ქსელის არსი და უპირატესობა.

ქსელები არიან სისტემები რომლებიც ყალიბდებიან კავშირებით. ვებ გვერდებს რომლებიც საშუალებას იძლევიან ინდივიდუალური კავშირების დამყარებას ერთმანეთის გვერდებთან სოციალური ქსელები ეწოდებათ. გარკვეული იდეების ნაკრებს შეიძლება ეწოდებოდეს კონცეპტუალური ქსელი. კავშირებს რომლებიც გაგაჩნიათ თქვენს მეგობრებთან შეიძლება ეწოდოს თქვენი პირადი ქსელი.

ქსელები ყოველდღიურად გამოიყენება :

- ფოსტის გასაგზავნად.
- სატელეფონო სისტემისთვის.
- საზოგადოებრივი ტრანსპორტისათვის.
- კორპორაციული კომპიუტერული ქსელისთვის.
- ინტერნეტისათვის.

კომპიუტერები შეიძლება იყვნენ დაკავშირებულნი ერთამანეთთან რათა გაინაწილონ მონაცემები და რესურსები. ქსელი შეიძლება იყოს იმდენად მარტივი როგორც ორი კომპიუტერი ერთმანეთთან დაკავშირებული ერთი კაბელით და ისეთივე რთული როგორც ასეულობით კომპიუტერი დაკავშირებული მოწყობილობებთან რომლებიც ახდენენ მონაცემთა ნაკადების მართვას. შეთავსებულ (Converged) მონაცემთა ქსელები შეიძლება შეიცავდნენ როგორც ზოგადი მოხმარების კომპიუტერებს და სერვერებს ასევე მოწყობილობებს უფრო კონკრეტული დანიშნულებით როგორიც არის : პრინტერები, ტელეფონები, ტელევიზორები და სათამაშო კონსოლები.
ყველანაირი მონაცემთა, ხმოვანი, ვიდეო და შეთავსებული ქსელები ინაწილებელ ინფორმაციას და გამოიყენებენ სხვადასხვა მეთოდს რათა წარმართონ ინფორმაციული ნაკადები. ინფორმაცია ქსელში მოგზაურობს ერთი ადგილიდან მეორეში, ზოგჯერ სხვადახვა გზით, სწორ დანიშნულების ადგილზე მისაღწევად.
საზოგადოებრივი სატრანსპორტო სისტემა არის მსგავსი მონაცემთა ქსელისა. მსუბუქი ავტომობილები, სატვირთო მანქანები და სხვა მიმოსვლის საშუალებები არიან მსგავსნი ინფორმაციული შეტყობინებებისა რომლებიც მოგზაურობენ ქსელში. თითოული მძღოლი განსაზღვრავს საწყის წერტილს(წყარო) და საბოლოო წერტილს(დანიშნულება). ამ სისტემაში არსებობენ წესები, დასამუხრუჭებელი ნიშნები და შუქნიშნები რომლების აკონტროლებენ ნაკადებს წყაროდან დანიშნულების ადგილმდე.

კომპიუტერული მონაცემთა ქსელი არის კოლექცია ჰოსტებისა დაკავშირებული ერთმანეთთან ქსელური მოწყობილობების საშუალებით. ჰოსტი არის ნებისმიერი მოწყობილობა რომელიც აგზავნის და ღებულობს ინფორმაციას ქსელში. ჰოსტებთან დაკავშირებულ მოწყობილობებს ეწოდებათ პერიფერიული მოწყობილობები. მაგ.

პრინტერი დაკავშირებული ლეპტოპთან რომელიც არის ქსელში ჩართული. თუმცა თუ პრინტერი არის დაკავშირებული პირდაპირ ისეთ ქსელურ მოწყობილობასთან როგორიც არის კონცენტრატორი, კომუტატორი ან მარშრუტიზატორი, ამ შემთხვევაში პრინტერიც არის ჰოსტი.

კომპიუტერული ქსელები ფართოდ გამოიყენებიან ბიზნესში, სახლის პირობებში, სკოლებში და სამთავრობო დაწესებულებებში. მრავალი ქსელი ერთმანეთთან არის დაკავშირებული ინტერნეტის საშუალებით.

ქსელთან დაკავაშირება მრავალი ტიპის მოწყობილობას შუძლია:

- მაგიდის კომპიუტერებს
- ლეპტოპებს
- პრინტერებს
- სკანერებს
- ხელის(მინი) კომპიუტერებს(PDA)
- სმარტფონებს
- ფაილურ და საბეჭდ სერვერბს

ქსელში შეიძლება იყოს განაწილებული მრავალი ტიპის რესურსი :

- მომსახურეობები, როგორიც არის ამობეჭდვა და დასკანირება.
- მონაცემების შესანახი სივრცე და მოძრავი(removable) მოწყობილობები, როგორებიც არიან მყარი და ოპტიკური დისკები.
- პროგრამები, მონაცემთა ბაზები.

თქვენ შეგიძლიათ გამოიყენოთ ქსელი რათა მიწვდეთ ინფორმაციას შენახულს სხვა კომპიუტერზე, ამობეჭდოთ დოკუმენტები განაწილებული პრინტერების საშუალებით, და მოახდინოთ თქვენი კალენდრის სინქრონიზაცია კომპიუტერსა და სმარტფონს შორის.

ქსელური მოწყობილობები ურთიერთდაკავშირებლნი არიან სხვადასხვა ტიპის კავშირებით:

- სპილენძის კაბელებით - იყენებენ დენის სიგნალს მონაცემთა გადასაცემათ მოწყობილობებს შორის.
- ოპტიკურ-ბოჭკოვანი კაბელებით - იყენებს შუშას და პლასტმასის სადენს, ე.წ. ბოჭკოვანს, რათა გადასცეს სინათლის პულსების მეშვეობით ინფორმაცია.
- უკაბელო კავშირი - იყენებს რადიო სიგნალებს, ინფრაწითელ ტექნოლოგიას(ლაზერებს), ან სატელიტურ კავშირებს.

