, თანაც ისე, რომ მომხმარებლები ვერაფერს გაიგებენ. ამიტომ შემდგომ ჩვენ შევისწავლით დაცვის ძირითად პრინციპებს, რომლებიც

გამოიყენება თანამედროვე ქსელურ ოპერაციულ სისტემებში, ვიმსჯელებთ ძირითადი „მუქარების“ შესახებ, რომლებიც წარმოადგენენ საფრთხეს კომპიუტერისათვის, მომხმარებლისათვის და მათი მონაცემებისათვის. აგრეთვე მივუთითებთ უსაფრთხოების უზრუნველყოფის უმარტივეს წესებს, რომლებიც უნდა დავიცვათ ქსელში მუშაობისას.

დაცული ოს-ბის აგების პრინციპები:

- ყველა თანამედროვე ოს არის *მრავალმომხმარებლური* - ისინი გათვალისწინებულია ბევრი მომხმარებლის სისტემაში მუშაობისათვის (მათ შორის ერთდროულად);

- იმისათვის, რომ გაირჩეს ერთი მომხმარებელი მეორესგან, იყენებენ *სააღრიცხვო ჩანაწერებს* (accounts) უნიკალური *სახელებითა* და *პაროლებით*;

- სააღრიცხვო ჩანაწერები განსხვავდებიან *უფლებემოსილების დონით (პრივილეგიებით, უფლებებით)* - ქმედებების კრებულით, რომელთა შესრულება შეუძლია სისტემაში მოცემული სააღრიცხვო ჩანაწერის მფლობელს. ჩვეულებრივად სააღრიცხვო ჩანაწერებს ყოფენ *ადმინისტრაციულ* - აქვთ მაქსიმალური პრივილეგიები და *მომხმარებლურ* - უფლებამოსილების კრებული საშუალებას აძლევს ნორმალურად იმუშაონ სისტემაში. სამაგიეროდ მომხმარებელს არ რთავს ნებას შეასრულოს მონაცემების უსაფრთხოების თვალსაზრისით კრიტიკული ოპერაციები, მაგალითად, დააფორმატოს მყარი დისკოს განყოფილებები ან ცვალოს ქსელის აწყობა-გამართვები.

Windows ოს-ბის ვერსიებში, რომლებსაც ჩვენ ვიხილავთ, დამატებით არსებობენ სააღრიცხვო ჩანაწერები უფლებების დონით. არის საშუალედო ადმინისტრაციულსა და მომხმარებლურს შორის (”გამოცდილი მომხმარებელის” ჯგუფის მონაწილეები), და აგრეთვე მინიმალური უფლებამოსილების მქონე *სტუმრის სააღრიცხვო ჩანაწერები* (”სტუმრების” ჯგუფის მონაწილეები, ”Guest” ან “Гость” (სტუმარი) - ჩაშენებული სააღრიცხვო ჩანაწერის ჩათვლით).

არსებობს სააღრიცხვო ჩანაწერების კიდევ ორი ტიპი - *ლოკალური* Windows ოს-ს მქონე კონკრეტული კომპიუტერის მონაცემთა ბაზიდან, და *გლობალური სააღრიცხვო ჩანაწერები დომენში*, რომლებიც ინახება დომენის კონტროლის გამწევებზე (მათზე უფრო დაწვრილებით იქნება ნათქვამი შემდგომში);

- კომპიუტერში შესვლისათვის აუცილებლად უნდა მივუთითოთ სააღრიცხვო ჩანაწერის სახელი და პაროლი, რომელიც რეგისტრირებულია მოცემულ სისტემაში. ხაზი უნდა გაესვას იმას, რომ "სისტემაში შესვლა" გულისხმობს არა მარტო უშუალოდ შეღწევას, არამედ კომპიუტერთან მუშაობის სხვა შესაძლებლობებსაც, მაგალითად *ქსელურ* ან *ტერმინალურ* შესვლას, რომელთათვის აგრეთვე საჭიროა მომხმარებლური სახელი და პაროლი.

!

Windows ოპერაციულ სისტემებში დაშვებულია აგრეთვე ქსელური შესვლა სახელისა და პაროლის მითითების გარეშე (*ანონიმური* შესვლა); ასეთი მიერთებები გამოიყენება Microsoft ქსელებში ზოგიერთი სახის ურთიერთქმედებისას;

- სისტემაში შესვლის შემდეგ (ინტერაქტიური, ქსელური და ა. შ.) მომხმარებელს ეძლევა საშუალება ხელმისაწვდომი გახდეს მისთვის იმ კომპიუტერის რესურსები, რომელშიც შევიდა (მაგალითად, ხელმისაწვდომობა ლოკალურ ფაილებთან ან კატალოგებთან). ამასთანავე ხელმისაწვდომობის დონე განისაზღვრება *ნებადართულობების სიით*, ე. ი. მოცემული მომხმარებლის მიერ განხორციელებული შესაძლო ქმედებები დაცული ობიექტით. მაგალითად, ერთ მომხმარებელს შეუძლია შეცვალოს ან წაშალოს ფაილი, მეორეს - მხოლოდ წაიკითხოს ის, მესამეს კი საერთოდ უარი ეთქვას ამ ფაილთან დაშვებაზე.

მუშა ჯგუფები და დომენები

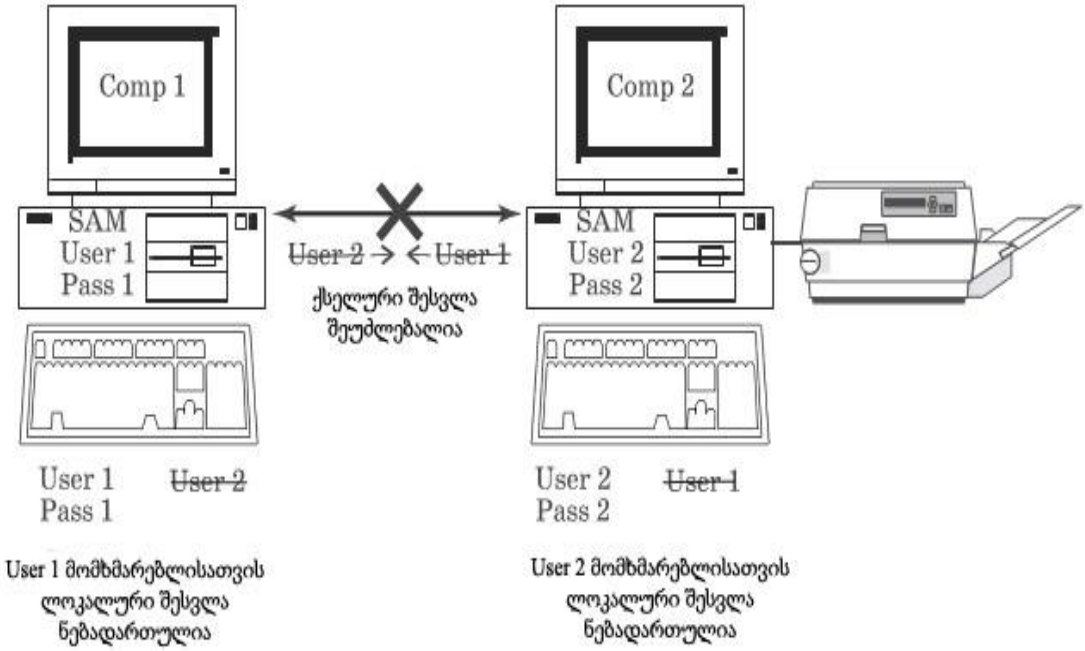
ჩვენ უკვე არაერთხელ ვახსენეთ *მუშა ჯგუფები* და *დომენები*. მოდით გავარკვიოთ, პრინციპულად რით განსხვავდებიან

ერთმანეთისაგან Microsoft ქსელებში ქსელური ურთიერთქმედების ეს ორი მოდელი.

მუშა ჯგუფი - საერთო სახელით გაერთიანებული კომპიუტერების ლოგიკური დაჯგუფება ერთი ქსელის ფარგლებში ნავიგაციის გასაადვილებლად. მუშა ჯგუფში ყოველი კომპიუტერი თანასწოუფლებიანია (ე. ი. ქსელი გამოდის ერთრანგიანი) (!) და *მხარს უჭერს მომხმარებლების სააღრიცხვო ჩანაწერების მონაცემთა საკუთარ ლოკალურ ბაზას* (*Security Accounts Manager, SAM*).

აქედან გამომდინარეობს ძირითადი პრობლემა - მუშა ჯგუფების გამოყენების შეუძლებლობა მსხვილ კორპორატიულ ქსელებში. მართლაც, თუ გავიხსენებთ, რომ დაცულ სისტემაში შესვლა სავალდებულოა, ხოლო უშუალო და ქსელური შესვლა პრინციპულად განსხვავდება ერთმანეთისაგან (უშუალო შესვლა კონტროლირდება ლოკალური კომპიუტერით, ხოლო ქსელური - დაშორებულით), მაშინ, მაგალითად, მომხმარებელს, რომელიც შევიდა Comp1 კომპიუტერში ლოკალური სააღრიცხვო ჩანაწერით User1, უარი ეთქმის დაშვებაზე Comp2 კომპიუტერის პრინტერთან, რადგან მის ლოკალურ ბაზაში არ არის ჩანაწერი User1 (ნახ. 9.1). ამგვარად, მუშა ჯგუფის "გამჭვირვალე" ურთიერთქმედებისათვის უნდა *შეიქმნას ერთნაირი სააღრიცხვო ჩანაწერები ყველა კომპიუტერზე ერთნაირი პაროლებით*, სადაც მუშაობენ მომხმარებლები და განთავსებულია რესურსები.

Windows XP Professional ოს-ში მუშა ჯგუფებისათვის გათვალისწინებულია სპეციალური რეჟიმი: "გამოიყენეთ ფაილებთან მარტივი საერთო დაშვება", რომელიც საშუალებას იძლევა თავი ავარიდოთ აღნიშნულ პრობლემას (მოცემული რეჟიმი ჩართულია დუმილით). ამ შემთხვევაში ქსელის ნებისმიერ კომპიუტერთან მიერთება ხორციელდება მისი ლოკალური, „სტუმრისეული" სააღრიცხვო ჩანაწერის სახელით, რომელიც ჩაირთვება *ქსელის აწყობა-გამართვის ოსტატის დახმარებით* (გათიშულია დუმილით) და რომლისათვის იწყობა ხელმისაწვდომობის საჭირო დონე.



ნახ. 9.1. სისტემაში ლოკალური და ქსელური შესვლა მუშა ჯგუფის ჩარჩოებში

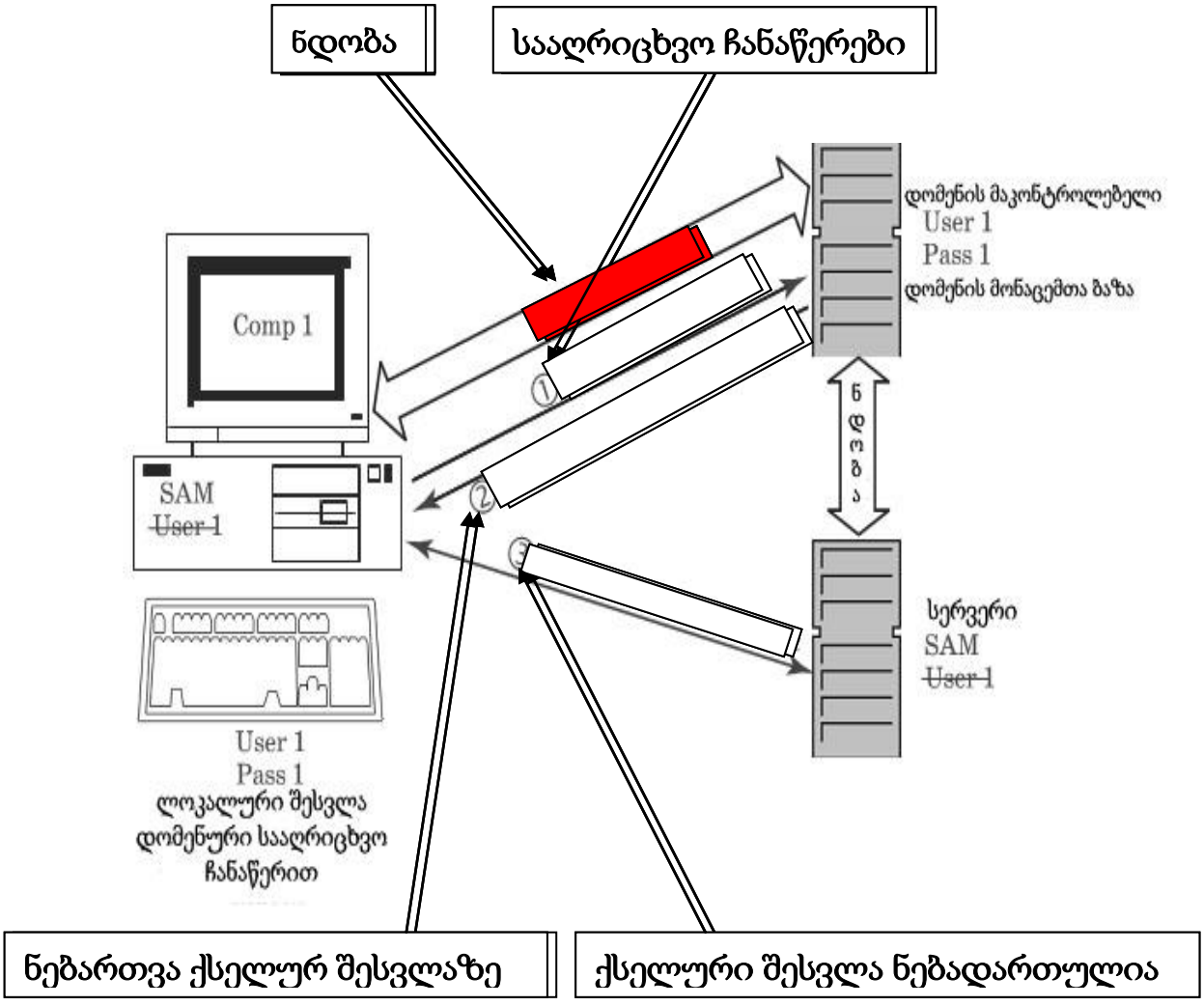
ოს Windows XP Home Edition-სათვის ქსელური ურთიერთქმედების ეს ხერხი არის ძირითადი და მისი გათიშვა არ შეიძლება (ამიტომ შეუძლებელია დომენის წევრად გავხადოთ მოცემული ოს-ს მქონე კომპიუტერები).

გასაგებია, რომ მუშა ჯგუფში სააღრიცხვო ჩანაწერებისა და რესურსების მართვა შეძლება მხოლოდ კომპიუტერებისა და მომხმარებლების მცირე რაოდენობის შემთხვევაში. მსხვილ ქსელებში უნდა გამოვიყენით დომენები.

დომენი - კომპიუტერების ლოგიკური დაჯგუფება, რომელიც გაერთიანებულია *მომხმარებლებისა და კომპიუტერების საერთო მონაცემთა ბაზით, უსაფრთხოების პოლიტიკითა და მართვით.*

დომენები იქმნება Windows ქსელური ოს-ის საფუძველზე, ხოლო მონაცემთა ბაზა, როგორც უკვე ვთქვით, მხარდაჭე–

რილია *დომენების მაკონტროლებლებით.* დომენებში მნიშვნელოვანია ის, რომ აქ ყველა კომპიუტერი თვითონ არ ახორციელებს შემოსასვლელზე მომხმარებლების შემოწმებას. ეს პროცედურა მინდობილი აქვთ მაკონტროლებლებს (ნახ. 9.2). შეღწევის ასეთი ორგანიზება იძლევა მომხმარებლის იოლი შემოწმების საშუალებას ქსელის შესასვლელზე, ხოლო შემდეგ, უკვე შემოწმების გარეშე, მიეცემა დაშვება დომენის ყველა კომპიუტერის რესურსებთან.



ძირითადი საფრთხეები ქსელში მუშაობისას

”ტროანულმა” პროგრამებმა თავისი სახელწოდება მიიღეს ეშმაკი ოდისევსის მიერ ტროას ხელში ჩასაგდებად მოგონილი სახელგანთქმული ”ტროას ცხენის“ პატივსაცემად. ტიპიური ”ტროანული” პროგრამა ”ინიღბება” რომელიმე სასარგებლო უტილიტის ქვეშ (ან შეიძლება იყოს დამალული რომელიმე პროგრამაში), თუ მომხმარებელი გამოიყენბს მას დანიშნულებისამებრ, ასეთი პროგრამა იწყებს კომპიუტერის კონტროლირებას, აძლევს რა ”ტროანული“ პროგრამის შემქმნელს მონაცემებისადმი შეღწევის საშუალებას (ე. წ. ”backdoor”-ს - უკანა შესასვლელს), რომელიც მიიტაცებს და გადაუგზავნის მას კლავიატურით აკრეფილ პაროლებსა და მსგავსებს.

კომპიუტერის ქსელთან მიერთებისას მომხმერებლისათვის შექმნილი საფრთხეები საკმაოდ ბევრია. მოვიყვანთ მხოლოდ რამდენიმე მათგანს:

- *კომპიუტერის ”შეტევა”* ჩვეულებრივად ხორციელდება ოპერაციულ სისტემაზე კონტროლის ხელში ჩასაგდებად და მონაცემებში შესაღწევად;
- *სისტემის დაზიანების* ორგანიზება უფრო ხშირად ხდება იმისათვის, რომ დაირღვეს რაიმე სახის სერვისების ან კომპიუტერების (ხშირად სერვერის) ქმედითუნარიანობა მთლიანად (გამოიწვიოს მომსახურების გაჩერება - ”Denial of Service”), ხოლო ზოგჯერ - ორგანიზაციის მთელი ინფრასტრუქტურისაც;
- *მონაცემების მოპარვა* დაშვების უფლებების არასწორად დაყენების გამო, მონაცემების გადაცემის ან სისტემის ”შეტეხვის” დროს საშუალებას აძლევს ბოროტმოქმედს მიიღოს დაშვება დაცული, ხშირად - კონფიდენციალური ინფორმაციისადმი აქედან გამომდინარე ყველა უსიამოვნებებით;
- *მონაცემების განადგურება* მიზნად ისახავს სისტემის, კომპიტერების, სერვერების ან მთელი ორგანიზაციის მუშაობის დარღვევას ან პარალიზებას.