ქსელური პრინციპების გაგება

მარტო-მდგომი(stand-alone) კომპიუტერების გავრცელებამ გვიანდელ 1970-იან წლებში, მისცა საშუალება მომხმარებლებს, შეექმნათ დოკუმენტები, ცხრილები და სხვა სახის მონაცემები და შეენახათ ისინი მომავალში გამოსაყენებლად. იმის და მიუხედავათ რომ სახლის კომპიუტერებისთვის და პატარა ბიზნესისთვის ეს საკმარისი იყო, დიდ კორპორაციებს ესაჭიროებოდათ ინფორმაციის ცვლა ოფისებს

შორის და ზოგჯერ უფრო დიდ მანძილზეც. მარტო-მდგომი კომპიუტერები იყო არასაკმარისი შემდეგი მიზეზების გამო:

- მათი პატარა მყარი დისკები არ იყვნენ საკმარისნი.
- ბეჭდვისთვის თითოეულ კომპიუტერს უნდა ჰქონოდა თავისი პრინტერი.
- დოკუმენტების ცვლა იყო ძნელი, ხალხი იღლებოდა იმისგან რომ უნდა შეენახათ მონაცემები დისკეტაზე და შემდეგ წაეღოთ ეს დისკეტა დანიშნულების ადგილზე.
- არ არსებობდა email-ი იყო მხოლოდ ოფისთაშორისი ფოსტა, რომელიც არ იყო სანდო და ხშირად წერილები დაგვიანებით მიდიოდნენ დანიშნულების ადგილამდე.

ამ პრობლემების გადასაჭრელად წარმოიშვნენ ქსელები, ქსელი აკავშირებს ორ ან მეტ კომპიუტერს ერთმანეთთან რათა მათ შეძლონ ინფორმაციის ცვლა. მათი წარმატება ეს იყო რევოლუცია კომპიუტერებში და ბიზნესში. გაქრა მრავალი პრინტერის არსებობის საჭიროება ერთ ქსელში დაკავშირებულ ყველა კომპიუტერს ახლა შეუძლიათ ერთი პრინტერი გამოიყენონ, ქსელები გვათაზობენ საშუალებას რათა მოხდეს რესურსების გაზიარება, და შესაბამისად მუშაობის შესრულების გაუმჯობესებას და ახალი აპარატურასა და პროგრამულ უზრუნველყოფაში დანახარჯების შემცირებას.

ქსელის უპირატესობები :

- ქსელში საჭიროა ნაკლები პერიფერიული მოწყობილობა.

იმის გამო რომ ქსელში გვაქს შესაძლებლობა გავანაწილოთ რესურსები და მივცეთ დაშორებულ კომპიუტერებს წვდომა ჩვენს პერიფერიულ მოწყობილობებზე ამოვარდა მიზეზი რომლითაც თითოეულ კომპიუტერს შეიძლებოდა დასჭირვებოდა ცალკე პრინტერი თუ სკანერი ან სხვა მოწყობილობა.

- ქსელის მეშვეობით იზრდება კავშირგაბმულობის შესაძლებლობები

ქსელი გვაძლევს შესაძლებლობას სხვადასხვა ტიპის ხელსაწყოების გამოყენებისა კავშირგაბმულობისათვის იქნება ეს ფორუმები, ჩეთები, იმეილები, აუდიო თუ ვიდეო კავშირის საშუალებები, ამ ხელსაწყოების გამოყენებით ადამიანს შეუძლია დაუკავშირდეს თავის მეგობრებს, ოჯახის წევრებსა და კოლეგებს.

- ფაილების დუბლირებისაგან და დაზიანებისაგან დაცვა

სერვერი განაგებს ქსელურ რესურსებს, ის ინახავს მონაცემებს და ანაწილებს მათ მომხმარებლებს შორის, კონფიდენციალური მონაცემების დაცვა შეიძლება განხორციელდეს და მასზე წვდომა იყოს დაშვებული მხოლოდ განსაკუთრებული მომხმარებლებისათვის. ასევე შეიძლება იქნეს გამოყენებული ე.წ.” Document tracking software” პროგრამული უზრუნველყოფა რომელიც არ დართავს ნებას ადამიანებს გადააწერონ ან შეცვალონ ის ფაილები რომლებზეც წვდომა სხცებსაც აქვთ ამ მომენტში.

- ლიცენზირების უფრო დაბალი ფასი

პროგრამების ლიცენზიები ხშირად უფრო ძვირია ინდივიდუალურ მანქანებზე დასაყენებლად. ბევრი მწარმოებელი კომპანია იძლევა შემოთავაზებას ეგრედწოდებული „Site license“-ის რაც ნიშნავს რომ ერთი კონკრეტული ფასით ადამიანთა რაიმე ჯგუფს ან კომპანიის ყველა თანამშრომელს შუძლია ჰქონდეს წვდომა პროგრამაზე.

- ცენტრალიზირებული ადმინისტრირება

ცენტრალიზირებული ადმინისტრირება ამცირებს ხალხის რაოდენობას რომელიც არის საჭირო ქსელური მოწყობილობებისა და ქსელში მონაცემების სამართავად, რაც თავის მხრივ ამცირებს კომპანიის დანახარჯებს როგორც ფინანსურს ასევე დროითს, ინდივიდუალურ მომხმარებლებს არ სჭირდებათ თავიანთი მონაცემებისა და მოწყობილობების მართვა, ერთ ადმინსიტრატორს შეუიძლია მართოს მონაცემები, მოწყობილობები და მომხმარებლების დაშვების უფლებები ქსელში, მონაცემების რეზერვირებაც მარტივდება რადგან ისინი სრულად ინახებიან ერთ ცენტრალურ ადგილზე.

- რესურსების ეკონომია

სამუშაო შეიძლება იქნას განაწილებული მრავალ კომპიუტერს შორის და შედეგად არ მოხდეს არცერთი ცალკე აღებული კომპიუტერის გადათვირთვა

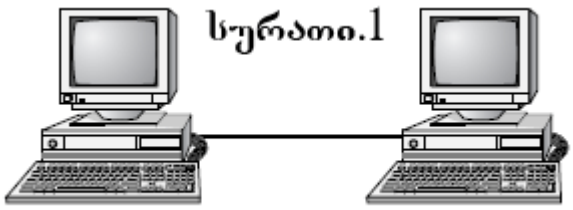
LAN-ის, WAN-ის, WLAN-ის, კლიენტ/სერვერ და peer-to-peer მოდელების აღწერა

LANs vs. WANs

ლოკალური ქსელები(LANs) იყვნენ შექმნილნი რათა მომხდარიყო დაკავშირება კომპიუტერების ერთი ოფისის შიგნით. ხოლო ფართო სივრცის ქსელები(WANs) იყვნენ შექმნილნი შენობების, ქალაქების, ქვეყნების და კონტინენტების დასაკავშირებლად ერთმანეთთან. დღევანდელ დღეს ლოკალური ქსელები არსებობენ მრავალ კომპანიაში, თუმცა ფართო სივრცის ქსელები ხდებიან, უფრო ფართოდ აღიარებულნი რადგანაც მეტი და მეტი კომპანია ფართოვდება უფრო დიდ და დიდ ტერიტორიაზე.