კომპიუტერებზე ან სერვერებზე შეტევები, ვირუსები, ”ჭიები”, ჯაშუშური ან ”ტროანული” პროგრამები - *პროგრამული უზრუნველყოფა* (*პუ)* იწერება იმისათვის, რომ ბოროტ მზრახველებმა ამა თუ იმ ხარისხით განახორციელონ ზემოთჩამოთვლილი მუქარები.

ქსელში მუშაობისას უსაფრთხოების ძირითადი ზომები საკმარისად მარტივია. მათი ფორმულირება შეიძლება შემდეგი წესების კრებულის სახით:

- გათიშეთ კომპიუტერი თუ მას არ იყენებთ. როგორც ამბობენ ხოლმე უსაფრთხოების დარგში ექსპერტები - ”ყველაზე დაცულია კომპიუტერი, რომელიც გათიშულია და ინახება საბანკო სეიფში”;

- დროულად განაახლეთ ოპერაციული სისტემა. პერიოდულად, ნებისმიერ ოს-ში აღმოჩნდება ხოლმე ე. წ. ”სუსტი ადგილები”, რომლებიც ამცირებენ თქვენი კომპიუტერის დაცულობას. სუსტი ადგილების არსებობას ყურადღებით ადევნეთ თვალყური (მათ შორის ”კომპიუტერული” პრესის ან ინტერნეტში ინფორმაციის წაკითხვით), იმისათვის, რომ დროულად მიიღოთ ზომები.

!

თუ მივმართავთ კორპორაცია Microsoft-ის Windows ოს-სათვის შექმნილ სპეციალურ Windows Update ვებ-კვანძს (მაგალითად WUPDMGR.EXE პროგრამის დახმარებით ან ბრძანებით **Windows Update** *”START” (“ПУСК”)* მენიუში), არ იქნება ძნელი თქვენი კომპიუტერისათვის საჭირო *განახლებების* ჩამოტვირთვა;

- ისარგებლეთ კარგად შემოწმებული გამოყენებების შეზღუდული კრებულით, ნუ დააყენებთ თქვენს კომპიუტერზე პროგრამებს შეუმოწმებელი წყაროებიდან (განსაკუთრებით ინტერნეტიდან) და არ მისცეთ ამის უფლება სხვებს. თუ გამოყენება აღარ გჭირდებათ, წაშალეთ ის;

- საჭიროების გარეშე ნუ გასცემთ თქვენი კომპიუტერის მონაცემებს საერთო სარგებლობაში. მაგრამ თუ მაინც საჭირო გახდა, აუცილებლად ააწყვეთ რესურსებისადმი მინიმალურად საჭირო ხელმისაწვდომობის დონე მხოლოდ რეგისტრირებული სააღრიცხვო ჩანაწერებისათვის;

- დააყენეთ (ან ჩართეთ) კომპიუტერზე *პერსონალური ქსელთაშორისი ეკრანი (ბრანდმაუერი).* თუ საუბარია კორპორატიულ ქსელებზე, დააყენეთ ბრანდმაუერები როგორც თქვენი ლოკალური ქსელის ინტერნეტთან მიერთების მარშრუტიზატორებზე, ასევე ქსელის ყველა კომპიუტერზე;

- აუცილებლად დააყენეთ კომპიუტერზე სპეციალური ანტივირუსული და ”ანტიჯაშუშური” პროგრამული უზრუნველყოფა. ააწყვეთ ის განახლებების ავტომატურ მიღებაზე სულ მცირე კვირაში ერთხელ (უკეთესია - ყოველდღიურად ან რამოდენიმეჯერ დღეში);

- კომპიუტერის ერთადერთ მფლობელსაც ჩვეულებრივი მუშაობისათვის სჭირდება *მომხმარებლური სააღრიცხვო ჩანაწერი*: ამ შემთხვევაში სისტემის დაზიანება, მაგალითად, ვირუსით, იქნება გაცილებით ნაკლები, ვიდრე ადმინისტრატორის უფლებებით მუშაობისას. ყველა სააღრიცხვო ჩანაწერისათვის, განსაკუთრებით ადმინისტრაციულებისთვის, დააყენეთ და დაიმახსოვრეთ რთული პაროლი.

i

!

რთულად ითვლება პაროლი, რომელიც შეიცავს ასოების, ციფრების და სპეციალური სიმბოლოების შემთხვევით კომბინაციას, მაგალითად, jxg1rgSN. პაროლი უნდა ემთხვეოდეს თქვენი სააღრიცხვო ჩანაწერის სახელს. Windows ოპერაციულ სისტემებში რთული პაროლის *გენერირება* შეიძლება ავტომატურად, თუ გამოვიყენებთ ბრძანებას NET USER გასაღებით/RANDOM, მაგალითად:

NET USER მომხმარებლის სახელი/RANDOM

პაროლი შემთხვევითი თანმიმდებრობით ძნელი დასამახსოვრებელია, ამიტომ ხშირად იყენებენ ასეთ ხერხს - პაროლი იკრიფება რუსული ასოებით, მაგრამ ინგლისური გაშლით. მაგალითად სიტყვა "პაროლ"-ს ექნება სახე "gfhjk". ამ ხერხს უნდა სიფრთხილით მიდგომა - ბოროტმზრახველებს დიდი ხანია აქვთ ამგვარად გარდაქმნილი სიტყვების მთელი ლექსიკონები, ასე რომ სასურველია პაროლებში სპეციალური სიმბოლოებისა და ციფრების ჩასმა.

სხვადასხვა სისტემებში შესასვლელად პაროლები უნდა იყოს განსხვავებული. დაუშვებელია ერთიდაიგივე პაროლის გამოყენება თქვენი კომპიუტერის ადმინისტრირებისა და შესვლისათვის, მაგალითად, სათამაშო ვებ-საიტზე;

- ელექტრონულ ფოსტასთან მუშაობისას უცებ არასოდეს გახსნათ უცნობი გამომგზავნებისგან მიღებული მიმაგრებები. შეინახეთ მიმაგრება დისკოზე, შეამოწმეთ ანტივირუსული პროგრამით და ამის შემდეგ გახსენით. თუ არის შესაძლებლობა, ჩართეთ თქვენს საფოსტო პროგრამაზე პოტენციურად საშიში შიგთავსისაგან დაცვა და გამორთეთ HTML-ის მხარდაჭერა;

- ვებ-საიტებთან მუშაობისას დაიცავით სიფრთხილის გონივრული ზომები: შეეცადეთ თავი აარიდოთ რეგისტრაციებს, არავის გადასცეთ თქვენი პერსონალური მონაცემები. ყურადღებით იმუშავეთ ინტერნეტ-მაღაზიებთან და სხვა სამსახურებთან, სადაც გამოიყე–

"ფიშინგი" ("თევზჭერა") - ასე ჰქვია დღეს ინტერნეტში გავრცელებული თაღლითობის სახეობას. ბოროტმზრახველები ქმნიან საიტებს, რომლებიც გარეგნულად ჰგვანან ინტერნეტ-მაღაზიების, ბანკების და სხვა დაწესებულებების საიტებს, ხოლო შემდგომ "იტყუებენ" მათზე დამთვალიერებლებსა (მაგალითად, სარეკლამო ბანერების დახმარებით) და გვთხოვენ "დავადასტუროთ" ჩვენი პერსონალური მონაცემები. ზოგჯერ ასეთივე მიზნებით ბოროტმზრახველები ახდენენ ელექტრონული წერილების დაგზავნას და საფოსტო სერვერის სახელით ითხოვენ "საფოსტო ყუთთან დაშვების პაროლის დადასტურებას".

ნება ონლაინ-გადახდის ხერხები საკრედიტო ბარათების ან WebMoney და ა. შ. ტიპის სისტემების დახმარებით. გადახდის ჩატარებისას დარწმუნდით, რომ შეერთება დაცულია Secure Sockets Layer (SSL) დაშიფრვის ტექნოლოგიით. ამ შემთხვევაში სამისამართო სტრიქონი აუცილებლად უნდა იწყებოდეს "https://„-თ;

- დაცვის ზემოთმოყვანილი ზომები მხოლოდ ამაღლებენ სისტემისა და მონაცემების საერთო დაცულობას, მაგრამ არ იძლევიან არავითარ გარანტიას მათი დაზიანების ან სრული დაკარგვის. ამიტომ აუცილებელია მოსახსნელ დისკოზე ან DVD-RW-ზე შეიქმნას სისტემისა და მონაცემების *სარეზერვო ასლები* - ეს საშუალებას მოგცემთ ადვილად აღადგინოთ ისინი დაკარგვისას. ასევე კარგი იქნება ერთი ეგზემპლარის შენახვა „სახლის" გარეთ, მაგალითად, სეიფში;

- განსაკუთრებით მნიშვნელოვანია ქსელებში უსაფრთხო მუშაობის საფუძვლების შესწავლა - როგორც საშინაო, ასევე კორპორატიულ ქსელებში - ერთი მომხმარებლის მიერ წესების დარღვევა საფრთხის წინაშე აყენებს დაცვის მთელ სისტემას.

ამგვარად, ქსელში მუშაობისათვის საჭიროა ოპერაციული სისტემები, რომელთა დაყოფა მიღებულია კლიენტურად და სერვერულად. კლიენტური ოს გამოირჩევა მომსახურებების მცირე კრებულით, მაგრამ თავისთავში შეიცავს ქსელური გამოყენებების სპექტრს. სერვერული სისტემები სხვადასხვა ტიპისაა და განკუთვნილია ქსელური კლიენტების ამა თუ იმ მოთხოვნების მომსახურებისათვის.

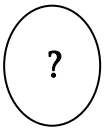
Microsoft ქსელებში მუშაობის ორგანიზებისათვის სარგებლობენ ორი მოდელით: მუშა ჯგუფები, რომლებიც გამოიყენებიან მცირე რაოდენობის კომპიუტერების შემთხვევაში, და დომენები, რომლებიც იძლევიან დიდი რაოდენობის მომხმარებლების, მუშა სადგურებისა და სერვერების ადვილად გაერთიანების საშუალებას.

ყველა ქსელური ოპერაციული სისტემა და კომპიუტერებში შენახული მონაცემები საიმედოდ უნდა იყოს დაცული, თანაც სასურველია, რომ გამოყენებული უსაფრთხოების სისტემა იყოს მრავალდონიანი.

i

სარეზერვო კოპირებისას სასარგებლოა მყარი დისკოს "სახეების" შესაქმნელი უტილიტების გამოყენება (ისეთების, როგორიცაა Norton Ghost). რეზერვირებული ასლი შეიძლება ავიღოთ "სისტემური" მყარი დისკოდან მასზე ყველა საჭირო პროგრამის დაყენებისა და ანტივირუსული შემოწმების შემდეგ. შევინახოთ ის სხვა მყარ დისკოზე (ქსელურზე ან მოსახსნელზე), იმისათვის რომ სისტემის დაზიანების შემთხვევაში ადვილად აღვადგინოთ მისი ქმედითუნარიანობა.

!



კითხვები და დავალებები

1. რისთვისაა საჭირო ქსელური ოპერაციული სისტემები? რით განსხვავდებიან ისინი ”არაქსელურისაგან”? როგორი ტიპის ქსელური ოპერაციული სისტემებია შესაძლებელი?
2. რით განსხვავდებიან კლიენტური და სერვერულ ოპერაციული სისტემები?
3. როგორი ქსელური სერვისებისა და სამსახურების მიწოდებაა შესაძლებელი Windows 2000-ში და XP-ში?
4. როგორი სახის შეიძლება იყოს სერვერები? როგორია მათი დანიშნულება? რით განსხვავდებიან ისინი ერთმანეთისაგან?
5. რაში მდგომარეობს ქსელში მუშაობისას უსაფრთხოების პრობლემა? რით არის ის განპირობებული?
6. როგორია დაცულ ოს-ში მომხმარებლების მუშაობის ორგანიზების პრინციპები?
7. რაში მდგომარეობს მომხმარებლის *ავტორიზაცია* (იდენტიფიკაცია)? როგორ ხორციელდება ის?
8. როგორი სახის სააღრიცხვო ჩანაწერებია შესაძლებელი? როგორი ინფორმაცია შედის სააღრიცხვო ჩანაწერში? დაშვების როგორი უფლებებით შეიძლება იყოს უზრუნველყოფილი Windows ოს-ში სააღრიცხვო ჩანაწერის მომხმარებელი?
9. რა არის მუშა ჯგუფი? რა არის დომენი? რაში მდგომარეობს მათ შორის ძირითადი განსხვავებები?
10. როგორია ძირითადი მუქარები ქსელში მუშაობისას? თქვენი აზრით, როგორია ბოროტმზრახველების ქმედებების ძირითადი მიზეზები (მოტივები)?
11. როგორია ქსელში მუშაობისას უსაფრთხოების ძირითადი წესები (ზომები)?
12. თქვენი აზრით, უსაფრთხოების როგორი დამატებითი ზომებია საჭირო, არასრულწლოვანების ქსელში მუშაობისას (კერძოდ, ინტერნეტში)? როგორ ორგანიზებას გაუკეთებდით თქვენი ბავშვის ინტერნეტთან მუშაობას საოჯახო კომპიუტერით? კომპიუტერულ კლასში?

თავი 10

ვუერთებთ ქსელს ინტერნეტს. ვიწყებთ მუშაობას ქსელში

ამ თავში თქვენ ნახავთ პასუხებს შემდეგ კითხვებზე:

- **ინტერნეტში შეღწევის როგორი ხერხებია შესაძლებელი?**
- **როგორ წყდება ინტერნეტში რეალური IP-მისამართების არყოფნის პრობლემა?**
- **რა არის ქსელური მისამართების რეტრანსლატორი?**
- **როგორ არის აგებული და როგორ მუშაობს DNS სისტემა?**
- **როგორ არის აგებული და როგორ მუშაობს მსოფლიო აბლაბუდა (WWW)?**
- **როგორ იქმნება ვებ-საიტები?**
- **როგორ ვიმუშაოთ ვებ-ბრაუზერთან?**

ახლა, როდესაც ჩვენი ქსელი მთლიანად აგებულია და დაცული, შესაძლებელია მისი ინტერნეტთან მიერთება. შეგახსენებთ, რომ ინტერნეტი - საკმარისად აგრესიული გარემოა და მისი მიერთება ლოკალურ ქსელთან უსაფრთხოების საიმედო ზომების უზრუნველყოფის გარეშე მეტია რისკზე. ჩვენ ამ თავში შევისწავლით ინტერნეტში შესვლის ძირითად ხერხებს (ფიზიკურ და საარხო დონეებზე), ვიმსჯელებთ, როგორ ხერხდება მსგავსი რამ ქსელურ დონეზე და როგორ წყდება სახელების განრჩევის საკითხები სასეანსო დონეზე. თქვენ აგრეთვე გაიგებთ ინტერნეტის რომელი სამსახურია ყველაზე პოპულარული, როგორაა ის ორგანიზებული და გამოყენებითი დონის რომელი პროგრამები გამოიყენება მასთან მუშაობისათვის.

დავიწყოთ *ინტერნეტში შესვლის ხერხის* ამორჩევით. დღეს ასეთი შემოთავაზებების რაოდენობა ძალიან დიდია.

მიერთება ფიზიკურ დონეზე

საქართველოში *ანალოგური მოდემები* დღემდე რჩება გავრცელებულ მოწყობილობებად, რომლებიც უზრუნველყოფენ საშინაო მომხმარებლის მიერთებას ინტერნეტთან. მათი პოპულარობა აიხსნება სატელეფონო არხების ხელმისაწვდომობით, როგორც მონაცემების გადაცემის გარემო და მათი სიიაფით (შედარებით იაფი შიდა მოდემი დღეს ღირს დაახლოებით 20 ლარი). მოდემების გამოყენების ნაკლოვანებებია - მონაცემების გადაცემის შედარებით დაბალი სიჩქარე (თეორიულად - არა უმეტეს 56 კბიტი/წმ, რეალურად უფრო ნაკლები) და საშინაო სატელეფონო ხაზის დაკავება ინტერნეტში მუშაობისას. კორპორაციულ გარემოში დღეს გამოიყენება იშვიათად, ძირითადად - მხოლოდ დიდი ფირმების პატარა ოფისებში.

სხვადასხვა ტიპის ციფრული მოდემები - xDSL-, ISDN- და საკაბელო მოდემები. მოყვანილი სიიდან ბოლო დროს ყველაზე დიდი პოპულარობა მოიპოვეს *ADSL-მოდემებმა (Asyimmetric Digital Subscriber Line)*. მათში მონაცემების გადაცემის სიჩქარე ინტერნეტიდან კლიენტურ

კომპიუტერზე (”ჩამოტვირთვა” - downloads) უფრო მაღალია, ვიდრე მონაცემების გადაცემა კლიენტური კომპიუტერიდან ინტერნეტში (გაგზავნა, upload), ამიტომ ისინი კარგად გამოიყენეს ინტერნეტთან მიერთებულმა საოჯახო მომხმარებლების უმრავლესობამ და პატარა ორგანიზაციებმაც. შედარებით მცირე ღირებულების ADSL-მოდემები უზრუნველყოფენ მონაცემების გადაცემის გაცილებით მეტ სიჩქარეს ანალოგურებთან შედარებით (მაგალითად, ADSL2+-ში მონაცემთა შემავალი ნაკადის სიჩქარემ შეიძლება მიაღწიოს 24 მბიტი/წმ-ს, გამომავალის კი 1 მბიტი/წმ-ში), ხოლო ფიზიკურ გარემოდ გამოიყენება იგივე სატელეფონო ხაზები (ოღონდ ეს ხაზები უნდა იყოს თანამედროვე, ამიტომ თბილისშიც კი ADSL-კავშირი არ არის ყველგან ხელმისაწვდომი). ADSL-მოდემების კოდევ ერთი არსებითი უპირატესობა ჩვეულებრივებთან შედარებით ის არის, რომ გადაცემისათვის იყენაბს უფრო მაღალ სიხშირეს სიგნალების და ხელს არ უშლის ჩვეულებრივ ტელეფონიას, რაც საკმაოდ მნიშვნელოვანია საოჯახო მომხმარებლებისათვის (ინტერნეტში მუშაობისას ტელეფონი თავისუფალია საუბრისათვის).

ISDN-მოდემები რამდენიმე წლის წინ წარმოადგენდნენ *”ბოლო მილის პრობლემის”* გადაწყვეტის ყველაზე გავრცელებულ ხერხს, ინტერნეტთან უშუალო მიერთების ორგანიზებისათვის. მაგრამ მაღალი ღირებულების გამო ის იშვიათად გამოიყენება.

კაბელური მოდემები იძლევიან ინტერნეტთან მიერთების საშუალებას საკაბელო ტელევიზიის სისტემების მეშვეობით, მაგრამ საკაბელო ქსელებით ინტერნეტ-მომსახურებების პროვაიდერების რაოდენობა ცოტაა.

ინტერნეტთან მოდემის დახმარებით მიერთებას უწოდებენ *კომუტირებადს*, როცა გამოიყენება ჩვეულებრივი სატელეფონო ხაზი, და *გამუდმებულს* - როცა მათთვის საჭიროა ე. წ. *გამოყოფილი ხაზები.* გამოყოფილი ხაზებით ხშირად სარგებლობენ ორგანიზაციები, თუმცა ასეთები ცოტა დარჩა.

ინტერნეტთან გამუდმებულ მიერთებას იყენებს ბევრი კოლექტიური საშინაო თუ მსხვილი კორპორაციული ქსელი. ასეთი მიერთება ფიზიკურად შეიძლება განხორციელდეს სხვადასხვა ხერხით, დაწყებული გამოყოფილი ხაზებით მოდემური მიერთებიდან და დამთავრებული სატელიტური ან მიწის ზედაპირული ხაზებით. ბოლო დროს ქალაქებში მსხვილი აბონენტების უმრავლესობა (საწარმოები და საშინაო ქსელები) იყენებენ ინტერნეტთან ჩვეულებრივ Ethernet-მიერთებას, სადაც გადაცემის გარემოდ გამოიყენება ოპტიკურ-ბოჭკოვანი არხები. ასეთი ხერხი, რა თქმა უნდა მეტი ჯდება, მაგრამ უზრუნველყოფს კავშირის მაქსიმალურ სიჩქარეს და

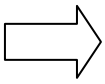
i

სიტყვა ”მოდემი” - შემოკლებული სახელწოდებაა ”**მო**დულატორი-**დემო**დულატორისა”, იგი შესანიშნავად აღწერს მოცემული მოწყობილობის ფუნქციონირების პრინციპს. სატელეფონო ხაზის ერთ მხარეს მოდემი გარდაქმნის (*ამოდულირებს*) კომპიუტერიდან მიღებულ ციფრულ სიგნალებს ანალოგურში (ბგერითი სიხშირის სიგნალებში - მოდემების ყველა მომხმარებლისათვის კარგად ცნობილი ”ხმაური”) და გადასცემს მას მოდემს ხაზის მეორე მხარეს, სადაც ხდება მისი უკუგარდაქმნა (*დემოდულაცია*).

i

საქართველოში ADSL-ტექნოლოგიით ინტერნეტში შეღწევის რეალიზაციის ცნობილი მაგალითია გაერთიანებული ტელეკომის ინტერნეტ არხი, რომელიც მიეწოდება ინტერნეტ-ოპერატორს ”Caucasus-Online”-ს მიერ.

საიმედოობას.



ბოლო დროს სულ უფრო პოპულარული ხდება ინტერნეტთან მიერთების უკაბელო ტექნოლოგიები, ისეთები, როგორიცაა GPRS, Wi-Fi, WiMAX ან LTE. მათი ძირითადი უპირატესობებია: ინტერნეტით მუშაობის საშუალება სხვადასხვა *მობილურ კომპიუტერებზე* (ნოუთბუკებზე, ჯიბის კომპიუტერებზე (ჯპკ), "სმარტფონებზე", ნეთბუკებზე, ახლახანს შემოსულ ე. წ. „დაფურ - tablet-ზე" და სხვა) კონკრეტულ სამუშაო ადგილთან "მიბმის" გარეშე. შეღწევის ასეთი ხერხი ხშირადაა რეალიზებული აეროპორტებში, რესტორნებში, კაფეებში და სხვა საზოგადოებრივ ადგილებში, სადაც ხდება *საყოველთაოდ ხელმისაწვდომი "Wi-Fi-ზონების" ორგანიზება;* მას ხშირად იწყებენ სასწავლო დაწესებულებებსა და მსხვილ ორგანიზაციებში თანამშრომლებისათვის ლოკალურ ან/და ინტერნეტში მუშაობის შესაძლებლობისათვის გადაადგილების სრული თავისუფლების შენარჩუნებით "Wi-Fi-ზონების" ტერიტორიაზე.

GPRS (General Packet Radio Service) ტექნოლოგია უზრუნველყოფს სრულყოფილ შეღწევას ინტერნეტში ფიჭური კავშირის ქსელებით. ამ დროს მობილური ტელეფონი უერთდება კომპიუტერს (ჩვეულებრივად - ნოუთბუკს ან ჯპკ-ს) კაბელით USB-პორტს (იშვიათად - COM პორტით) ან უკაბელოდ (Bluetooth-ს დახმარებით ან ინფრაწითელი კავშირით) და ფაქტიურად ასრულებს 170 კბიტი/წმ სიჩქარით მომუშავე მოდემის როლს. ფიჭური ტელეფონების თანამედროვე მოდელები და "სმარტფონები" (მოწყობილობა, რომელიც თავისთავში შეთავსებული აქვს მობილური ტელეფონის და ჯიბის კომპიუტერის ფუნქციები) იძლევიან GPRS-ით ინტერნეტთან მუშაობის საშუალებას ჩაშენებული პროგრამული უზრუნველყოფით (პროგრამებით ელექტრონული ფოსტით გაცვლისათვის, ბრაუზერებისათვის და სხვა).

Wi-Fi-ტექნოლოგია იძლევა ინტერნეტში შეღწევის საშუალებას *უკაბელო შეღწევის წერტილთან* შეერთების გზით, რომელიც მიერთებულია ინტერნეტში გასასვლელის მქონე ლოკალური ქსელის სერვერთან ან უშუალოდ საკაბელო ინტერნეტ-არხთან (მანძილი მომხმარებელსა და შეღწევის წერტილს შორის რამდენიმე ასეული მეტრია).

WiMAX და LTE ტექნოლოგიები ვითარდებიან აქტიურად. ისინი Wi-Fi-ს ანალოგიურია, მაგრამ მისგან განსხვავებით, უზრუნველყოფენ კავშირს შეღწევის წერტილებთან (*საბაზო სადგურებთან*) დიდ მანძილებზე - რამოდენიმე მილის დაშორებით და შეუძლიათ ფიჭური ტელეკომუნიკაციის მსგავსი მობილურობის უზრუნველყოფა. ამიტომ WiMAX და LTE ტექნოლოგია საკმარისად პერსპექტიული გადაწყვეტილებებია საქართველოში, განსაკუთრებით სოფლის მიდამოებისათვის,

ფიჭური ტელეფონების თანამედროვე მოდელები თავისთავში შეიცავენ ჩაშენებულ მოდემს და იძლევიან საშუალებას დავურეკოთ ნებისმიერ პროვაიდერს, იხდიან რა დამატებით შეერთების დროისთვის ფიჭური კავშირგავმულობის ჩვეულებრივი ტარიფით. ამისგან განსხვავებით *GPRS-ტექნოლოგია* გულისხმობს მხოლოდ ტრაფიკის გადასახადს - მიღებული ინფორმაციის მოცულობის, ინტერნეტში მუშაობის ხანგრძლივობის მიუხედავათ.

მათ შორის იმათთვის, რომელთაც ამჟამად არ აქვთ სატელეფონო კავშირი.

მიერთება ქსელურ დონეზე

შეგახსენებთ, რომ ინტერნეტში მუშაობისათვის ყველა კომპიუტერს უნდა ჰქონდეს *უნიკალური, საჯარო IP-მისამართი*, ამიტომ ჩვენთვის სასურველია ვიცოდეთ, როგორი ხერხებითაა უზრუნველყოფილი *ინტერნეტთან მიერთება IP-პროტოკოლის დონეზე*.

თავდაპირველად, როგორც უკვე ითქვა, ინტერნეტთან მიერთებად ყველა კომპიუტერს გამოეყოფოდა *რეალური IP-მისამართი,* ხოლო თავად შეერთება, ბუნებრივია, ხორციელდებოდა ჩვეულებრივი მარშრუტიზატორების დახმარებით. ინტერნეტთან ურთიერთქმედების ეს მეთოდი იყო ყველაზე მარტივი, ეფექტური და ამასთან უზრუნველყოფდა *ინტერნეტის ყველა კომპიუტერთან* სწრაფ დაკავშირებას. მაგრამ არსებობდა "მედლის მეორე მხარეც". ჯერ ერთი, საჭირო იყო საჯარო IP-მისამართების დიდი რაოდენობა, რასაც მივყავდით სულ უფრო მათ ზრდად დეფიციტამდე და ინტერნეტით სარგებლობისათვის საკმარისად დიდ ანგარიშებამდე (ორგანიზაციების უმრავლესობას უხდებოდა გადახდა ყველა კომპიუტერის ყოველი მისამართისათვის). რაც მთავარია - ლოკალური ქსელის ყველა კომპიუტერი ხდებოდა მთელი ინტერნეტისათვის *ხელმისაწვდომი*, ე. ი. იყო ადვილად შელახვადი. ბოლო გარემოება განსაკუთრებით თვალსაჩინო გახდა მას შემდეგ, რაც მორისის "ჭიამ" 1988 წელს მწყობრიდან გამოიყვანა მაშინდელი ინტერნეტის ყოველი მეათე (!) კომპიუტერი, რამაც ორი დღით პრაქტიკულად მთლიანად მოახდინა ქსელის მუშაობის პარალიზება.

!

რეალური IP-მისამართების მქონე ლოკალური ქსელების ინტერნეტთან მიერთებისას მარშრუტიზატორებზე დაცვის უზრუნველსაყოფად ჩვეულებრივად აწყობენ ე. წ. *IP-ფილტრებს* (ანუ *შეღწევის სიებს, IP Access Lists*), რომლებიც შიგა ქსელში პაკეტების გადაგზავნის ნებას რთავენ მხოლოდ გარკვეული პროტოკოლებით გარკვეული კომპიუტერებისათვის.

ლოკალური ქსელების დაცვისა და რეალური IP-მისამართების უკმარისობის პრობლემების გადასაწყვეტად - 90-ნი წლებიდან დაიწყო იმ დროისათვის უკვე შემუშავებული *ქსელური მისამართების ტრანსლაციის* ტექნოლოგიის ინტენსიური გამოყენება (*Network Address Translation, NAT*; იხ. 1984 წლის RFC 1631). მისი გამოყენებით პროვაიდერისგან შეიძლება მივიღოთ

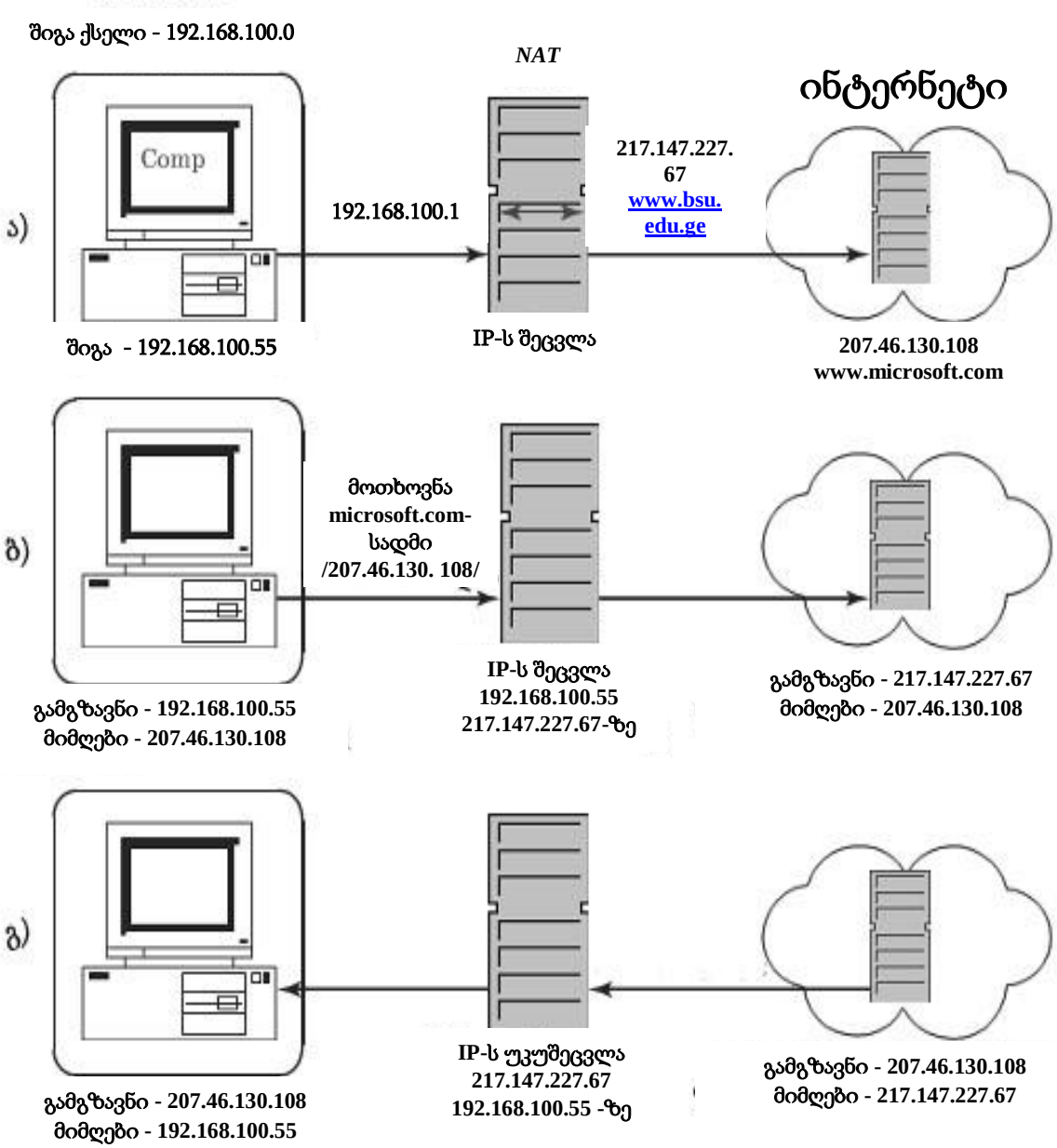
ერთადერთი საჯარო IP-მისამართი (თუმცა ჩვეულებრივად ღებულობენ რამოდენიმეს, რომ ჰქონდეთ შესაძლებლობა რეალური IP-მისამართების ქვეშ გამოაქვეყნონ შიდა საფოსტო და ვებ-სერვერები). IP-მისამართი მიენიჭება *NAT-მარშრუტიზატორის გარე ინტერფეისს* ქსელის ინტერნეტთან მისაერთებლად.

შიდა ქსელში იყენებენ IP-ქსელისათვის დაშვებულ მისამართებს (მაგალითად, 192.168.0.0 დიაპაზონიდან), ასე რომ ორგანიზაციის ქსელის ფარგლებში კომპიუტერები ურთიერთ-ქმედებენ ერთმანეთთან ჩვეულებრივ IP-თი.

მაგრამ *შიდა მისამართების გამოყენებით ინტერნეტთან უშუალო მუშაობა შეუძლებელია* (გაიხსენეთ, რომ პაკეტები IP-მისამართებით, რომლის წყარო ლოკალური ქსელის დიაპაზონიდანაა, ინტერნეტში არ მარშრუტიზირდება). ამიტომ, ინტერნეტში ყოველი პაკეტის გაგზავნისას NAT-მარშრუტიზატორმა უნდა შეცვალოს (გააკეთოს *ტრანსლირება*) წყაროს IP-მისამართი (ე. ი. შიდა კომპიუტერის მისამართი) ნებადართულ მარშრუტიზირებად საინტერნეტო IP-მისამართზე, რომელიც მისი გარე ინტერფეისის ერთ-ერთი მისამართია. პაკეტი მიდის ინტერნეტში რეალური IP-მისამართით დანიშნულებისამებრ - მაგალითად, ვებ-სერვერამდე. სერვერი კი ინტერნეტში პასუხობს შეკითხვაზე პაკეტით, რომელშიც დანიშნულების IP-მისამართად მითითებულია NAT-მარშრუტიზატორის გარე ინტერფეისის მისამართი, და ეს პაკეტიც ასევე უპრობლემოდ მიიტანება. მიიღებს რა მას, NAT-მარშრუტიზატორი ახდენს უკუგარდაქმნას - დანიშნულების IP-მისამართს (ე. ი. თავისი გარე ინტერფეისის მისამართს) პაკეტში ცვლის მოთხოვნილი შიგა კომპიუტერის მისამართით და აგზავნის პაკეტს შიდა ქსელში (ნახ. 10.1).

შედეგად შიდა და გარე კომპიუტერები "თვლიან", რომ უშუალოდ ურთიერთქმედებენ ერთმანეთთან, "ვერაფერს ხვდებიან" შუამავლის არსებობის შესახებ, რომლის როლს ასრულებს მარშრუტიზატორი NAT მხარდაჭერით.

NAT-ს გამოყენების უპირატესობებს შორის ძირითადია ის, რომ გარე კომპიუტერებმა "არაფერი იციან" შიდა IP-ადრესაციის შესახებ, და *არ შეუძლიათ მიიღონ პირდაპირი, უშუალო შეღწევა იქ მყოფ კომპიუტერებთან.* ეს მიმზიდველს ხდის NAT-ტექნოლოგიას ოკალუტი ქსელების უსაფრთხოების უზრუნ-ველყოფისათვის.



ნახ. 10.1. ქსელური მისამართების რეტრანსლატორის მუშაობა ინტერნეტთან ურთიერთქმედებისას

მაინც როგორ მუშაობს ქსელური მისამართების ტრანსლაციის ტექნოლოგიის ინტენსიური გამოყენება (NAT) სხვადასხვა ტიპის მიერთებებისათვის? მოდემების გამოყენებისას ყველაფერი საკმაოდ მარტივადაა. *პროვაიდერის* მოდემთან - ინტერნეტ მომსახურებების მომწოდებელთან (*ISP, Internet Service Provider*) კავშირის დამყარების შემდეგ, კლიენტური მოდემი ავტომატურად ღებულობს პროვაიდერის მიერ დარეგისტრირებულ *რეალურ IP-მისამართებიდან ერთ-ერთს.* (აღვნიშნავთ, რომ ზოგიერთი პროვაიდერი აძლევს კლიენტებს ლოკალური ქსელებისათვის განკუთვნილ IP-მისამართებს, და მერე იყენებს NAT-მარშრუტიზატორებს).

!

ყურადღება!