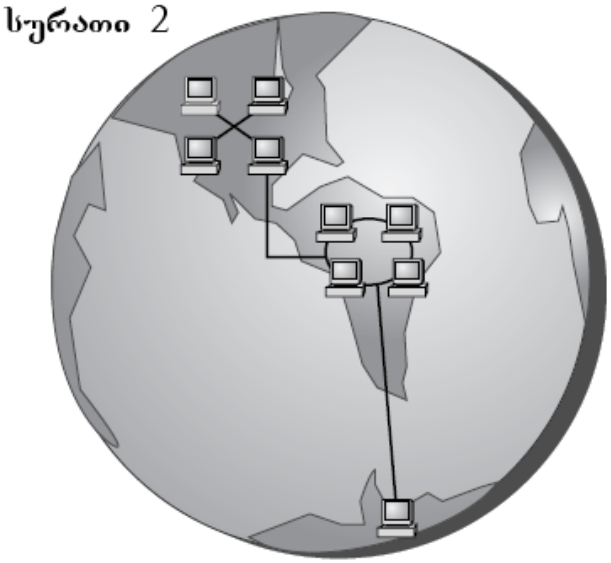
ლოკალური ქსელები (LANs)

პირველი ტიპის ლოკალური ქსელი ფირმა Novell-ის მიერ იქნა შექმნილი მას ShareNet-ი ერქვა, შეეძლო მაქსიმუმ 30 მომხმარებლისთვის (კომპიუტერისთვის) კავშირის უზრუნველყოფა (იხ. სურათი 1). თავდაპირველად ძალიან ცოტა პროგრამას შეეძლო ქსელის გამოყენება და ამ პროგრამებსაც არ შეეძლოთ ერთზე მეტი მომხმარებლის უზრუნველყოფა კავშირით (ამას ერქვა File Locking-ი) და ქსელიც მხოლოდ ერთ სართულზე განლაგებულ კომპიუტერებს აკავშირებდა, რადგან არ შეეძლო დიდ მანძილზე მუშაობა.



ფართო სივრცის ქსელები (WANs)

გადიოდა დრო, ქსელები ფართოვდებოდა და მოიცავდა ათასობით მომხმარებელს, კორპორაციები და მათი ფილიალები ქვეყნის სხვადასხვა კიდეში ისე შეთანხმებულად მუშაობდნენ, თითქოს ერთ მაგიდასთან მსხდარიყვნენ. მალე მსოფლიოში ყველამ დაინახა ახალი გზა, როგორ ეკეთებინა ერთი საქმე არა მხოლოდ რამდენიმე კილომეტრით დაცილებისას, არამედ სხვადასხვა მატერიკზეც. თუკი ლოკალური ქსელები ერთი შენობით იფარგლებიან, ფართო სივრცის ქსელები ერთმანეთს აკავშირებენ შენობებს, ქალაქებს, ქვეყნებს და კონტინენტებს (იხ. სურათი 2).



პირველადი ქსელური კომპონენტები

ახლა ქსელის აწყობა აღარ არის ისე მარტივი, როგორც ადრე იყო. დღესდღეობით ვეღარ ჩათვლი ორ ერთმანეთთან კაბელით დაკავშირებულ კომპიუტერს სრულყოფილ ქსელად, დღევანდელ ქსელს ესაჭიროება სამი ძირითადი კომპონენტი:

- სერვერი
- სამომხმარებლო/სამუშაო მანქანა

- რესურსები

არც ერთი ქსელი არ იქნება სრული ამ კომპონენტების გარეშე.

სერვერები

სერვერი არის ქსელის ბირთვი. ის აწვდის კავშირს რესურსებზე, რომლებიც საჭიროა მოქმედების შესასრულებლად. ეს რესურსი, რომელზეც კავშირი მიგვითითებს, შეიძლება იყოს განთავსებული ან სერვერზე, ან მომხმარებლის კომპიუტერზე. სერვერი არის ლიდერი, რომელიც აძლევს გეზს მომხმარებლთა კომპიუტერებს, რას უნდა მიმართონ რომ მიიღონ ის, რაც ესაჭიროებათ.

სერვერები ქსელებს რესურსების კონტროლის ცენტრალიზების საშუალებას აძლევენ და, შესაბამისად, ამცირებენ ადმინისტრირების სიძნელეებს. მათ შეუძლიათ გაანაწილონ პროცესები კომპიტერებს შორის ისე, რომ გააუმჯობესონ გამოთვლების სიჩქარე. მათ ასევე ფაილების ისე გნაწილება შეუძლიათ, რომ ერთი სერვერის გაფუჭების შემთხვევაშიყ ველა არ დაიკარგოს.

სერვერი ასრულებს რამდენიმე ამოცანას, მაგალითად, ქსელის მომხმარებლებს აწვდის ფაილებს, ემსახურება ამობეჭდვას და ა. შ. ფაილების მიმწოდებელ სერვერს ფაილური სერვერი ეწოდება, ამობეჭდვას რომელიც ემსახურება – მბეჭდავის სერვერი. სერვერები შეიძლება იყვნენ ერთი ან მრავალი დანიშნულების. მრავალი დანიშნულების სერვერი ერთდროულად შეიძლება იყოს ფაილურიც და მბეჭდავიც.

კიდევ ერთი განსხვავება, რომელიც არსებობს სერვერებს შორის – ზოგი არის მიძღვნილი (dedicated) და ზოგი – არამიძღვნილი (nondedicated).