იმისათვის, რომ ასეთ სიტუაციაში დაიცვათ თქვენი კომპიუტერი "გატეხვისა" და მონაცემების დაკარგვისაგან, *აუცილებლად უნდა გამოიყენოთ პერსონალური* Firewall-ი (Брандмауэр) - უნდა ჩართოთ თქვენს ინტერნეტთან მოდემური მიერთების თვისებებში (Prorerties, Свойства).

ამასთან, თუ Windows 2000 ან XP ოს-ს მქონე კომპიუტერზე ნებას დავრთავთ მოდემური მიერთების თვისებებში *ინტერნეტთან მიერთების საერთო შეღწევას* (*Internet Connection Sharing, ICS*), მაშინ თქვენი კომპიუტერი ხდება მარშრუტიზატორიც NAT-მხარდაჭერით. ამით უზრუნველყოფთ *მთელი საშინაო ქსელის ინტერნეტთან ურთიერთქმედებას.* ამ დროს ქსელურ ინტერფეისს ენიშნება 192.168.0.1 IP-მისამართი, და თქვენს კომპიუტერზე მუშაობას იწყებენ *DHCP და DNS-პროქსი სამსახურები.* პირველი მათგანი საშინაო ქსელის ყველა სხვა კომპიუტერისათვის გასცემს ისეთ პარამეტრებს, როგორიცაა IP-მისამართი 192.168.0.0 დიაპაზონიდან, ქვექსელის ნიღაბი (255.255.255.0), რაბის მისამართი (192.168.0.1), ხოლო მეორე - ემსახურება საშინაო ქსელის DNS-კლიენტების მოთხოვნილებებს, გადაუგზავნის რა მათ DNS-პროვაიდერის სერვერს. ამასთანავე, გეძლევათ ინტერნეტიდან შიდა კომპიუტერებში შეღწევის უზრუნველყოფის შესაძლებლობა. მაგალითად, ინტერნეტში თქვენი საშინაო ვებ- ან საფოსტო სერვერის გამოსაქვეყნებლად.

მსგავსად მუშაობს თანამედროვე ჩქაროსნული მოდემების აბსოლუტური უმრავლესობა საშინაო და მცირე ორგანიზაციების ქსელებში. ისინი, როგორც წესი, არიან *ჰიბრიდული მოწყობილობები (რაგები)*, აერთიანებენ რა თავისთავში მოდემებისა და NAT-მარშრუტიზატორების ფუქციონალობებს, ხოლო ზოგიერთები გვევლინებიან უკაბელო შეღწევის წერტილებად და ბრანდმაუერებად. მსხვილი კოლექტიური საშინაო ან კორპორატიული ქსელების ინტერნეტთან მიერთებისას ძირითადად იყენებენ *მესამე დონის კომუტატორებს* ანუ *მარშრუტიზატორებს*, ხოლო შიდა ქსელების დაცვის ორგანიზებას ახორციელებენ სპეციალიზებული *სრულფუნქციონალური „ცეცხლგამძლე კედლის“ (Windows Firewall, Брандмауэр)* დახმარებით (რა თქმა უნდა, NAT მხარდაჭერით). პერსონალური ქსელთაშორისი ეკრანებისგან განსხვავებით, ასეთ Firewall-ებს შეუძლიათ განახორციელონ გადაცემადი მონაცემების კონტროლი არა მარტო IP-ფილტრების ან დაყენებული TCP-შეერთებების დონეზე, არამედ მათ შეუძლიათ HTTP, FTP ან SMTP პროტოკოლების ბრძანებების ანალიზი და მონაცემების გადაცემის ბლოკირება აკრძალული ბრძანებებისას. ასეთ Firewall-ებს ხშირად აერთიანებენ *პროქსი სერვერებთან.*

i

ფაილი HOSTS, ოღონდ გაფართოების გარეშე, დღესაც არსებობს და მუშაობს ყველა Windows ოპერაციულ სისტემებში, რომლებიც მხარს უჭერენ TCP/IP პროტოკოლს (ის შეიძლება ვნახოთ %Windir%\System32\Drivers\Etc კატალოგში).

სახელების დომენური სისტემა (DNS) ინტერნეტში

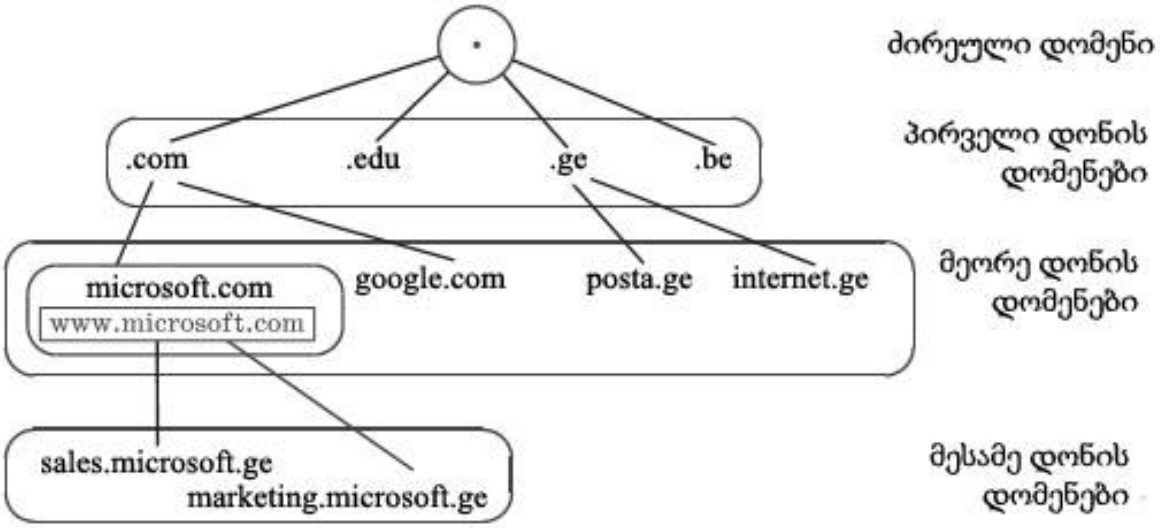
ჩვენ ვისაუბრეთ კომპიუტერების (მათ კიდევ *კვანძებსაც* უწოდებენ) ინტერნეტში ურთიერთქმედებისათვის რიცხვითი IP-მისამართების გამოყენებაზე, მაშინ როცა ადამიანებისათვის მოსახერხებელია სიტყვიერ სახელებთან მუშაობა. ქსელურ გამოყენებებში სიტყვიერი სახელებით სარგებლობისათვის საჭიროა *სახელების IP-მისამართებში გარდაქმნის მექანიზმი.*

შესაძლებელია ორი ასეთი ხერხი: შეიძლება გამოვიყენოთ ტექსტური ფაილი, რომელშიც ჩავწერთ IP-მისამართებისადმი ყველა შესაბამისობას, და შეიძლება ვისარგებლოთ სპეციალური სამსახურით - *DNS სისტემით.* თავდაპირველად, ინტერნეტში სიმცირის გამო იყენებდენ სტენფორდის უნივერსიტეტის ქსელური ცენტრის (Stanford Research Institute's Network Information Center) მიერ მხარდაჭერილ ფაილს სახელწოდებით HOSTS.TXT. მასში ცვლილებები (ფაქტობრივად - კომპიუტერების სახელების *რეგისტრაცია*) მხოლოდ ამ უნივერსიტეტში შეჰქონდათ, ხოლო შემდეგ ეს ფაილი

იტვირთებოდა ინტერნეტის ყველა დანარჩენ კვანძებზე.

80-ანი წლების დასაწყისში დაიწყო ინტერნეტში კვანძების რაოდენობის „ფეთქებადი“ ზრდა. ასეთმა სისტემამ უბრალოდ შეწყვიტა ნორმალური მუშაობა - განუწყვეტლივ ხდებოდა ფაილში ცვლილებების შეტანა, რასაც თან ახლდა ახალი კვანძების დამატება და ინტერნეტის ყველა კომპიუტერში შეცვლილი ფაილების კოპირებაზე სულ უფრო მეტი დაროის ხარჯვა.

შედეგად, უარი ითქვა ერთიან ფაილზე და მოხდა გადასვლა *დომენური სახელების განაწილებულ ბაზაზე*, რომელშიც გამოყოფილია *პასუხისმგებლობის ზონები*. ასეთმა სისტემამ მიიღო *DNS (Domain Name Sistem)* სახელწოდება. მას აქვს ხის მსგავსი აგებულება და შესაბამისადაა აგებული დომენური სახელების სტრუქტურა (ნახ. 10.2).



ნახ.10. 2. დომენური სახელების სტრუქტურის მაგალითი

!

2011 წლის 20 ივნისისათვის დომენების შექმნისა და IP-მისამართების გამანაწილებელმა ორგანიზაციამ (ICANN) მიიღო წესები, რომლის მიხედვით პირველი დონის დომენს შეიძლება ჰქონდეს ნებისმიერი სახელი, მაგრამ განაცხადის წამრდეგენმა უნდა დაასაბუთოს, რომ უფლება აქვს გამოიყენოს არჩეული სიტყვა და გადაიხადოს 200 000 აშშ დოლარი.
http://www.bbc.co.uk/russian/science/2011/06/110619_icann_domain_names.shtml

მსხვილი ფირმები, რა თქმა უნდა, მიისწრაფვიან მიიღონ "პრესტიჟული" დომენური სახელები, რომლებიც გამოსახავენ მათ სახელწოდებას ან საქმიანობის სფეროს. ამას, ზოგჯერ კურიოზამდეც კი მივყავართ: მაგალითად, სახელმწიფომ კუნძულზე - ტუვალუ, რომელიც არაფრით გამოირჩევა, მიიღო ზედა დონის საკუთარი დომენი (tv) და სავსებით შეიძლება გახდეს ტელეკომპანიებისა და სხვა "სატელევიზიო ბიზნესის" ფირმების საიტებისათვის უფრო ქვედა დონეების დომენური სახელების მთავარ "ექსპორტიორად" (საკმაოდ დიდი ყოველწლიური შემოსავლით).

მას შემდეგ, *ქსელური საინფორმაციო ცენტრი* (ის ახლა ატარებს "InterNIC" სახელს) პასუხისმგებელია მხოლოდ სისტემის "ძირზე", ე. წ. DNS root domain (მას ჩვეულებრივად აღნიშნავენ ერთი წერტილით - ".") და კვანძების სახელებში ჩვეულებრივად გამოტოვებულია), შესაბამის *ძირეულ სერვერებზე* (*Root Servers* ან *Root Hints*) და მაღალი დონის სერვერების რეგისტრაციაზე (*Top Level Domains, TLD*). მაღალი დონის დომენების სახელები ჩვეულებრივად ირჩევა ორგანიზაციების ტიპების მიხედვით, კერძოდ, აშშ-სთვის (com - კომერციისთვის, edu - განათლების, gov - სახელმწიფოებრივის და ა. შ.), ან ქვეყნების მიხედვით (ge - საქართველო, be - ბელგია და სხვა).

ქვევით განლაგდებიან *მეორე დონის დომენები*, რომლებიც რეგისტრირდებიან ზედა დონის დომენებში და მათში უკვე დასაშვებია როგორც კვანძების, ასევე *„შვილობილი" დომენების* (*SubDomain*) რეგისტრაცია. ვთქვათ ადმინისტრატორმა დაარეგისტრირა დომენი company.ge. მას *აქვს სრული უფლება საკუთარ დომენზე* - შეუძლია შექმნას შვილობილი დომენები და არეგისტრიროს კვანძები ზედა დონეების დომენების გაფრთხილების გარეშე, მაგრამ პასუხისმგებელია DNS სისტემის სწორ ფუნქციონირებაზე თავისი პასუხისმგებელობის ფარგლებში.

DNS სამსახური მუშაობს საკმაოდ ეფექტურად. DNS-ში დარეგისტრირებული ნებისმიერი კომპიუტერის მოძიებისათვის (მაგალითად, www.company.ge) საკმარისია მივმართოთ ერთ-ერთ *ძირეულ სერვერს*, რომელიც დაგვიბრუნებს ge დომენზე პასუხისმგებელ DNS-სერვერების სიას. მოთხოვნები მათ მიმართ საშუალებას მოგვცემს გავარკვიოთ company.ge დომენის მხარდამჭერ DNS-სერვერების სია, რომლთაგან შეიძლება გავარკვიოთ www.company.ge კომპიუტერის IP-მისამართი. სწორეთ ქმედების ასეთი ალგორითმი გამოიყენება DNS-სერვერების უმრავლესობისათვის *სახელების განრჩევისას.*

მსოფლიო აბლაბუდა (World Wide Web)

ახლა, როცა ჩვენი ქსელი აგებულია, დაცულია, მიერთებულია ინტერნეტთან და მომართულია კვანძების სახელებთან მუშაობისათვის, დაგვრჩენია გავიგოთ, როგორ *სამსახურებს* გვთავაზობს ინტერნეტი და როგორი პროგრამები უნდა გამოვიყენოთ ამ სამსახურებთან მუშაობისათვის.

დავიწყოთ დღეს ინტერნეტის ყველაზე პოპულარული სერვისით - *მსოფლიო აბლაბუდით*, ანუ *World Wide Web* (*WWW, W*[3]). WWW არის ერთერთი ინტერნეტში მომუშავე მრავალი სამსახურებიდან. სწორედ ამ სამსახურისათვის უერთდება ინტერნეტს მომხმარებლების აბსოლუტური უმრავლესობა (ბევრი მათგანი თვლის კიდეც, რომ "WWW" და "ინტერნეტი" ერთიდაიგივეა).

WWW-ს საფუძვლები ჩაეყარა XX საუკუნის 80-იანი წლების ბოლოს ბირთვული კვლევების ევროპულ ცენტრში (CERN), ჟენევაში. WWW სამსახური ჩაფიქრებული იყო უნივერსალურ გარემოდ, რომლის დახმარებით მეცნიერებს შეეძლებოდათ ნებისმიერი ტიპის ინფორმაციის სწრაფი ურთიერთგაცვლა; გარემო რომელშიც *მითითებებს (references)* შეეძლებოდათ *ჩვენი პლანეტის ნებისმიერ ადგილას* მყოფი *ჰიპერტექსტური ობიექტების* მითითება. შედეგად შემუშავებულ იქნა WWW სისტემა, *ვებ-გვერდების მონიშვნის ენა HTTP* (*HyperText Transfer Protocol*) და *ადრესაციის ხერხი რესურსის უნივერსალური იდენტიფიკაციის* (*URL, Uniform Resource Locator*) დახმარებით. გარდა ამისა, შეიქმნა *ვებ-გვერდების გადათვალიერების პროგრამა* (*ბრაუზერი*), პირველი *ვებ-სერვერი* და შემუშავდა *მათი ურთიერთქმედების პროტოკოლი - HTML* (*HyperText Markup Language*). 1991 წელს ეს ყველაფერი გამოქვეყნდა ინტერნეტში თავისუფალი სარგებლობისათვის.

World Wide Web შეიძლება განვმარტოთ, როგორც *ჰიპერტექსტზე* დაფუძნებული *განაწილებული საინფორმაციო სისტემა.* სიტყვა "განაწილებული" მოცემულ შემთხვევაში ნიშნავს, რომ მონაცემები ასეხული თქვენი ვებ-ბრაუზერით, შეიძლება განლაგებული იყოს როგორც მეზობელ კომპიუტერზე, ასევე სერვერზე დედამიწის მეორე ბოლოში. მაგალითად, ერთ სერვერზე განთავსებული *ვებ-გვერდის* ფარგლებში შეიძლება გამოსახული იყოს სხვა სერვერზე შენახული ნახატი, რომელისთვისაც ვებ-გვერდის ტექსტში (HTML ენაზე) მითითებულია ამ ნახატის განთავსების ზუსტი მისამართი.

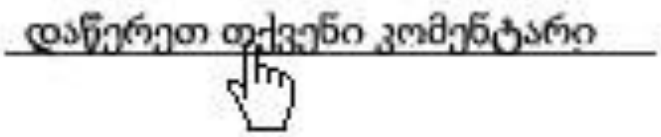
ინფორმაცია WWW-ში წარმოდგენილია ჩვეულებრივი ტექსტის ან *ჰიპერტექსტის, პრაქტიკულად ნებისმიერი მონაცემების* (გრაფიკა, მუსიკალური ან ვიდეო-რგოლები) *შემცველი* ვებ-გვერდების სახით. გარდა ამისა, ვებ-გვერდებზე

i

ინტერნეტში არსებობენ საყოველთაოდ ხელმისაწვდომი სპეციალური სერვერები ვებ-საიტების განსათავსებლად (ჰოსტინგისათვის), მაგალითად freeservers.com ან 000webhost.com. აქ (რეგისტრაციის არც თუ რთული პროცედურის ჩატარების შემდეგ) ნებისმიერ მსურველს შეუძლია განათავსოს თავისი საკუთარი საიტი.

შეიძლება იყოს *მითითებები* სხვა ვებ-გვერდების შესახებ, რომლებიც ინახებიან ამავე ან ნებისმიერ სხვა სერვერზე ინტერნეტში.

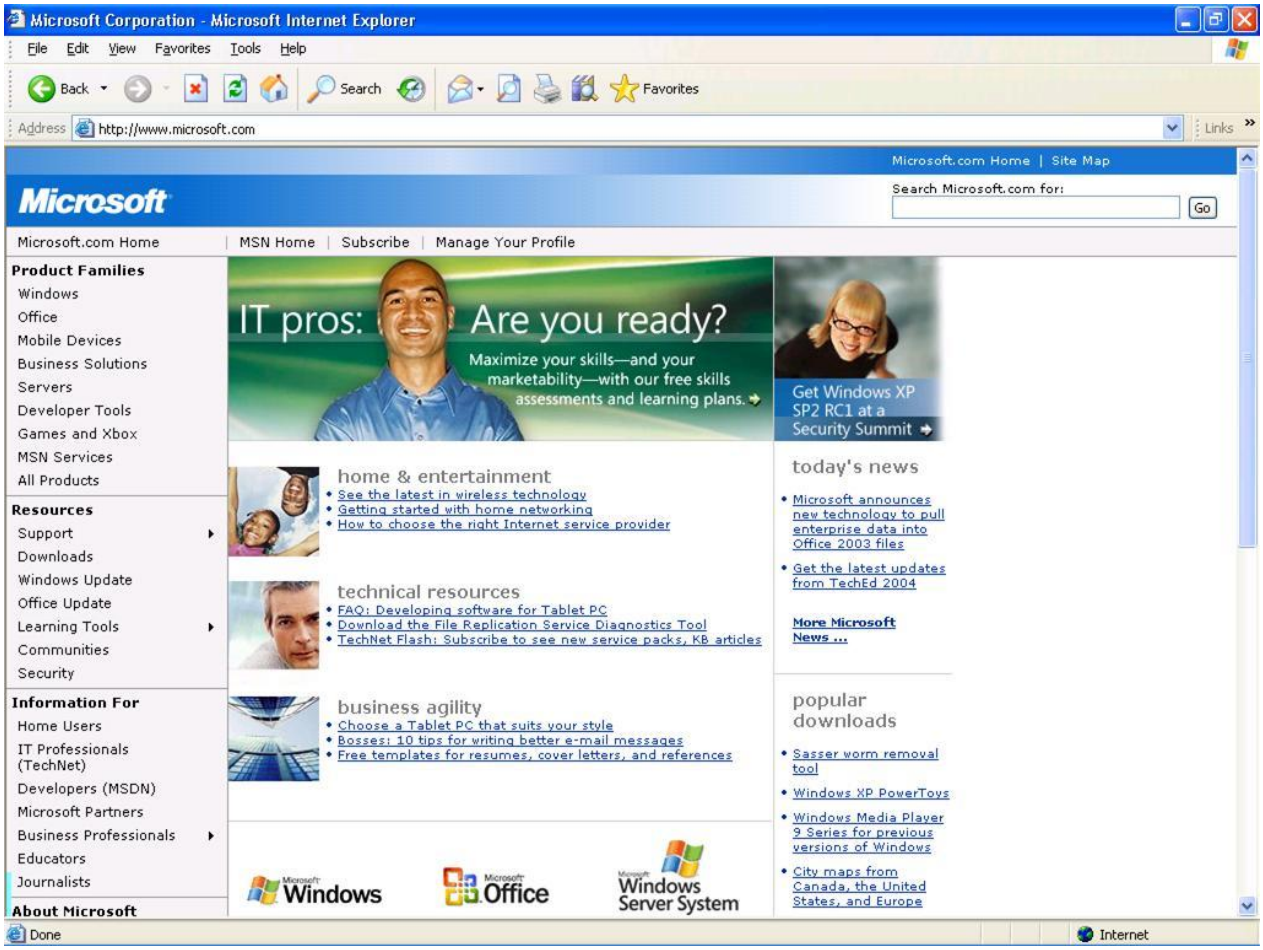
მითითებები ვებ-გვერდებზე აისახება გამოყოფილი (ჩვეულებრივად ფერით და ხაზის გასმით) ტექსტით ან გრაფიკული გამოსახულებებით (ნახ. 10.3). თუ მითითებაზე დავაყენებთ თაგვის მაჩვენებელს, იგი ისრიდან გადაიქცევა "მაჩვენებელთითიანი ხელის" გამოსახულებად. ნებისმიერი ასეთი მითითება ახორციელებს *გადასვლას* სხვა ჰიპერტექსტურ დოკუმენტზე, რომელიც შეიძლება აღმოჩნდეს არა უბრალოდ ვებ-გვერდი, არამედ, მაგალითად, შესრულებადი პროგრამა ან მულტიმედიური ფაილი; მაშინ მითითებაზე თაგვით დაწკაპუნება გახსნის ამ დოკუმენტს.



ნახ. 10.3. ტიპიური მითითება ვებ-გვერდზე

ვებ-გვერდების განთავსება WWW-ში ხდება ვებ-სერვერზე ერთმანეთთან გადაბმული კრებულების სახით, რომლებსაც *საიტებს* ეძახიან. საიტები შეიძლება ეკუთვნოდეს რომელიმე კონკრეტულ პიროვნებას ან ორგანიზაციას. მათ მხარდაჭერას ახორციელებენ შემმუშავებლები (*ვებ-ოსტატები*).

ვებ-საიტისადმი მიმართვისას ყოველთვის იხსნება *მთავარი გვერდი*, რომელსაც ხანდახან *საშინაოს* ეძახიან (*home page*). მთავარი გვერდი (ნახ. 10.4) - თითქმის იგივეა, რაც ჟურნალის ყდა ან გაზეთის პირველი გვერდი. ჩვეულებრივად, მასზე ქვეყნდება საიტის შინაარსის ამსახველი ყველაზე მიმზიდველი ინფორმაცია (ზოგჯერ - უბრალოდ სურათი ან მულტიმედიური რგოლი). მუშაობის მოხერხებულობისათვის მთავარ გვერდზე ხშირად ათავსებენ დასათაურების სვეტს, *რუკას*, ან *სანავიგაციო დაფას*, რომელიც საშუალებას აძლევს დამთვალიერებელს ადვილად მონახოს საჭირო ინფორმაცია.

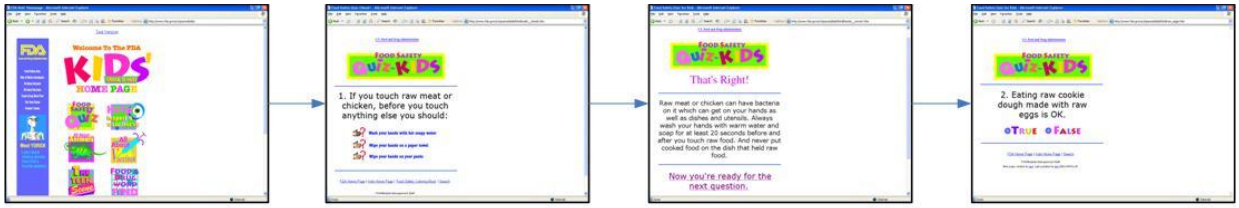


ნახ.10.4. Microsoft კორპორაციის საიტის მთავარი გვერდის მაგალითი

ვებ-საიტის გვერდების სტრუქტურირებას, ჩვეულებრივად, ახდენენ სამი ხერხიდან ერთ-ერთით: ხაზოვანით, ხის მსგავსით ან ნებისმიერით.

ხაზოვანი ვებ-საიტი (*Linear Web Site*) ჩვეულებრივი წიგნის მსგავსია: თქვენ იწყებთ პირველი (მთავარი) გვერდით, შემდეგ გადადიხართ მეორეზე, მესამეზე, მეოთხეზე და ასე შემდეგ (ნახ. 10.5). ასეთი საიტები ხელსაყრელია იმით, რომ ძნელია ”აგებნეს გზა” - თქვენ ყოველთვის შეგიძლიათ დაუბრუნდეთ არამარტო წინა გვერდს, არამედ, ნებისმიერ სხვას, თუ ეს გათვალისწინებულია საიტის შემქმნელის მიერ. ინფორმაციის

წარმოდგენის ასეთ ხერხს ხშირად იყენებენ იმისათვის, რომ მკითხველს ერთმანეთთან დაკავშირებული მასალების ან სტატიების მთელი სერია წარმოუდგინონ.

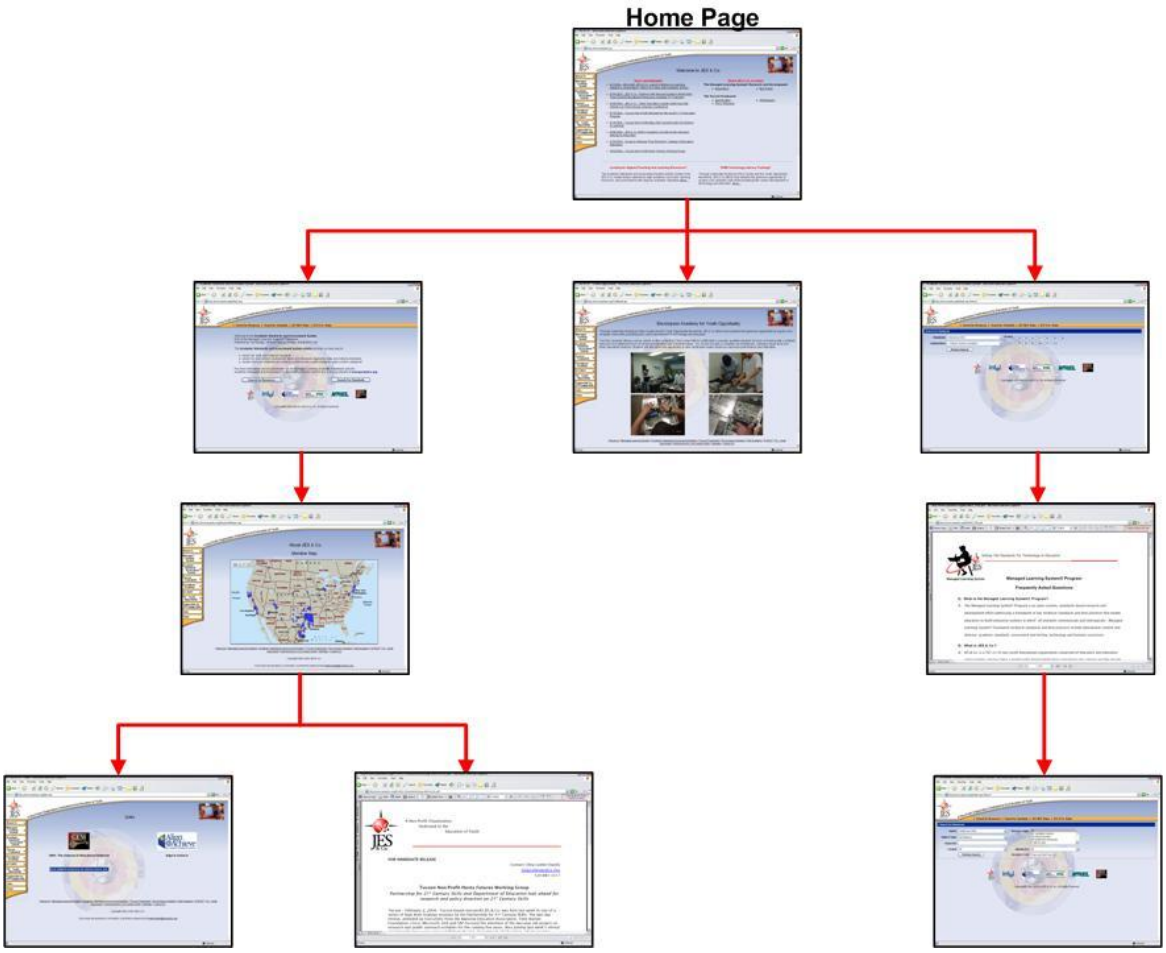


ნახ.10.5. ხაზოვანი ვებ-საიტი

ხის მსგავსი სტრუქტურის ვებ-საიტი (*Tree Web Site*) ორგანიზებულია "გენიალოგიური ხის" მსგავსად. თქვენ იწყებთ მთავარი გვერდით, ხოლო შემდეგ შეგიძლიათ აირჩიოთ საიტის რამდენიმე *განყოფილებიდან* ერთერთი (ნახ. 10.6). ასეთი სტრუქტურა დამახასიათებელია მრავალპროფილიანი ორგანიზაციების ან კომპანიებისათვის (მაგალითად, პროგრამული უზრუნველყოფის ან მოწყობილობების მწარმოებლებისათვის, რომლებსაც აქვთ სურვილი წარმოადგინონ თავისი პროდუქციის სხვადასხვა მიმართულებები), ინტერნეტ-მაღაზიებისათვის, რომლებიც ვაჭრობენ სხვადასხვა საქონელით და სხვა. საიტის ასეთი ორგანიზების ტიპიური მაგალითია კომპანია Microsoft-ს ვებ-საიტი (www.microsoft.com).

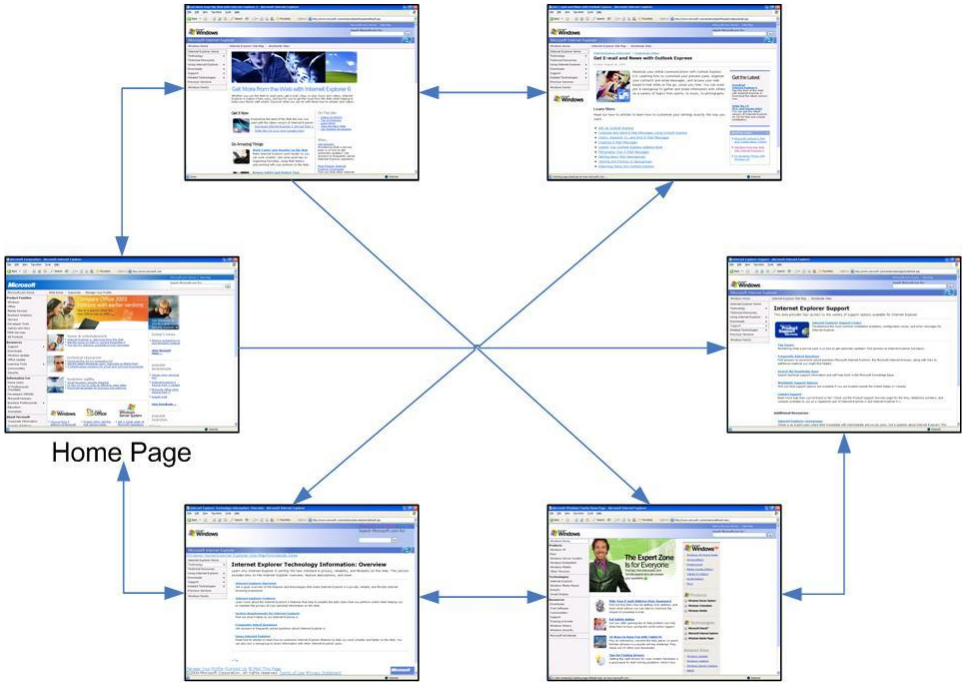
ვებ-საიტს ნებისმიერი სტრუქტურით (*Randome Web Site*) პრაქტიკულად არა აქვს მკაფიო ორგანიზება და ხშირად წარმოადგენს ერთმანეთთან ჯვარედინი მითითებებით დაკავშირებული ინფორმაციის ქაოტურ მასივს. თქვენ შეგიძლიათ გადახვიდეთ გვერდიდან გვერდზე, მაგრამ გაგიძნელდებათ ნახოთ საიტის რომელ ადგილას იმყოფებით ან მთავარ გვერდზე დაბრუნება (ნახ. 10.7). ასეთი არაპროფესიონალური სტრუქტურა დამახასიათებელია დამწყები ვებ-ოსტატებისათვის ან ორგანიზაციებისათვის, რომლებსაც არა აქვთ მკაფიო წარმოდგენა იმის შესახებ, თუ რა ინფორმაცია და როგორი სახით უნდათ განათავსონ თავიანთ ვებ-საიტზე.

დაბოლოს უნდა ვახსენოთ ე. წ. *ვებ-პორტალების* და *საძიებო სისტემების შესახებ* (ამ ფუნქციებს ხშირად აერთიანებენ). ვებ-პორტალის ტიპიური მაგალითებია



ნახ. 10.6. ხის მსგავსი სტრუქტურის ვებ-საიტი

www.caucasus.net და www.yahoo.com. პორტალის სათაო გვერდიდან ინტერნეტში ახალბედას შეუძლია გადავიდეს ცხოვრების პრაქტიკულად ყველა სფეროსადმი მიძღვნილ საიტზე, ამასთან, როგორც წესი, ეს იქნება ყველაზე მეტად დათვალიერებადი საიტები. ამ დროს მთავარია "ქსელში არ აგებნეთ გზა-კვალი", ე. ი. უნდა გახსოვდეთ, რომელი ინფორმაციის ნახვა გინდოდათ ინტერნეტში და არ მიაქციოთ ყურადღება სხვა, შესაძლოა, უფრო საინტერესოს. პორტალებზე რეალიზებულია აგრეთვე საძიებო სისტემები, რომელთა საშუალებით ვეძებთ ინფორმაციას ინტერნეტში მოთხოვნით (*საკვანძო სიტყვით* ან *ფრაზით*). სუფთა საძიებო სისტემების მაგალითებია - www.googl.ge, www.searche.msn.com, და სხვა.



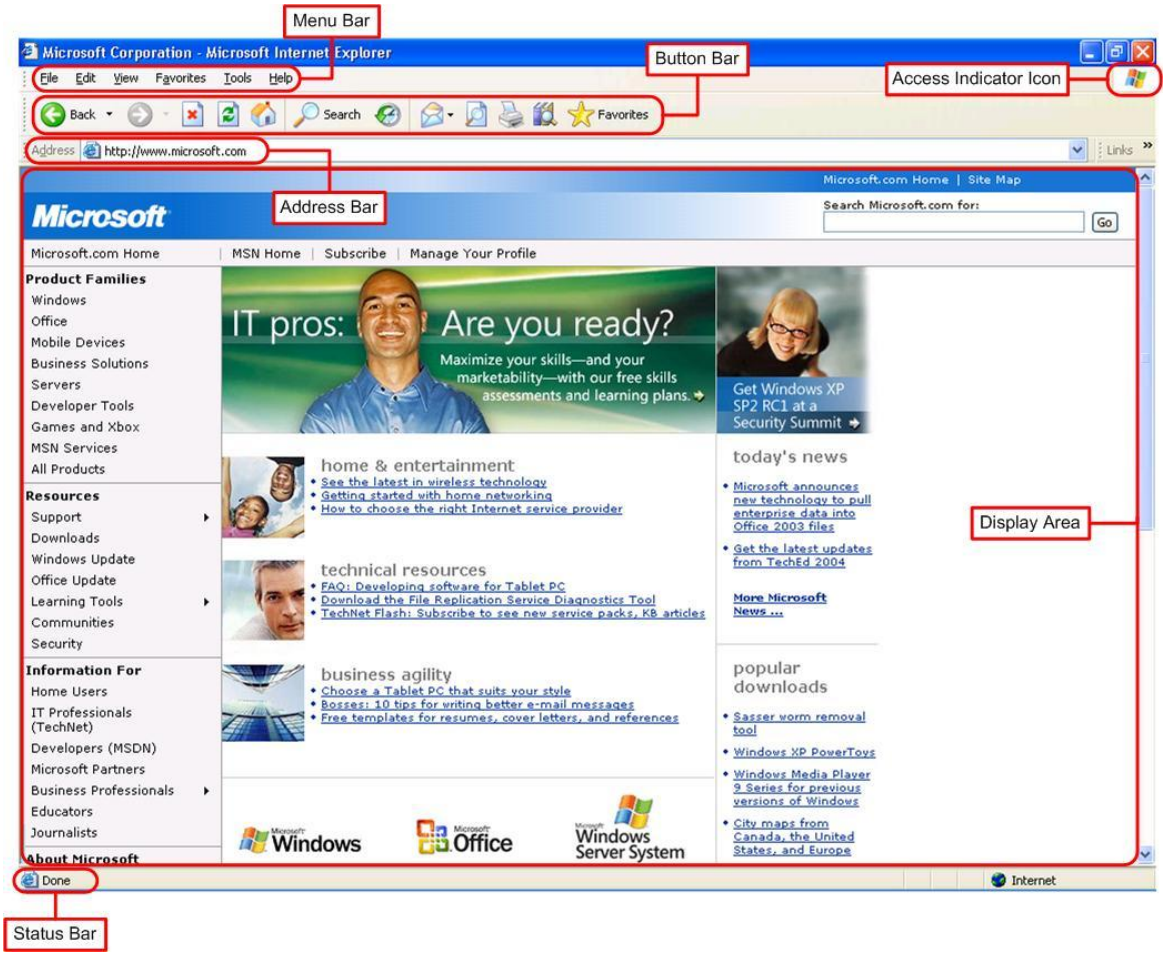
ნახ. 10.7. ვებ-საიტი ნებისმიერი სტრუქტურით

i

სკრიპტი - პატარა პროგრამაა, რომელიც ახორციელებს ამა თუ იმ ქმედებებს ვებ-გვერდზე, მაგალითად ინტერაქტიური ურთიერთქმედება მომხმარებელთან, და წარმოადგენს ტექსტს (*ლისტინგს*) პროგრამირების განსაკუთრებულ ენაზე (*JavaScript* ან *VBScript*). სკრიპტის ლისტინგის ამოღებას ვებ-გვერდის ტექსტიდან და მის აღსრულებას ახორციელებს ვებ-ბრაუზერი.