მიძღვნილი სერვერი

მიძღვნილი სერვერი ასრულებს მხოლოდ სპეციფიკურ ამოცანებს და ემსახურება ქსელს. ამის გამო ნაკლებ რესურსს მოიხმარს იმ კომპიუტერისგან, რომელზეც არის განთავსებული. ეს დანაზოგი შესაძლოა გარდაიქმნეს ეფექტურობაში და მოახდინოს დადებითი ზეგავლენა ქსელის ფუნქციონირებაზე. ვებსერვერი არის მაგალითი მიძღვნილი სერვერისა ის ერთადერთი ფუნქციისთვისაა განკუთვნილი – რათა ვებგვერდების მომსახურებისთვის.

არამიძღვნილი სერვერი

არამიძღვნილი სერვერი არის განკუთვნილი რამდენიმე ქსელური მომსახურებისთვის და ლოკალური კავშირისთვის, არამიძღვნილი სერვერისგან უფრო მეტ ყოველდღიურ მოქნილობას ელიან მიძღვნილ სერვერთან შედარებით.

არამიძღვნილი სერვერი არა მარტო ქსელური ტრეფიკის მიმართვისთვის და ადმინისტრაციული ქმედებებისთვის უნდა იყოს გამოყოფილი, არამედ ზოგჯერ ტერმინალის მოვალეობაც უნდა შეასრულს ადმინისტრატორისთვის სხვა პროგრამებთან სამუშაოდ, ან ურუნველყოს ერთზე მეტი ქსელის მომსახურება. მაგალითად, არამიძღვნილ ვებსერვერს შეუძლია ემსახუროს ერთზე მეტ ვებგვერდს, მაშინ როცა მიძღვნილი ვებსერვერი ემსახურება მხოლოდ ერთს. არამიძღვნილ სერვერს ზოგიერთმა შესაძლოა არც კი უწოდოს სერვერი, იმიტომ რომ მას იმავდროულად შეუძლია იმუშაოს როგორც სამუშაო მანქანამაც. მაგალითად, სამუშაო ჯგუფის სერვერი თქვენს ოფისში არის არამიძღვნილი სერვერი. ის შეიძლება იყოს კომბინაცია ფაილური სერვერისა, მბეჭდავი სერვერისა და საფოსტო სერვერისა. თავისი არსიდან გამომდინარე, დამატებით, არამიძღვნილი სერვერი კარგად მუშაობს peer-to-peer გარემოში. ბევრ ქსელს მიერთებული აქვს ორივენაირი სერვერი, რათა გამოიყენოს ორივეს დადებითი მხარეები.

სამუშო მანქანები

სამუშო მანქანები ეწოდება კომპიუტერებს რომლებზეც ქსელის მომხმარებლები ასრულებენ თავიანთ სამუშაოს. ეს მანქანები ისეთივენი არიან, როგორებიც ჩვეულებრივი პერსონალური კომპიუტერები, მხოლოდ ერთი განსხვავებით – ისინი ჩართულნი არიან ქსელში, რომელიც მათ დამატებით რესურსებს სთავაზობს. ისინი ასევე ცნობილნი არიან როგორც სამომხმარებლო კომპიუტერები. როგორც სამომხმარებლო კომპიუტერებს მათ აქვთ საშუალება მიმართონ სერვერებს, რათა გამოიყენონ ქსელის რესურსები.

შესაძლებელია სამუშაო მანქანის კლიენტის კომპიუტერად გადაქცევა. ამისთვის ჯერ უნდა დავაყენოთ ქსელური ადაპტერი, ეს არის მოწყობილობა, რომელიც საშუალებას აძლევს კომპიუტერს მონაცემების გაცვლისა ქსელში; შემდეგ უნდა შევუერთოდ კაბელი, რომელიც დაკავშირებულია სხვა კომპიუტერთან ან კომპიუტერების ჯგუფთან. ამის შემდეგ უნდა დავაინსტალიროთ სპეციფიური პროგრამული უზრუნველყოფა, რომელიც კომპიუტერს სერვერთან დაკავშირების საშუალებას მისცემს და მოითხოვს რესურსებს მისგან. მას შემდეგ, რაც ყველაფერი ეს შესრულდება, კომპიუტერი ჩაერთვება ქსელში. სამომხმარებლო კომპიუტერს სერვერი საშუალებას მისცემს შეინახოს მეტი ინფორმაცია, ან გაცვალოს ინფორმაცია სხვა კომპიუტერებთან, რომლებიც ასევე არიან ჩართულნი ქსელში.

- სამომხმარებლო კომპიუტერებს შეუძლიათ შეინახონ მეტი ინფორმაცია იმიტომ, რომ ინფორმაციის შენახვა სერვერზე და ქსელში ჩართულ სხვა კომპიუტერებში
- მათ შეუძლიათ გამოიყენონ ის პროგრამები, რომლებიც შესაძლოა ძალიან დიდი ან რთული იყოს მათი კომპიუტერისთვის.

ქსელური რესურსები

ქსელში სერვერის ფუნქცია (დანიშნულება) რესურსებთან კავშირის დამყარებაა, ხოლო სამუშაო მანქანისა – ამ რესურსების გამოყენება; მაგრამ რა არის (რას წარმოადგენს) თავად ეს რესურსები? რესურსი არის ნებისმიერი მოწყობილობა, რომელიც შეიძლება იყოს გამოყენებული ქსელში. ასეთი მოწყობილობა ბევრია. აი უმნიშვნელოვანესების ჩამონათვალი:

- პრინტერები და სხვა პერიფერიული მოწყობილობები
- ფაილები
- პროგრამები
- მონაცემების შესანახი სივცრე

რადგან სერვერი შეიძლება განკუთვნილი იყოს მხოლოდ განსაზღვრული დანიშნულებისთვის, ის შეიძლება გამოვიყენოთ ყველა დიდი ფაილის შესანახად, რომლებზეც ხდება მუშაობა ყოველდღიურად, ამით ჩვენ გავათავისუფლებთ ადგილს სამომხმარებლო მანაქანაზე. ასევე ჩვენ შეგვიძლია ჩავწეროთ პროგრამები სერვერზე და გამოვიყენოთ მრავალ მანქანაზე მათზე დაინსტალირების გარეშე ქსელის კავშირის გამოყენებით.