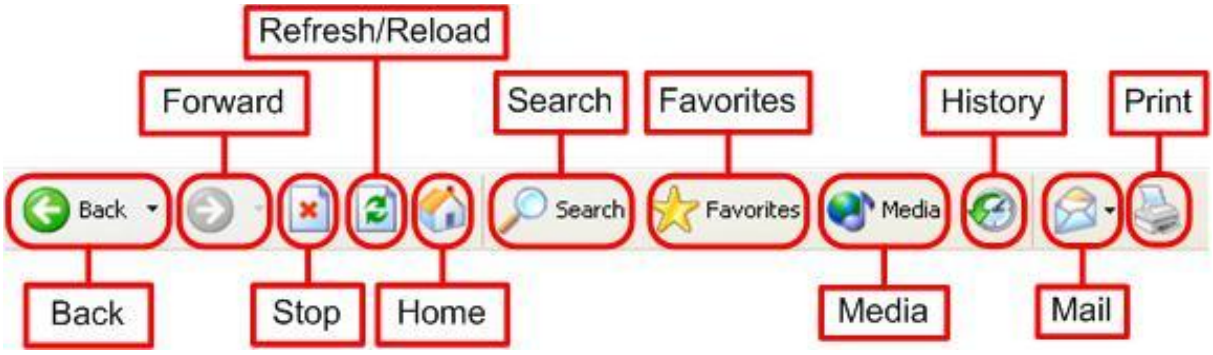
როგორც უკვე ვთქვით, ვებ-გვერდის დათვალიერება ხორციელდება სპეციალური პროგრამების - *ვებ-ბრაუზერების* დახმარებით. ბრაუზერები უზრუნველყოფენ ვებ-სერვერებთან ურთიერთქმედებას სპეციალური HTTP პროტოკოლით. მიიღებენ რა ინფომაციას HTML ფორმატში, ბრაუზერები სწორად ასახავენ მას ეკრანზე (ჩართავენ, თუ ეს არის მუსიკა ან ვიდეოფაილი, ან გაუშვებენ შესრულებაზე, თუ ეს არის პროგრამა ან *სკრიპტი*). ისინი აგრეთვე საშუალებას იძლევიან ადვილად გადავიდეთ გვერდიდან გვერდზე, საიტიდან საიტზე - ასეთ მოგზაურობებს ხშირად "ქსელურ სერფინგს" ეძახიან (*web surfing*).

მიუხედავად იმისა, რომ დღეს არსებობს ბევრი სხვადასხვა ბრაუზერი, ყველას აქვს საერთო თვისება. ნახ.10.8-ზე ნაჩვენებია Internet Explorer ბრაუზერის ფანჯრის ძირითადი კომპონენტები - მსგავსი რამ შეიძლება ნახოთ პრაქტიკულად ნებისმიერ თანამედროვე ბრაუზერში.



ნახ.10.8. Internet Explorer ბრაუზერის ფანჯრის კომპონენტები

ბრაუზერის ინსტრუმენტების პანელი შეიცავს სხვადასხვა ღილაკებს, რომლებიც უფრო მოხერხებულს ხდის მსოფლიო აბლაბუდაში მოგზაურობას (ნახ.10.9).



ნახ. 10.9. Internet Explorer ბრაუზერის ღილაკების (ინსტრუმენტების) სტანდარტული პანელი

დღეს "საშინაო გვერდს" უწოდებენ ნებისმიერ ვებ-საიტს (ან უბრალოდ "სუფთა ფურცელს" ყოველგვარი ინფორმაციის გარეშე), რომლითაც ყოველთვის იწყება მუშაობა დუმილით ინტერნეტში ბრაუზერის გაშვების შემდეგ. ამ საიტის მისამართი შეიძლება მივუთითოთ ბრაუზერის აწყობებში, მაგალითად, გადავაქციოთ "საშინაო გვერდად" http://internet.ge/ პორტალი.

აქ ყოველი ღილაკი ასრულებს განსაკუთრებულ მისიას:

- **უკან (Back)** - გაბრუნებთ წინა, ნანახ ვებ-გვერდზე;
- **წინ (Forward)** - გადადიხართ შემდეგ გვერდზე, თუ მანამდე თქვენ დააწექით ღილაკს **„უკან“**;
- **გაჩერება (Stop)** - შეწყვეტს მიმდინარე ვებ-გვერდის ჩამოტვირთვას;
- **განახლება (Refresh/Reload)** - ხელახლა ჩამოგიტვირთავთ მიმდინარე გვერდს იმავე ფანჯარაში და განაახლებს მის შიგთავსს;
- **სახლში (Home)** - გიჩვენებთ გვერდს, რომელიც ჩვენ გავმართეთ როგორც "საშინაო";
- **ძებნა (Search)** - გახსნის სპეციალურ გვერდს (ან ბრაუზერის პანელს), სადაც შეიძლება შეიყვანოთ search.msn.com სამსახურისადმი საძიებო მოთხოვნა;
- **ამორჩეული (Favorites)** - გახსნის გვერდების სიას, რომლებზედაც გაკეთებული აღნიშვნები თქვენ შეინახეთ ადრე (ვებ-საიტების მისამართების თავისებური "უბის წიგნაკი");
- **მულტიმედია (Media)** – მიუთითებს მულტიმედიურ WindowsMedia.com საიტზე;
- **ჟურნალი (History)** - გახსნის ვებ-გვერდების სიას, რომლებიც თქვენ მოინახულეთ ბოლო დღეებში (დუმილით - ბოლო 20 დღის განმავლობაში);
- **ფოსტა (Mail)** - გახსნის თქვენი ელექტრონული ფოსტის პროგრამას და გაძლევთ საშუალებას გააგზავნოთ ვინმეს შეტყობინება, ვებ-გვერდის ასლი (ან მასზე მითითება), რომელსაც ათვალიერებთ;
- **ბეჭდვა (Print)** - იძლევა მიმდინარე ვებ-გვერდის ქაღალდზე ამობეჭდვის საშუალებას.

!

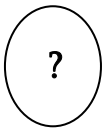
საშინაო/საოჯახო მომხმარებლების ინტერნეტთან დასაკავშირებლად ძირითადად გამოიყენება სხვადასხვა მოდემური გადაწყვეტილება. კოლქტიური საშინაო მომხმარებლები და კორპორატიული კლიენტები, როგორც წესი, იყენებენ გამუდმებულ ჩქაროსნულ მიერთებას გამოყოფილი ხაზით ან ბოჭკოვან-ოპტიკური არხით.

IP პროტოკოლის დონეზე ინტერნეტთან მუშაობისათვის გამოიყენება ან ჩვეულებრივი მარშრუტიზატორები (მოითხოვს დიდი რაოდენობის რეალურ IP-მისამართებს) ან მარშრუტიზატორები ქსელური მისამართების ტრანსლირების (NAT) ტექნოლოგიის მხარდაჭერით.

ინტერნეტთან მოხერხებული მუშაობისათვის ქსელში უნდა დავაყენოთ და ავაწყოთ დომენური სახელების სისტემის DNS სერვერი, რომელიც კვანძების სახელებს გარდაქმნის IP-მისამართებად.

ინტერნეტის ყველაზე პოპულარული სამსახურია WWW - წარმოადგენს ვებ-სერვერების გლობალურ განაწილებულ სისტემას სხვადასხვა ჰიპერტექსტური ინფორმაციით, რომელთანაც დაშვება ხოლციელდება სპეციალური ბრაუზერ-პროგრამების დახმარებით.

კითხვები და დავალებები



1. ინტერნეტში შესვლის როგორი ხერხებია შესაძლებელი? რითი განსხვავდებიან ისინი ერთმანეთისგან ძირითადად?
2. როგორი სახის მოდემები იცით? რაშია მათი ფუნქციონირების მსგავსება და განსხვავება ინტერნეტთან მუშაობისას?
3. რით განსხვავდებიან რეალური IP-მისამართების გამოყოფის და ქსელური მისამართების ტრანსლირების ტექნოლოგიები? რომელი მათგანია უფრო უკეთესი და რატომ?
4. რაში მდგომარეობს ქსელური მისამართების ტრანსლირების არსი? აქვს თუ არა მას ნაკლი რეალური IP-მისამართების გამოყოფასთან შედარებით?
5. შეიძლება თუ არა ინტერნეტთან პროვაიდერით შეერთებული კომპიუტერი "გადავაქციოთ" მთელი საშინაო ქსელისათვის "ინტერნეტში შესვლის სერვერად"? რა არის ამისათვის საჭირო?
6. რა არის DNS? როგორ მუშაობს ის?
7. როგორ არის დაკავშირებული დომენური სახელების ჩაწერის სტრუქტურა (რამდენიმე "სიტყვა" განცალკევებული სიმბოლოთი "წერტილი") DNS სამსახურის ხის მსგავს სტრუქტურასთან?
8. რაში მდგომარეობს DNS-ს ძირითადი უპირატესობა?
9. რატომ იწვევს მთელს მსოფლიოში შესამჩნევ აჟიოტაჟს ზედა დონის ახალი დომენური სახელების გამოჩენა?
10. როგორ ფიქრობთ, რა უპირატესობები და ნაკლოვანებები შეიძლება მოიტანოს დომენური სახელების არა ინგლისურ, არამედ ნაციონალურ ენებზე (მაგალითად, ქართულზე) რეგისტრირების შესაძლებლობამ?
11. დაახლოებით 10 წლის წინ რუსეთის ერთერთი ფირმა შემოვიდა "რუსული დომენური სახელების სამსახურის" შექმნის წინადადებით, რომელიც "რუსულენოვან" საიტებს მისცემდა რეგისტრირების საშუალებას (დღეს ასეთი დომენური სახელების სამსახური უკვე არსებობს). ამ დროს არანაირად არ ეხებოდნენ არსებულ DNS სისტემას, ხოლო "რუსული" საიტების მისამართებთან მუშაობისას ყველა კლიენტს სთავზობდნენ თავის კომპიუტერზე სპეციალური პროგრამა-უტილიტის დაყენებას. როგორ შეიძლება, ქვენი აზრით, ასეთი "სახელების სამსახურის" მუშაობის ორგანიზება?

12. რა არის ”მსოფლიო აბლაბუდა”? როგორია მისი წარმოშობის ისტორია? რა ძირითადი კომპონენტები გახდა საჭირო მისი რეალიზებისათვის?
13. რას ნიშნავს ტერმინი ”განაწილებული” WWW-ს განმარტებაში: ”განაწილებული საინფორმაციო სისტემა”? რა უპირატესობები და ნაკლოვანებები არის დაკავშირებული WWW-ს ამ თვისებასთან?
14. რაში მდგომარეობს ინფორმაციის ჰიპერტექსტური წარმოდგენის იდეა? როგორია მისი უპირატესობები?
15. რას ნიშნავს ვებ-გვერდი? ვებ-საიტი? ვებ-სერვერი? როგორი ურთიერთკავშირია ამ ცნებებს შორის?
16. როგორი შეიძლება იყოს ვებ-საიტის ტიპიური სტრუქტურა? რაში მდგომარეობს თითოეული ვებ-საიტის სტრუქტურის (სამი სახეობიდან) უპირატესობები და ნაკლოვანებები? რა შემთხვევაში აქვს აზრი ამა თუ იმ სტრუქტურის გამოყენებას?
17. როგორია ვებ-პორტალების და საძიებო სისტემების დანიშნულება? (მოიყვანეთ მაგალითები).
18. რა არის ბრაუზერი? როგორია მისი დანიშნულება? როგორ ფიქრობთ, რატომ არის Internet Explorer-ი ყველაზე პოპულარული ბრაუზერი, თუმცა, შეიძლოა პრაქტიკულად ნებისმიერი სხვა ბრაუზერის დაყენება სხვა ”ოჯახებიდან”?
19. როგორია Internet Explorer-ის ბრაუზერის ძირითადი ფუნქციონალური შესაძლებლობები? როგორ ვმართოთ ისინი?

თავი 11

ურთიერთობებისა და მონაცემთა გაცვლის საშუალებები. ინტერნეტში ქცევის წესები

ამ თავში
თქვენ ნახავთ პასუხებს შემდეგ კითხვებზე:

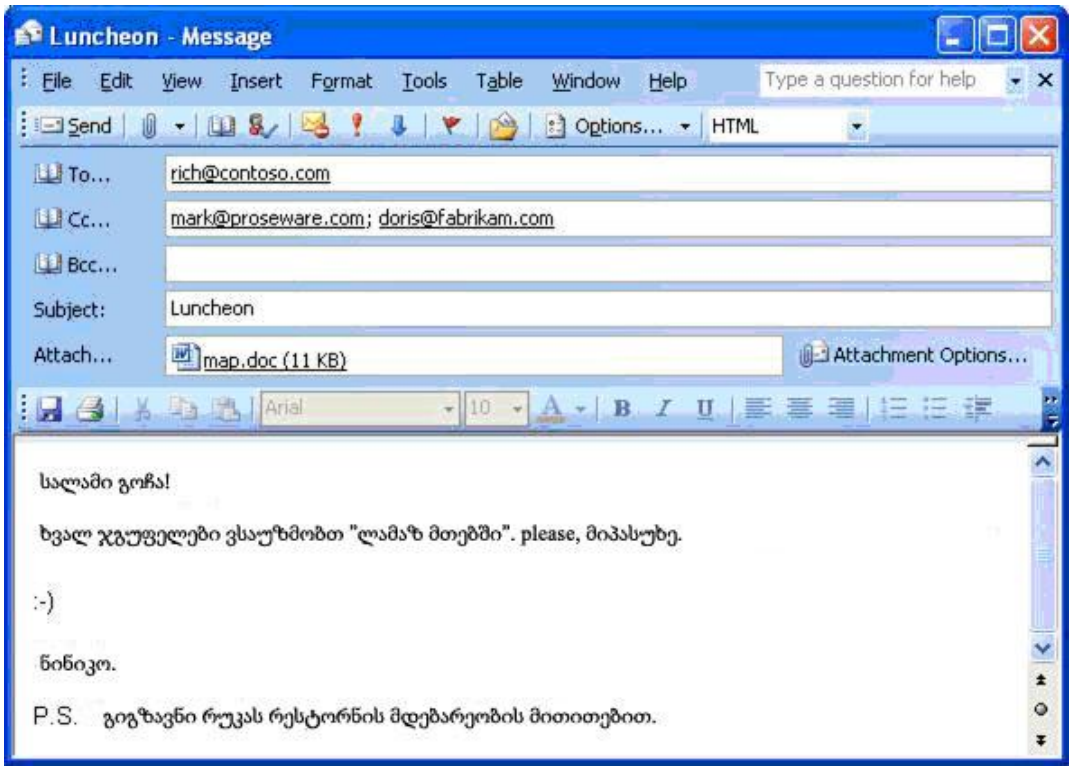
- როგორ მუშაობს ელექტრონული ფოსტა?
- როგორ შევქმნათ ელექტრონული ფოსტის სააღრიცხვო ჩანაწერი?
- როგორ მივიღოთ და გავაგზავნოთ ელექტრონული შეტყობინებები?
- როგორია თავაზიანობის წესები ინტერნეტში ურთიერთობისას?
- რისთვის იქმნება სადისკუსიო ჯგუფები (ფორუმები)?
- რა არის მყისიერი შეტყობინებები?
- როგორ მივიღოთ და გავაგზავნოთ მყისიერი შეტყობინებები?
- რაში მდგომარეობს ფაილების ერთობლივი გამოყენება?
- როგორ დავადგინოთ ლეგალურია თუ არა ფაილების ერთობლივი გამოყენება?

ადრე ჩვენ გავეცანით მსოფლიო აბლაბუდას (WWW) - ერთერთ ძირითად რესურსთაგანს, რის გამოც მომხმარებელთა უმრავლესობა უერთდება ინტერნეტს. ინტერნეტი, როგორც ინფორმაციის გადაცემის გლობალური სისტემა, გვაწვდის სხვა საინტერესო შესაძლებლობებს: ელექტრონული ფოსტის, მყისიერი შეტყობინებების გაცვლის, ფაილების გაცვლისა და სხვა. ეს თავი მიეძღვნება მათ გაცნობას.

ელექტრონული ფოსტა

ელექტრონული ფოსტა, e-mail-ი ინტერნეტის ერთერთი ხშირად გამოყენებადი (WWW-ს შემდეგ) შესაძლებლობაა. ყოველ დღიურად ასობით მილიონი ელექტრონული შეტყობინება იგზავნება და მიიღება მსოფლიოში. ინტერნეტში შესვლის საშუალების მქონე ნებისმიერ მომხმარებელს ადვილად შეუძლია დაირეგისტრიროს უფასო საფოსტო ყუთი ელექტრონული ფოსტის ყველასათვის ხელმისაწვდომ ერთერთ სერვერზე, შეატყობინოს მეგობრებსა და ნაცნობებს და თითქმის იმწამსვე დაიწყოს e-mail-ბის გაგზავნა და მიღება (ნახ. 11.1). კორპორატიულ გარემოში ელექტრონული ფოსტა გახდა თანამშრომლებს შორის ურთიერთქმედების ერთერთი მთავარი საშუალება. ელექტრონული ფოსტა მუშაობს პრაქტიკულად ჩვეულებრივის მსგავსად. მასშიც არის წერილები, კონვერტები მისამართებით, მიტანის სამსახური, საფოსტო ყუთები. ოღონდ ჩვეულებრივი "ქაღალდიანისაგან" განსხვავებით, ელექტრონული წერილის მიტანას იშვიათად ესაჭიროება წუთზე მეტი.

ელექტრონული შეტყობინებების გასაგზავნად და მისაღებად თქვენ დაგჭირდებათ *ელექტრონულ ფოსტასთან სამუშაო კლიენტური პროგრამული უზრუნველყოფა.* ეს



ნახ. 11.1 ელექტრონული შეტყობინების მაგალითი

შეიძლება იყოს, მაგალითად, Microsoft Outlook, Outlook Express ან ნებისმიერი სხვა *საფოსტო კლიენტი*, ან უბრალოდ *ბრაუზერი*, რადგან ბევრი საფოსტო სერვერი, განსაკუთრებით საყოველთაოდ ხელმისაწვდომი, აწოდებს მომხმარებელს ვებ-ინტერფეისებს საკუთარ საფოსტო ყუთებთან სამუშაოდ.

!

კლიენტური საფოსტო პროგრამების უმრავლესობა მომხმარებლის საფოსტო ყუთთან მიერთებისათვის, იყენებს POP3 და IMAP4 პროტოკოლებს, SMTP პროტოკოლს - წერილების გასაგზავნად. საფოსტო ყუთებთან ვებ-დაშვება ხორციელდება HTTP პროტოკოლის თანახმად.

საფოსტო შეტყობინებების გაგზავნისა და მიღების დაცვის უზრუნველსაყოფად რეკომენდებულია *SSL (Secure Sockets Layer)* პროტოკოლის გამოყენება.

საფოსტო სერვერ Exchange-თან სამუშაოდ პროგრამა Microsoft Outlook იყენებს *RPC პროტოკოლს*, რომელიც თავისთავში შეიცავს არხის უსაფრთხოების უზრუნველყოფის ჩაშენებულ მექანიზმს.

შეგახსენებთ, რომ ელექტრონულ ფოსტასთან მუშაობისას აუცილებლია თანამედროვე ანტივირუსული პროგრამებისა და არასასურველი ფოსტის - *სპამისაგან* დაცვის საშუალებების გამოყენება.

ნებისმიერ შემთხვევაში ელექტრონული ფოსტის ფუნქციონირების პრინციპებია:

- აკრიფოთ თქვენი წერილი, მიუთითებთ რა მიმღების ელექტრონულ მისამართს (მაგალითად, myfriend@gmail.com);
- ღილაკზე - **გაგზავნა** დაწოლის შემდეგ საფოსტო პროგრამა (ანუ ბრაუზერი) აკონვერტირებს შეტყობინებას საჭირო ფორმატში და გაუგზავნის მას თქვენს საფოსტო სერვერს.

ამის შემდეგ მუშაობას იწყებს საფოსტო სერვერი:

- დომენის DNS-სერვერისადმი წერილის მიმართვის შემდეგ, თქვენი სერვერი დაადგენს მიმღების საფოსტო სერვერის სახელსა და IP-მისამართს (ამისათვის DNS-ში რეგისტრირდება სპეციალური "*საფოსტო გამცვლელი*" - *Mail Exchanger,* ანუ *MX*);
- ორივე საფოსტო სერვერს შორის მყარდება კავშირი *SMTP (Simple Mail Transfer Protocol* - ანუ "ფოსტის გადაცემის მარტივი პროტოკოლი"*) პროტოკოლით* და თქვენი წერილი გადაეცემა მიმღების დაშორებულ სერვერს.

ადრესატის სერვერი ღებულობს წერილს, ადგენს - არსებობს თუ არა ამ სერვერზე მოთხოვნილი საფოსტო ყუთი, ატარებს სხვა შემოწმებებს (მაგალითად, ხომ არ არის გადავსებული მიმღების საფოსტო ყუთი) და, თუ ყველაფერი წესრიგშია, აწვდის წერილს. წერილის მიმღები, იყენებს რა თავის საფოსტო პროგრამას, ნახულობს თქვენს შეტყობინებას.

მრავალრიცხოვანი კლიენტ-სერვერული და სერვერ-სერვერული ოპერაციების მიუხედავად, ელექტრონული წერილის მიტანა, როგორც უკვე ვთქვით, ხდება ძალიან სწრაფად, ზოგჯერ წამებშიც.

ელექტრონული წერილების მისაღებად და გასაგზავნად, საჭიროა *ელექტრონული ფოსტის სააღრიცხვო ჩანაწერი, რომელიც* შეიძლება მივიღოთ სასწავლო დაწესებულებაში, სამსახურში, პროვაიდერთან, ან, როგორც უკვე ითქვა, დავარეგისტრიროთ საყოველთაოდ ხელმისაწვდომ უფასო სერვერზე.

i

სპამი *(SPAM, "Shoulder Pork and hAM"/ "SPiced hAM")* - პირდაპირი თარგმანით ნიშნავს "დაწნეხილ შაშხს სანელებლებით" (ოდესღაც ამ საქონლის მწარმოებელი ფირმა პირდაპირ "ავსებდა" ბევრი ამერიკელის საფოსტო ყუთს - მაშინ მხოლოდ ჩვეულებრივს, არაელექტრონულებს). დღეს ეს ცნება ნიშნავს ელექტრონული ფოსტის უსარგებლო შეტყობინებებს, რომლებიც იძულებით ეგზავნება აბონენტების დიდ რაოდენობას. ასეთი შეტყობინებები შეიცავენ ჩვეულებრივად სარეკლამო განცხადებებს, "სწრაფი გამდიდრების ხერხების" აღწერებს და სხვა. სამწუხაროდ, დღეს ელექტრონული წერილების 80% ინტერნეტში არის სპამი.

უჩვეულო სიმბოლო ”@”, რომელსაც ხალხში ”ძაღლუკა” დაარქვეს, კომპიუტერულ ყოველდღიურობაში შემოიტანა ერთ-ერთი საფოსტო პროგრამის ARPANet-ის შემქმნელმა რეი ტომლინსონმა. ინგლისურ ენაში სიმბოლო ”@” (”კომერციული ეთ”) ხშირად გამოიყენება საფასურებში (მაგალითად, ჩანაწერი ”10 items @ $5.28” ნიშნავს ”10 ცალი 5.28 დოლარად”). ტომილსონმა ეს სიმბოლო აარჩია იმიტომ, რომ ის არ იხმარება არცერთ სახელში და, შესაბამისად, არ შეიძლება გამოიწვიოს არევ-დარევა.

საფოსტო პროგრამების უმრავლესობა თავისთავში შეიცავს *საგამისამართო წიგნს* რომელიც იძლევა ხშირად გამოყენებული ელექტრონული ფოსტის მისამართების შენახვის საშუალებას შემდგომი სწრაფი ჩასმისათვის წერილის შესაბამის ველებში.

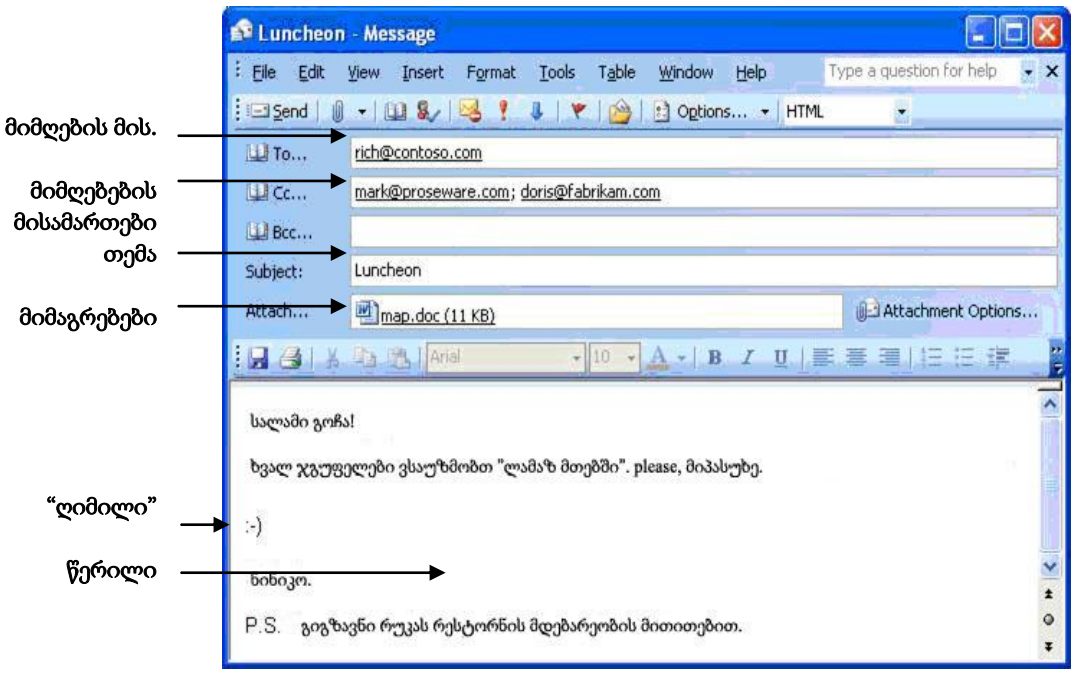
სააღრიცხვო ჩანაწერის შექმნისას თქვენთვის დარეგისტრირებული იქნება უნიკალური *ელექტრონული მისამართი*, რომელიც შედგება მომხმარებლის სახელისაგან (როგორც წესი, შეიძლება ავირჩიოთ სურვილისამებრ), ”@” ნიშნისა და დომენის სახელისაგან: მაგალითად, myname@posta.ge. გარდა ამისა, თქვენ მიიღებთ მომხმარებლის უნიკალურ სახელს *(account, login name)* და *პაროლს*, რომელიც დაგჭირდებათ სერვერთან შეერთებისას ფოსტის შემოწმების მიზნით (მიღება და გაგზავნა).

ელექტრონული შეტყობინებების გადაცემის ყველა სისტემა ხასიათდება წერილებისა და ”ელექტრონული კონვერტების” სხვადასხვა შიდა ფორმატებით (შეგახსენებთ, რომ სხვადასხვა საფოსტო სისტემების ურთიერთქმედებისათვის გამოიყენება *საფოსტო რაბები*). მიუხედავად ამისა, იყენებენ შეტყობინებების მსგავს საბაზო ელემენტებს (ნახ. 11.2). თუ თქვენ გაიგებთ ამ ელემენტთაგან თითოეულის დანიშნულებას, შეგეძლებათ მიიღოთ და გააგზავნოთ ელექტრონული შეტყობინებები ნებისმიერ საფოსტო სისტემაში.

ელექტრონული შეტყობინებების საბაზო ელემენტებია:

- *მიმღების სახელი და მისამართი* - როგორც ჩვეულებრივი წერილის გაგზავნისას, ***აუცილებელად*** (სხვანაირად წერილის მიტანა იქნება შეუძლებელი) უნდა მიუთითოთ ელექტრონული მისამართი, ვისაც უგზავნით შეტყობინებას (ველი „to”);
- *გამგზავნის სახელი და მისამართი* - თქვენი საკუთარი სახელი და მისამართი. ეს პარამეტრები ავტომატურად ჩაისმება საფოსტო პროგრამის ან სერვერის მიერ წერილის გაგზავნისას;
- *თემა* (ველი “Subject”)- თქვენი წერილის შინაარსის მოკლე ფორმულირება;
- *დრო და თარიღი* - როგორც წესი, ავტომატურად ივსება საფოსტო პროგრამის ან სერვერის მიერ წერილის გაგზავნისას;
- *წერილის შინაარსი* (შეიძლება იყოს მითითება “Plane Text”) - თავად ტექსტური შეტყობინება;
- *მიმაგრებები* (შეიძლება იყოს “Attach” მითითების სახით)- ელექტრონულ შეტყობინებაზე მიმაგრებული ფაილები, მათ შორის გრაფიკული გამოსახულებები, ხმის ციფრული ჩანაწერები, პროგრამები და დოკუმენტები;

- *ასლი* (ველი Cc, "Carbon copy"-ს შემოკლება - "ასლების გადასაღები ქაღალდი") - ამ ველში შეიძლება შეიყვანოთ სხვა პიროვნების ელექტრონული მისამართიც, თუ გსურთ, რომ მასაც გაეგზავნოს მოცემული წერილის ასლი;
- *"ბრმა ასლი"* (შეიძლება იყოს "BCC" მითითების სახით - "blind cc") - იგივეა, რაც ჩვეულებრივი ასლი, მაგრამ "ძირითად" ადრესატს *არ ეცოდინება*, რომ წერილის ასლი სხვა მიმღებს გადაეგზავნა.



ნახ.11.2. ელექტრონული შეტყობინების ტიპიური ელემენტები

ელ. ფოსტასთან მუშაობისას თავაზიანობის წესები

ელექტრონულმა ფოსტამ ადამიანებს მისცა ურთიერთობის ახალი შესაძლებლობის საშუალება და აღადგინა ეპისტოლური ჟანრი, თითქმის მივიწყებული ტელეფონის საყოველთაო გავრცელების შემდეგ. იმისათვის, რომ ურთიერთობა იყოს უსაფრთხო და თავაზიანი, საჭიროა ზოგიერთი მარტივი წესის დამახსოვრება. *ქსელური ეთიკის წესების* სრული კრებული, ან *"წეთიკეტი" (Netiquette)*, ადვილად შეიძლება მოვიძიოთ ინტერნეტში, მაგალითად, http://www.albion.com/netiquette/ გვერდზე.

ზოგიერთი შემოკლებები, რომლებიც გამოიყენება ველში **„თემა“ - Subject** (და საერთოდ ინტერნეტში ურთიერთობისას):
FYI (“For your info”) – „ცნობისათვის“;
ASAP (“As soon as possible”) – ”რაც შეიძლება სწრაფად”;
IMO (“In my opinion”) – ”ჩემი აზრით”;
IMHO (“In my humble opinion”) – ”ჩემი მოკრძალებული აზრით”;
AFAIK (“AS far as I know”) – ”რამდენადაც ჩემთვის არის ცნობილი”;
BTW (“By the way”) – ”სიტყვამ მოიტანა და”;
BBL (“Be back late(r)”) – ”დამაგვიანდება”;
TTL (“Talk to you later”) – ”მერე ვილაპარაკოთ”;
SIT (“Stay touch”) – “იყავი კავშირზე”;
BCNU (“Be seeing you”) – ”შევხვდეთ ერთმანეთს”;

ეს ”ღიმილები” დაგეხმარებათ გამოხატოთ ემოციები ელექრონულ შეტყობინებებში:

1. ყოველთვის გახსოვდეთ, რომ *თქვენ ურთიერთობთ ადამიანებთან და არა კომპიუტერებთან.* ეს ყველაზე მთავარია ინტერნეტში მუშაობისას.

2. ეცადეთ, ყოველთვის მიუთითოთ, რაზეა ლაპარაკი წერილში, რომ მიმღებმა უცებ გაიგოს მისი შინაარსის შესახებ.

3. ეცადეთ, არ გამოიყენოთ ხელნაწერი ასოები: ეს ხშირად აღიქმება როგორც უზრდელობა (იგივეა, რაც ყვირილი ჩვეულებრივი საუბრისას).

4. იმისათვის, რომ ნაცნობებთან და ახლო ადამიანებთან ურთიერთობა გავხადოთ უფრო ემოციური, შეიძლება გამოიყენოთ ე. წ. ”*სმაილები*” – რამოდენიმე სიმბოლოსგან შედგენილი ”ღიმილები”.

5. შეეცადეთ წეროთ მოკლე შეტყობინენები, ხოლო გრძელები - განაცალკევეთ ცარიელი სტრიქონებით ადვილად გაგებისათვის.

6. წერეთ წიგნიერად, კორექტულად შეადგინეთ ფრაზები, წინააღმდეგ შემთხვევაში შესაძლებელია თქვენი სიტყვების არასწორი გაგება.

7. წერილზე პასუხის გაცემისას შეიტანეთ მასში ამომავალი შეტყობინების მხოლოდ ის ნაწილები (*მოახდინეთ ციტირება*), რომლებიც საჭიროა თქვენი პასუხის გასაგებად.

8. მოერიდეთ ზედმეტ მორთულობებს - ბევრი სურათი, სხვადასხვა ფერისა და ზომის შრიფტები და ა. შ. მხოლოდ აძნელებენ წერილის კითხვას და ზრდიან მის მოცულობას (აქედან გამომდინარე, გადაგზავნის დროს).

9. ყოველთვის მოაწერეთ ხელი საკუთარ წერილს, ჩართეთ ხელის მოწერაში საკუთარი სახელი და ურთიერთობისათვის მნიშვნელოვანი ინფორმაცია (მაგალითად, ტელეფონი, მისამართი, თანამდებობა და სხვა).

10. გახსოვდეთ, რომ ჩვეულებრივად წერილი ქსელით გადაიცემა დაშიფრვის გარეშე, ამიტომ *არასოდეს არ შეიტანოთ ელექტრონულ შეტყობინებაში ინფორმაცია სახელების, დაშვების პაროლების, საკრედიტო ბარათების ნომრების და ა. შ. შესახებ.*

სადისკუსიო ჯგუფები (ფორუმები)

ელექტრონული შეტყობინებების ერთი ან რამდენიმე ადრესატისადმი გაგზავნის გარდა, ელექტრონული ფოსტა შეიძლება გამოვიყენოთ *სადისკუსიო ჯგუფში (ფორუმში, სიახლეთა ჯგუფში)* ურთიერთობისათვის.

სადისკუსიო ჯგუფი - ინტერნეტის იმ მომხმარებლების გაერთიანება, რომლებსაც აქვთ საერთო ინტერესები და ურთიერთობენ ელექტრონული ფოსტის დახმარებით ან სპეციალური ვებ-საიტების დახმარებით. თქვენ შეგიძლიათ გააგზავნოთ ელექტრონული შეტყობინება ჯგუფის მთავარ მისამართზე, ხოლო სერვერი ავტომატურად დაუგზავნის წერილის ასლს ჯგუფის ყველა წევრს, გამოიყენებს რა მისამართებს *დაგზავნის სიიდან*. მაგალითად, მოსწავლეთა ჯგუფი ესწრება საზაფხულო მეცადინეობებს. ორგანიზაციას, რომელიც ატარებს ამ ღონისძიებას, შეუძლია შექმნას მსმენელთათვის ცალკე სადისკუსიო ჯგუფი. იმის შემდეგ, რაც მსურველები ხელს მოაწერენ დაგზავნის სიას, მათ შეეძლებათ გაუგზავნონ შეტყობინებები თითოეულს ცალკ-ცალკე და ასევე ჯგუფის ყველა წევრს ერთდროულად.