პროგრამის ამ სახით გამოყენებას სჭირდება განსაკუთრებული შეთანხმება მწარმოებელთან. როგორც წესი, მწარმოებელი ფასს ადებს ლიცენზიას იმის მიხედვით, თუ რამდენი მომხმარებელი ეყოლება პროგრამას.

ქსელური ოპერაციული სისტემა
(NOS – Network Operation System)

პერსონალური კომპიუტერები გამოიყენებენ დისკურ ოპერაციულ სისტემას, რომელიც მართავს ფაილურ სისტემას და კავშირს პროგრამებისა მყარ დისკთან. ქსელები იყენებენ ქსელურ ოპერაციულ სისტემას, რათა გააკონტროლონ კავშირი რესურსებთან და მონაცემების ნაკადი ქსელში. იგი ჩაწერილია სერვერზე. ბევრი კომპანია სთავაზობს პროგრამულ უზრუნველყოფას ქსელის გასამართად. ყველაზე პოპულარული მაგალითები არიან: UNIX, ნოველის NetWere, Linux, მაიკროსოფტის Window's NT Server, Windows 2000 Server, Windows 2003 Server და Windows 2008 Server.

ლოკალური და გლობალური ქსელების ახალი ფუნქციების წყალობით, ქსელური ოპერატიული სისტემის გამოყენებით, ლონდონში თქვენს ოფისში მჯდომმა შეგიძლიათ დაბეჭდოთ დოკუმენტი პრინტერზე პარიზში, სათაო ოფისში, ან დისტანციიდან მართოთ შვებულებაში გასული თანამშრომლის კომპიუტერი.

ქსელურ რესურსებთან კავშირი

ახლა განვიხილოთ, თუ როგორ ხდება ქსელში რესურსებთან დაკავშირება. არსებობს ამის ორი ძირითადი მოდელი – peer-to-peer და მომხმარებელი სერვერი. გაითვალისწინეთ შემდეგი შეკითხვები:

- ორგანიზაციის ფართი
- უსაფრთხოების მასშტაბი
- რა პროგრამული და აპარეტურული უზრუნველყოფა ესაჭიროება რესურსს
- რამდენი ადმინისტრირება ესაჭიროება
- ღირებულება
- დააკმაყოფილებს თუ არა ეს რესურსი დღევანდელ და სამომავლო მოთხოვნებს
- გახდება თუ არა საჭირო თანამშრომლების ტრეინინგი

ქსელმა ეფექტურად და ნაყოფიერად რომ იმუშაოს, წინასწარ დიდი სამუშაოა ჩასატარებელი, ის დაკვირვებით და გონივრულად უნდა დაიგეგმოს, ისე რომ პასუხობდეს ზემოთ ჩამოთვლილ პუნქტებს.

პასუხები ამ კითხვაზე დაეხმარება დიზაინერს აირჩიოს რესურსების საჭირო მოდელი.

peer-to-peer ქსელები

ამ ქსელებში კომპიუტერები ერთდროულად მოქმედებენ ორი ფუნქციით – როგორც მომსახურების მიმწოდებლები და როგორც ისე მომთხოვნები. მაგალითი ამ ქსელისა ნაჩვენებია სურათზე.

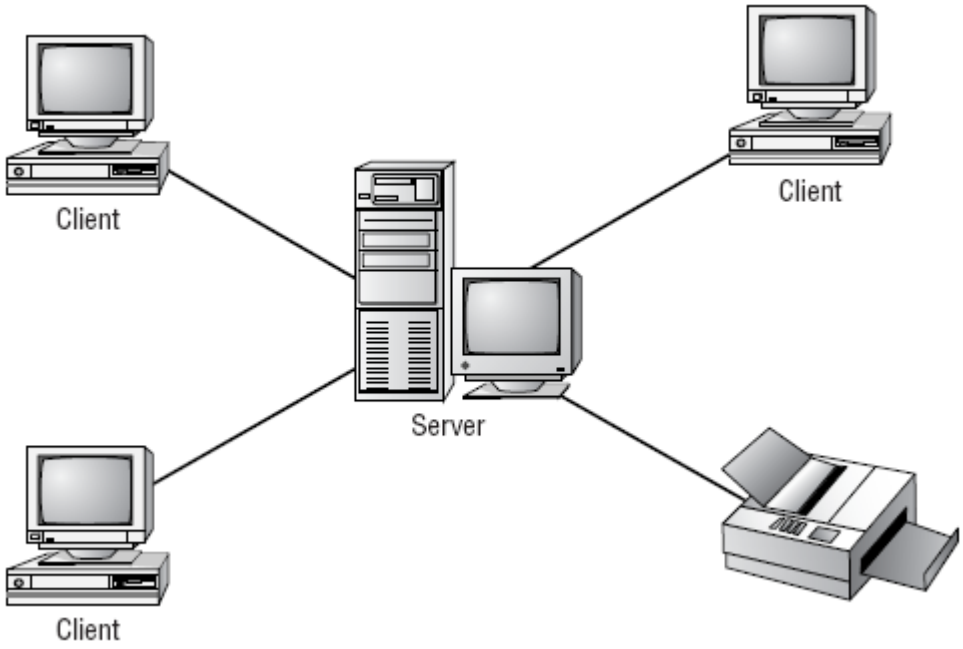
ეს მოდელი არის იდეალური პატარა, მარტივი და იაფი ქსელებისთვის, მისი აწყობა შეიძლება ძალიან სწრაფად. Windows 3.11, Windows 9x, Windows NT, Windows XP, Linux და Mac OS არიან პოპულარული ოპერაციული სისტემებია, რომლებიც გამართულად peer-to-peer მოდელით მუშაობენ.

ზოგადად რომ ვთქვათ, ამ მოდელში არ არის ცენტრალური ადმინისტრირება. თითოეულ მანქანას აქვს ინდივიდუალური კონტროლი რესურსებზე, რომელიც მხოლოდ მას ეკუთვნის და თითოეული სადგურის ადმინისტრირება უნდა მოხდეს ცალ-ცალკე. თუმცა სწორედ იმიტომ, რომ არ არსებობა ცენტრალური ადმინისტრირება, რთულდება მისი მართვა, ამავე მიზეზით აქ მეტი რისკი ემუქრება უსაფრთხოებას.

როგორც წესი, ამ მოდელს ირჩევენ პატარა კომპანიებისთვის, რომლებიც არც მომავალში ელოდებიან დიდ ზრდას. მაგრამ კომპანიებმა, რომლებიც ფიქრობენ გაფართოებას, ეს მოდელი არ უნდა აირჩიონ.

რესურსების მოდელი
მომხმარებელი-სერვერი (client-server)

მოდელი მომხმარებელი-სერვერი ასევე ცნობილია სახელწოდებით სერვერზე დაფუძნებული მოდელი (Server-based). დიდ ქსელებში ეს სერვისი უკეთესია (ვთქვათ, 10-ზე მეტი კომპიუტერის დროს შემთხვევაში). მათ ესაჭიროებათ უფრო მეტად უსაფრთხო გარემო. ეს მოდელი იყენებს მიძღვნილ, ცენტრალიზებულ სერვერს. მართვის ყველა ფუნქცია და განაწილება (ფაილების, პროგრამების, მონაცემების შესანახი სივრცის) ხორციელდება ამ წერტილიდან. ეს ხდის უფრო ადვილს რესურსების განაწილებას, მონაცემების რეზერვირებას, და მხარდაჭერა თითქმის შეუზღუდავი რაოდენობით მომხმარებლებისა. უფრო საიმედოა ამ მოდელის უსაფრთხოება. თუმცა სერვერს ესაჭიროება მეტი აპარატურული უზრუნველყოფა, ვიდრე ჩვეულებრივ სამუშაო მანქანას, რომელსაც ვიყენებთ peer-to-peer მოდელში. დამატებით მას კიდევ ესაჭიროება სპეციალიზებული პროგრამული უზრუნველყოფა (ქსელური ოპერაციული სისტემა), რათა ვმართოთ სერვერის როლი გარემოში. სერვერის და ქსელური ოპერაციული სისტემის ფასთან თუ გავითვალისწინებთ, სერვერზე დაფუძნებული მოდელი უფრო ძვირი დაჯდება peer-to-peer მოდელთან შედარებით. თუმცა დიდი ქსელებისთვის ეს ერთადერთი არჩევანია. სერვერზე დაფუძნებული ქსელის მოდელის მაგალითი იხილეთ სურათზე.



ეს მოდელი შექმნილია დიდი და მზარდი ორგანიზაციების მოთხოვნების შესაბამისად.

სერვერზე დაფუძნებული ქსელები იძლევიან საშუალებას, რომ ქსელს შეუზღუდავი რაოდენობის რესურსები და მომხმარებლები დავამატოთ. იმისდა მიუხედავათ, რომ აპარატურული უზრუნველყოფა არის უფრო ძვირი, ცენტრალიზირებული მართვა დროის დაზოგვის საშუალებას იძლევა. ამ მოდელის მართვას მხოლოდ რამდენი ადმინისტრატორის ტრეინინგი დაჭირდება. მისი მომხმარებლები პასუხისმგებელნი არიან მხოლოდ თავიანთ სამუშაო გარემოზე.

რომელი მოდელიც არ უნდა აირჩიოთ, დიდი გულისყურით მოეკიდეთ მის დაგეგმვას, ამისთვის არც დრო დაინანოთ, არც ხარჯი, თუ არ გინდათ რომ მომავალში აღმოაჩინოთ, რომ თქვენმა ქსელმა ვერ უპასუხა კომპანიის მოთხოვნებს. ახლანდელი ხარჯი სამომავლო დანაზოგის განმაპირობებელი იქნება.

დამისამართება, გამტარუნარიანობა და მონაცემთა გადაცემა. დინამიურად ჰოსტის დაკონფიგურირების პროტოკოლი

გამტარუნარიანობა (Bandwidth)

დროის მოცემულ მომენტში მონაცემების გადაცემის მაქსიმალურ მნიშვნელობას გამტარუნარიანობა ეწოდება. როდესაც მონაცემი იგზავნება ქსელში, ხდება მისი დაყოფა პატარ-

პატარა ნაწილებად, რომლებსაც პაკეტები ეწოდება. თითოეულ პაკეტს აქვს თავისი თავსართი. ეს თავსართი არის პაკეტზე წამძღვარებული ინფორმაცია, რომელიც გვაუწყებს ამ პაკეტის წყაროსა და დანიშნულების ადგილს, ასევე თუ როგორ უნდა მოხდეს ამ პაკეტების დალაგება, როდესაც ისინი მიაღწევენ დაშინულების ადგილს. გამტარუნარიანობა განსაზღვრავს, თუ რამდენი ინფორმაციის გადაცემა შეგვიძლია.

გამტარუნარიანობა გაიზომება ბიტებით წამში და ჩამოთვლილთაგან რომელიმე აღმნიშველით შეიძლება შეგვხდეს :

- bps – ბიტი/წამში
- Kbps – კილობიტი/წამში
- Mbps – მეგაბიტი/წამში

შენიშვნა: 8 ბიტი = 1 ბაიტს. ბიტის აბრევიატურა პატარა b ასოთი ხდება ხოლო ბაიტის – მთავრული B ასოთი. ერთი MBps უდრის დაახლოებით 8 Mbps.

მონაცემთა გადაცემა ქსელში ხდება სამი მეთოდით: simplex, half-duplex ან full-duplex.

simplex

ეს მეთოდი ასევე ცნობილია, როგორც ცალმხრივი, მისი მაგალითია სატელევიზიო სიგნალი, რომელიც მოდის ტელევიზორებში სადგურიდან.

half-duplex

ნახევარ-დუპლექსური გადაცემა მონაცემების ხდება მაშინ, როდესაც გადაცემა მიმდინარეობს ჯერ ერთ მხარეს, ხოლო შემდგომ მეორე მხარეს. ანუ მონაცემთა ნაკადს შეუძლია იმოგზაუროს ორივე მხარეს, თუმცა არა ერთდროულად. მაგალითი ასეთი კავშირგაბმულობისა არის რაცია (walkie-talkie), როდესაც ერთ-ერთი მოსაუბრე აჭერს ღილაკს და იწყებს ლაპარაკს, მას არ ესმის მეორე მოსაუბრის, ხოლო თუ ორივემ ერთდროულად გადაწყვიტა საუბარი. ვერცერთი სიგნალი ვერ მივა დანიშნულების ადგილზე.