ინტერნეტში არსებობს სხვადასხვა თემებისადმი მიძღვნილი ათასობით სადისკუსიო ჯგუფი. როდესაც იპოვით თქვენთვის საინტერესო თემით გაერთიანებულ ჯგუფს, უპირველეს ყოვლისა უნდა გააგზავნოთ შეტყობინება ხელმოწერის თხოვნით. პასუხად ჩვეულებრივ მოდის შეტყობინება, რომ თქვენ გახდით ჯგუფის წევრი, ან ჯგუფის უკვე არსებულ წევრთაგან ვინმემ უნდა დაადასტუროს თქვენი რეგისტრაცია და დაგამატოთ ხელმომწერთა სიაში. ყოველ სადიკუსიო ჯგუფს აქვს ხელმომწერების დამატების წესების თავისი კრებული; თქვენთვის საინტერესო ჯგუფში მუშაობის დაწყების წინ აუცილებლად გაეცანით ამ წესებს და დაიცავით ისინი.

სადისკუსიო ჯგუფის (ფორუმის) სხვა შესაძლო ვარიანტი შეიძლება რეალიზებულ იქნას ვებ-საიტის სახით (*სტუმრის წიგნის* ანალოგიურად). ამ შემთხვევაში ფორუმის ყველა მონაწილეს, რომლებიც რეგისტრირებული არიან მათთვის საინტერესო თემით ურთიერთობისათვის, შეუძლიათ დაუმატონ საერთო სიას თავიანთი შეტყობინებები ან პასუხები და კომენტარები არსებულ შეტყობინებებზე. ამ საიტის სხვა დამთვალიერებელს თავისუფლად შეუძლია წაიკითხოს

:-) - ღიმილი;
;-) - თვალის ჩაკვრა;
:-* - კოცნა;
:-(- სევდა;
:-o - გაოცება;
:-O - ყვირილი;
:-D - სიცილი;
:-P - ენის ჩვენება;
:-I - ფიქრებში ყოფნა;
:-> - ბოროტი ჩაცინება;
:-/ - გაუგებრობა
8-) - კმაყოფილება;
და ა. შ.

i

სტუმრების წიგნი საიტზე განთავსებული ერთ-ერთი "სერვისთაგა-ნია", რომ მის მნახველებს შეეძლოთ თავისი სურვილების, შექებების ან, შესაძლოა, კრიტიკული შენიშვნების დატოვება.

ეს შეტყობინებები (ტექსტის რამდენიმე ფრაგმენტის გარდა), მაგრამ არ შეუძლია თავისი შეტყობინებების დამატება სანამ არ გაივლის რეგისტრაციის პროცედურას.

მყისიერი შეტყობინებების გაცვლა ინტერნეტში

ელექტრონული ფოსტა მუშაობს უფრო სწრაფად ვიდრე ჩვეულებრივი, მიუხედავად იმისა არავითარი გარანტია არ არსებობს, რომ ადრესატი დაუყონებლივ გიპასუხებთ თქვენს ელექტრონულ წერილზე. *რეალურ დროში* ინტერნეტით ურთიერთობისას შეიძლება გამოიყენოთ უამრავი ხერხი, მაგრამ ყველაზე პოპულარულია მყისიერი შეტყობინებების გამოყენება.

მყისიერი შეტყობინება - ტექსტი, რომელიც შეგყავთ სპეციალური პროგრამის ფანჯარაში. ადამიანი, რომელთანაც თქვენ ურთიერთობთ, მიიღებს შეტყობინებას უკვე წამის შემდეგ. ცხადია, მეყვსეული შეტყობინებებით გაცვლისათვის ორივე მოსაუბრე იმ მომენტში მიერთებული უნდა იყოს ინტერნეტთან და იყენებდეს შეთავსებად პროგრამულ უზრუნველყოფას. თქვენ აგრეთვე შეგიძლიათ ერთდროულად ისაუბროთ რამდენიმე ადამიანთან *ჩატ-ჯგუფში* (ინგლისურად "chat" - ლაქლაქი). ჩატ-ჯგუფის ყველა წევრი მყისიერად ხედავს ყველა შეტყობინებას, რომელიც ეგზავნება ნებისმიერ მომხმარებელს სხვა მომხმარებლებისაგან. სპეციალური პროგრამების დახმარებით თქვენ შეგიძლიათ მიუერთდეთ ღია ჩატ-ჯგუფებს, რომლებიც მიძღვნილია გარკვეული თემებისა და ინტერესებისადმი, ან შექმნათ თქვენი საკუთარი ჩატ-ჯგუფი, რომელშიც შეხვდებით და ესაუბრებით თქვენს მეგობრებს.

არსებობს შეტყობინებების მყისიერი გაცვლის რამდენიმე პოპულარული გამოყენება, ერთ-ერთი მათგანია Microsoft-ის მიერ შემოთავაზებული MSN Messenger პროგრამა (ნახ. 11.3).

სიტყვები "რეალურ დროში" ნიშნავს, რომ შეტყობინებების მყისიერი გაცვლის პროგრამაში შეგყავთ საკუთარი შეტყობინება და როგორც კი თქვენ დააწვებით ღილაკს **გაგზავნა - Send**, ყველა თქვენთან მოსაუბრე, რომელიც მოცემულ მომენტში მუშაობს ქსელში, შეძლებს მის წაკითხვას პრაქტიკულად მაშინვე. ამიტომ, სანამ დააწვებით ღილაკს, კიდევ ერთხელ გადაიკითხეთ საკუთარი შეტყობინება, შეამოწმეთ გამონათქვამების კორექტულობა და გაასწორეთ დაშვებული შეცდომები.

შეტყობინებების მყისიერი გაცვლის სხვა პოპულარული პროგრამაა ICQ. ამბობენ, რომ ეს არის ინგლისური "I seek you"-ს – "მე გეძებ შენ"-ის განსხვავებული სახე. მაგრამ პროგრამა ICQ უნდა ჩამოტვირთოთ ინტერნეტიდან და დააყენოთ ცალკე, მაშინ როდესაც MSN Messenger-ი არის Windows-ის სტანდარტული გამოყენება (კერძოდ, XP-ვერსიაში).

ნახ. 11.3. MSN Messenger პროგრამის ფანჯარა

მყისიერი შეტყობინებების გამოყენებისათვის, ჯერ უნდა დავრეგისტრირდეთ მოცემული სერვისის სამსახურში, მივიღოთ მომხმარებლის სახელი და პაროლი, და დავაყენოთ საკუთარ კომპიუტერზე სპეციალური პროგრამული უზრუნველყოფა. მყისიერი შეტყობინებების გაცვლის პროგრამების უმრავლესობა საშუალებას მოგცემთ შექმნათ ნაცნობების სია, რამლებთანაც თქვენ ხშირად საუბრობთ. მყისიერი შეტყობინებების გაცვლის

სისტემების ერთერთი მნიშვნელოვანი თავისებურება ის არის, რომ ამ სიაში შეგეძლებათ ნახოთ *მიმდინარე ინფორმაცია თქვენი მეგობრებისა და ნაცნობების ქსელში ყოფნის შესახებ*, ე. ი. ყოველთვის შეიძლება შეამოწმოთ, მიერთებული არიან თუ არა ისინი ინტერნეტთან მოცემულ მომენტში, იმყოფებიან თავიანთ კომპიუტერთან, თუ არა. თქვენი პროგრამა შეგიძლიათ ააწყოთ ისე, რომ მხოლოდ ნაცნობებმა იცოდნენ, ხართ თუ არა მიერთებული ინტერნეტთან მოცემულ მომენტში.

სააღრიცხვო ჩანაწერის გაკეთების შემდეგ, შეგიძლიათ სიაში აირჩიოთ პიროვნება, რომელთანაც გსურთ ურთიერთობა. თქვენს კომპიუტერზე პროგრამის ფანჯარაში შეიყვანეთ გზავნილის ტექსტი, ხოლო შემდეგ დააწექით გაგზავნის ღილაკს. იმ მომენტში მომხმარებელი არჩეული სახელით მიიღებს თქვენს შეტყობინებას და შეძლებს გიპასუხოთ.

თუ რამდენიმე ხნით ტოვებთ კომპიუტერს ან უბრალოდ გინდათ, რომ არ შეგაწუხონ, შეცვალეთ პროგრამაში *საკუთარი მდგომარეობა ქსელში*. თქვენი ნაცნობები უცებ დაინახავენ, რომ ხართ წასული ან დაკავებული. ამასთან ისინი გამოგიგზავნიან შეტყობინებას, რომელიც დაგელოდებათ მანამ დაბრუნდებით ან გათავისუფლდებით (ზუსტად ისევე, როგორც ელექტრონული ფოსტის წერილი).

ფაილებთან ერთობ-ივი შეღწევის პრო-გრამა KAZZA იყო ერთ-ერთი პირველი საყოველთაოდ ცნო-ბილი პროგრამა, მა-გრამ მისი სერვერი მოგვიანებით დაიხუ-რა ამ პროგრამის მომ-ხმარებლების მიერ სა-ავტორო უფლებების მრავალრიცხოვანი დარღვევების გამო. ამიტომ დღეს არ-სებული ფაილებთან ერთობლივი შეღწევის პროგრამები (eMule, eDonkee და სხვა) მუშაობენ *დეცენტრა-ლიზებულად* (მათ-თვის არ არსებობს ერთიანი სერვერი, რომლის დახურვამ შეიძლება შეწყვიტოს სერვისის მუშაობა), ქმნიან რა ფაქტიურად ინტერნეტის "ბაზაზე" გან-ალკევებულ, ე. წ. "*პირიწგულ*" ქსელს.

ფაილების გაცვლა ინტერნეტში

ფაილების გადაცემა ინტერნეტში ინფორმაციის გაცვლის ერთერთი ყველეზე გავრცელებული ხერხია. ისიც საკმარისია ითქვას, რომ FTP ფაილების გადაცემის პროტოკოლოს პირველი ვერსია შემუშავდა ჯერ კიდევ 1971 წ. მას შემდეგ ფაილების გაცვლის პრინციპები რამდენადმე შეიცვალა და ამჟამად ყველაზე პოპულარულია პროგრამები, რომლებიც უზრუნველყოფენ *ფაილებთან ერთობლივ შეღწევას (per-to-per file sharing)*. ეს დიდადაა დაკავშირებული ისეთი ფორმატების გამოჩენასთან და ფართო გავრცელებასთან, როგორიცაა **JPEG, MP3, WMA, MPEG4** და სხვა, რომლებიც საშუალებას იძლევიან კომპაქტური სახით შევინახოთ გრაფიკა, აუდიო- და

ვიდეომონაცემები.

ამ ფორმატების პოპულარობის გამო, ზოგიერთმა კომპანიებმა ფაილებისადმი ერთობლივი შეღწევისათვის შეიმუშავეს სპეციალური პროგრამული უზრუნველყოფა, რამაც მომხმარებლებს მისცა თავის კომპიუტერებზე მუსიკალური ფაილების შენახვისა და მათი საყოველთაოდ ხელმისაწვდომად გადაქცევის საშუალება ინტერნეტში. თავდაპირველად საერთო შეღწევას იყენებდნენ მხოლოდ ციფრული მუსიკისათვის. დღეს საერთო გამოყენება გავრცელდა პრაქტიკულად ყველა ფაილზე, მათ შორის ტაბულებიან და ტექსტურ დოკუმენტებზე, პროგრამებზე, გრაფიკაზე და ვიდეოფილებზე.

იმისათვის, რომ ერთობლივად გამოიყენოთ ფაილები, დაგჭირდებათ სპეციალური პროგრამა. ამის შემდეგ ხდება თქვენი კომპიუტერის დაკავშირება სერვერთან, რომელიც მართავს მრავალ მომხმარებლურ კომპიუტერზე ინტერნეტში განლაგებული *საერთო ფაილების სიებს*. სერვერი მხარს უჭერს აგრეთვე ყველა მომხმარებლის სიას და შეუძლია საერთო ფაილებში შეღწევის მართვა. მიიღებს რა ინფორმაციას სერვერისგან, თქვენი კომპიუტერი გაცვლის პროგრამით უკავშირდება ერთ-ერთ კომპიუტერს, რომელშიც ინახება თქვენთვის საინტერესო ფაილი (ან მისი რომელიმე ნაწილი). პროგრამა აგზავნის ქვენი კომპიუტერის მისამართს, თქვენს საიდენტიფიკაციო ინფორმაციას და მოითხოვს საჭირო ფაილს. თუ ყველა შემოწმება დასრულდა წარმატებით, დაშორებული კომპიუტერი ინტერნეტით უგზავნის მონაცემებს უშუალოდ თქვენს კომპიუტერს. ამგვარად, ერთობლივი გამოყენების სისტემა გაძლევთ საშუალებას პირდაპირ დაუკავშირდეთ ინტერნეტში სხვა მომხმარებლის კომპიუტერს და გაცვალოთ მასთან ფაილები.

ინტერნეტიდან ინფორმაციის გამოყენების ლეგალურობა

ფაილების გადაგზავნისას, განსაკუთრებით ფაილებისადმი ერთობლივი შეღწევისას, უნდა ვიქონიოთ მხედველობაში, რომ ინტერნეტში წარმოდგენილი ინფორმაციის უმრავლესობა დაცულია *კანონით საავტორო უფლებების შესახებ* (თუნდაც შესაბამის ვებ-საიტებზე პირდაპირ არაფერი ითქვას). ის რომ ფაილები ადვილად ხელმისაწვდომია ინტერნეტის ყველა

მომხმარებლისათვის, არ ნიშნავს, რომ ისინი შეიძლება თავისუფლად დავაკოპიროთ და გავავრცელოთ. ასეთი კოპირება და გავრცელება შემთხვევათა აბსოლუტურ უმრავლესობაში, უკანონოა. ინტერნეტიდან რაიმე ინფორმაციის გამოყენებისას, საკუთარ მოხსენებაში, პრეზენტაციაში ან რეფერატში, აუცილებლია ინფორმაციის მფლობელისაგან ან ვებ-საიტისგან თანხმობის მიღება და გააკეთოთ მითითება ინტერნეტის გვერდებზე საიდანაც იყო აღებული მასალები. (სიტყვამ მოიტანა, მფლობელების უმრავლესობა სიამოვნებით მოგცემენ ასეთ ნებართვას - მათთვის ეს იქნება იმის ნიშანი, რომ ინტერნეტში გამოქვეყნებული მასალები მართლაც საინტერესოა და სასარგებლო.)

უნებართვოდ მხოლოდ ისეთი ინფორმაციის გამოყენება და თავისუფლად გავრცელება შეიძლება, რომლებზედაც მფლობელის მიერ მკაფიოდაა მითითებული, რომ ისინი *განკუთვნილია თავისუფალი გავრცელებისათვის*. ასეთ შემთხვევაშიც, როგორც წესი, არ შეიძლება მონაცემების მოდიფიცირება და გავრცელება პირველწყაროს მითითების გარეშე.

!

ამგვარად, მსოფლიო აბლაბუდას გარდა, ინტერნეტი თავის მომხმარებლებს თავისუფალი ურთიერთობის ფართო საშუალებას აძლევს. მათ შორის ძირითადებია ელექტრონული ფოსტა, რომელიც მუშაობს საფოსტო სერვერების მთელი სისტემის წყალობით, მყისიერი შეტყობინებების გადაცემა და სადისკუსიო ჯგუფები. გარდა ამისა, ინტერნეტში ფუნქციონირებს ფაილებთან ერთობლივი შეღწევის ბევრი სისტემა, რომლებიც მომხმარებლებს საშუალებას აძლევენ გაცვალონ მუსიკალური ფაილები და სხვა მონაცემები.

ინფორმაციასთან მუშაობისას და მისი გაცვლისას არ უნდა დაგვავიწყდეს, რომ ინტერნეტში განთავსებული ფაილები და სხვა მონაცემები დაცულია კანონით საავტორო უფლებების შესახებ, ამიტომ მათი კოპირება და გავრცელება მფლობელის ნებართვის გარეშე შეიძლება იყოს არამართლზომიერი.

კითხვები და დავალებები

?

1. შექმენით ინტერნეტის სერვისებისა და სამსახურების ტაბულა მათი ძირითადი მახასიათებლების მითითებით.
2. როგორია ელექტრონული ფოსტის ფუნქციონირების ძირითადი პრინციპები?
3. რისთვისაა საჭირო **IMAP, POP3, SMTP, SSL, RPC** პროტოკოლები?
4. რატომ უწოდებენ ელექტრონულ ფოსტას ”ასინქრონული ურთიერთობის საშუალებას” (ე. ი. ურთიერთობას, გაყოფილს დროში)?
5. რა არის ელექტრონული ფოსტის სააღრიცხვო ჩანაწერი? როგორ მივიღოთ ის?
6. რა ელემენტებისაგან შედგება ელექტრონული შეტყობინება?
7. ”ქსელური ეტიკეტის” როგორი წესები იცით? ახსენით მათი არსი.
8. რა არის სადისკუსიო ჯგუფი (საფოსტო დაგზავნის ფორმით)? რაშია მსგავსება და განსხვავება ასეთ სადისკუსიო ჯგუფსა და ჩვეულებრივ საფოსტო მიმოწერას შორის?
9. რა არის მყისიერი შეტყობინებებით გაცვლა? რაშია მსგავსობა და განსხვავება ამ ტექნოლოგიასა და ელექტრონულ ფოსტას შორის?
10. რატომ ეძახიან **MSN, ICQ** და სხვა პროგრამებს ”ინტერნეტ-პეიჯერებს”, ხოლო მათთან მუშაობას - ”ურთიერთობას რეალურ დროში”?
11. რა იგულისხმება ფაილებთან საერთო შეღწევის ქვეშ? როგორია ძირითადი განსხვავება ამ სერვისებთან მუშაობასა და ინტერნეტიდან **FTP** პროტოკოლით ჩვეულებრივ ჩამოტვირთვას შორის?
12. რაში მდგომარეობს ინტერნეტიდან ინფორმაციის გამოყენების ლეგალურობის პრობლემა?

ს ა რ ჩ ე ვ ი