full-duplex

სრულ-დუპლექსური მონაცემთა გადაცემა ხდება მაშინ, როდესაც ინფორმაცია ერთდროულად მოგზაურობს ორივე მიმართულებით, მაგრამ ამის და მიუხედავად გამტარუნარიანობა განისაზღვრება ერთ მხარეს მიღწევადი გამტარობით, 100Mbps სიჩქარით. სრულ-დუპლექსში გააჩნია 100Mbps გამტარუნარიანობა. სატელეფონო საუბარი არის მაგალითი ასეთი კავშირგაბმულობისა – ორივე მოსაუბრეს ერთდროულად შეუძლია ლაპარაკიც და მოსმენაც. სრული დუპლექსის ტექნოლოგია აუმჯობესებს ქსელის მუშაობის უნარიანობას, რადგანაც

გვიჩნდება საუშუალება გავაგზავნოთ და მივიღოთ მონაცემები ერთდროულად. Broadband ტექნოლოგიები საშუალებას იძლევა ორმა სიგნალმა ერთ სადენზე ერთდროულად იმოძრაოს. ასეთი ტექნოლოგიების მაგალითია DSL და კაბელური კავშირი, ისინი მუშაობენ სრულ-დუპლექსურ რეჟიმში. მაგალითად, DSL-ის შემთხვევაში ერთდროულად შეგვიძლია მონცამები გადმოვწეროთ დისტანციაზე მყოფი კომპიუტერიდან და ვილაპარაკოთ კიდეც ტელეფონით.

IP მისამართი არის ციფრების მნიშვნელობა, რომელიც გამოიყენება მოწყობილობის იდენტიფიცირებისათვის ქსელში. თითოეულ მოწყობილობას უნდა ჰქონდეს ერთ ქსელში უნიკალური IP მისამართი რათა შეძლოს კავშირის დამყარება სხვა მოწყობილობებთან. როგორც უკვე ვახსენეთ, ჰოსტი არის მოწყობილობა, რომელიც აგზავნის და იღებს ინფორმაციას ქსელში. ხოლო ქსელური მოწყობილობები ის მოწყობილობებია, რომლებიც გადააადგილებენ ამ ინფორმაციას ქსელში, ესენია კონცენტრატორები, კომუტატორები და მარშრუტიზატორები. ლოკალურ ქსელში თითოეულ ჰოსტს და ქსელურ მოწყობილობას უნდა ჰქონდეს თავისი IP მისამართი საერთო ქსელიდან, რათა დაამყარონ კავშირი ერთმანეთთან.

პიროვნების სახელი და თითის ანაბეჭდები, როგორც წესი, უცვლელია, ისინი გვაძლევენ საშუალებას მოვახდინოთ ამა თუ იმ პიროვნების იდენტიფიცირების, ხოლო საფოსტო მისამართი გვატყობინებს, თუ სად ცხოვრობს ადამიანი ამჟამად. ეს მისამართი შეიძლება შეიცვალოს. ჰოსტს აქვს ფიზიკური მისამართი (MAC), რომელიც უცვლელია, იმისდა მიუხედავად თუ სად იქნება ჰოსტი განთავსებული, შესაბამისად, შეგვიძლია ის შევადაროთ ადამიანის სახელსა და თითის ანაბეჭდებს, რომლებიც არ იცვლება იმისდა მიხედვით, თუ სად დასახლდება ადამიანი.

IP მისამართი კი ჰგავს ადამიანის საფოსტო მისამართს, ის არის ცნობილი როგორც ლოგიკური მისამართი, რადგანაც მისი მინიჭება ხდება ლოგიკით, იმისდა მიხედვით, თუ სად მდებარეობს ჰოსტი. IP მისამართი ან ქსელის მისამართი არის დამოკიდებული ლოკალურ ქსელზე და, როგორც წესი, ქსელური ადმინისტრატორის მიერ არის მინიჭებული. ეს წააგავს შემთხვევას, როდესაც ქუჩას სახელს ქალაქის, სოფლის ან უბნის ლოგიკური მნიშვნელობიდან გამომდინარე არქმევენ.

IP მისამართი შედგება 32 ორობითი ბიტისაგან (1-იანები და 0-იანები). ადამიანებისათვის ძალიან რთულია წაიკითხონ ორობითი მისამართი და აქედან გამომდინარე, 32 ბიტი არის დაყოფილი ოთხ 8-ბიტიან ჯგუფად, რომლებსაც ეწოდებათ ოქტეტები. თუმცა ამ ფორმატშიც ინფორმაცია რთული წასაკითხი და დასაწერია ადამიანებისათვის, შესაბამისად, თითოეული ოქტეტის შიგთავსი

გამოსახულია ათობითი მნიშვნელობით და გამოყოფილი წერტილით, ამ ფორმატს ეწოდება dotted-decimal notation. როდესაც ხდება ჰოსტზე IP მისამართის კონფიგურირება, მისი შეყვანა ხდება როგორც ათობითი მნიშვნელობა დაყოფილი წერტილებით, მაგ., 192.168.1.5. წარმოიდგინეთ, რომ დაგჭირვებოდათ შეგეყვანათ 32 ბიტი ორობითი მნიშვნელობა ზემოთ ნახსენები მისამართისა, იქნებოდა: 11000000101010000000000100000101. ერთი ბიტის არასწორად შეყვანის შემთხვევაში მისამართი არასწორი იქნებოდა და დიდი ალბათობა, რომ კავშირი არ დამყარებულიყო ქსელთან.

ლოგიკური 32-ბიტიანი IP მისამართი არის იერარქიული და შედგება ორი ნაწილისაგან. პირველი ნაწილი ქსელის იდენტიფიცირებას ახდენს, ხოლო მეორე – ჰოსტის იდენტიფიცირებას ამ ქსელზე. IP მისამართში ორივე ნაწილი აუცილებელია. მაგ., თუ ჰოსტს აქვს IP მისამართი 192.168.18.57, პირველი სამი ოქტეტი ახდენს ქსელის იდენტიფიცირებას, ხოლო უკანასკნელი, 57, ჰოსტის – იდენტიფიცირებას. ამას ეწოდება იერარქიული დამისამართება, იმიტომ რომ ქსელური ნაწილი გვაუწყებს, თუ რომელ ქსელში არის განთავსებული ჰოსტის უნიკალური მისამართი. მარშრუტიზატორებს ესაჭიროებათ მხოლოდ იმის ცოდნა, თუ როგორ მიიღწევა თითოეული ქსელი და არა თითოეული ჰოსტი ამ ქსელში.

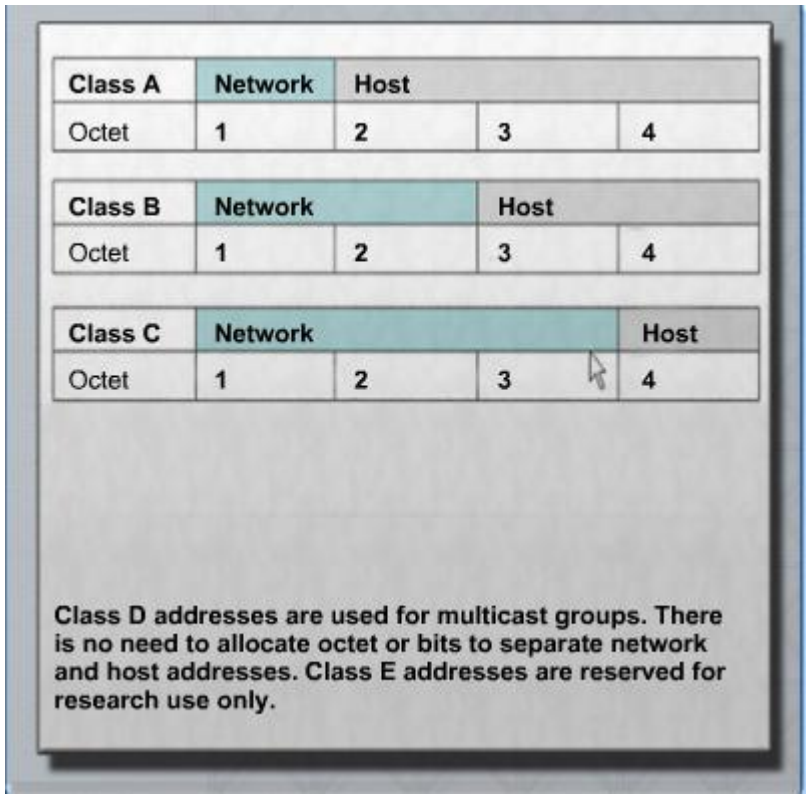
IP მისამართები დაყოფილნი არიან A, B, C, D, E კლასებად:

- Class A – დიდი ქსელები, გამოიყენება დიდი კომპანიების მიერ და ზოგიერთი ქვეყნის მიერ
- Class B – საშუალო ზომის ქსელები, გამოიყენება უნივერსიტეტების მიერ
- Class C – პატარა ქსელები, გამოიყენება ინტერნეტპროვაიდერების მიერ მომხმარებელთათვის მისამართების გამოსაყოფად
- Class D – განკუთვნილია განსაკუთრებული დანისნულების, multicasting-ისათვის
- Class E – გამოიყენება ექსპერიმენტებისათვის

ქვექსელის ნიღაბი

ქვექსელის ნიღაბი გამოიყენება IP მისამართის ქსელის და ჰოსტის ნაწილის ერთმანეთისაგან გასარჩევად. ისევე როგორც IP მისამართი, ქვექსელის ნიღაბიც 32-ბიტიანია და გამოისახება როგორც ათობითი რიცხვი დაყოფილი ოთხ ოქტეტად.

როგორც წესი, ლოკალურ ქსელში ყველა ჰოსტს ერთი და იმავე ქვექსელის ნიღაბი აქვს.



- 255.0.0.0 – Class A გვაუწყებს, რომ პირველი ოქტეტი IP მისამართისა არის ქსელის ნაწილი
- 255.255.0.0 – Class B გვაუწყებს, რომ პირველი ორი ოქტეტი IP მისამართისა არის ქსელის ნაწილი
- 255.255.255.0 – Class C გვაუწყებს, რომ პირველი სამი ოქტეტი IP მისამართისა არის ქსელის ნაწილი

თუ ორგანიზაციას ეკუთვნის ერთი B კლასის ქსელი, მაგრამ უნდა გამოიყენოს ის ოთხ ლოკალურ ქსელში, მან უნდა დაანაწევროს ეს B კლასის ქსელი ოთხ უფრო მცირე ნაწილად. Subnetting, ანუ ქვექსელებად დაჭრა არის ქსელის ლოგიკურად დანაწევრების საშუალება. ქსელის გამოცდილი ადმინისტრატორი ახდენს ამ გამოთვლებს და შემდგომ შესაძლებელი იქნება ამ ოთხ ქსელში ჰოსტებზე IP მისამართების კონფიგურირება.

ხელოვნური კონფიგურირება

ქსელში, რომელშიც არის მცირე რაოდენობის ჰოსტები, ადვილია IP მისამართის ხელით დაკონფიგურირება თითოეული მოწყობილობისათვის. ქსელის ადმინისტრატორმა უნდა მიანიჭოს მათ მისამართები, მას უნდა შეეძლოს შესაბამისი მისამართის მინიჭება კონკრეტული ქსელისათვის. IP მისამართი, რომელიც კონფიგურირდება, უნიკალური უნდა იყოს თითოეული ჰოსტისათვის ერთ ქსელში, ან ქვექსელში.

იმისთვის, რომ ხელით მიანიჭოთ IP მისამართი ჰოსტს, გადადით TCP/IP პარამეტრებში ქსელური ადაპტერის Properties-იდან. ქსელური ადაპტერი არის მოწყობილობა, რომელიც აკავშირებს კომპიუტერს ქსელთან. მას აქვს მისამართი, რომელსაც ეწოდება Media Access Control (MAC) მისამართი. როგორც უკვე ვთქვით, IP მისამართი არის ლოგიკური მისამართი, რომელსაც ანიჭებს ადმინისტრტორი, ხოლო ფიზიკური (MAC) მისამართი ჩაწერილია ქარხნულად და მისი შეცვლა ჩვენი ქსელის ადაპტერში არ შეიძლება, განსხვავებით IP მისამართისაგან, რომლის შეცვლაც შესაძლებელია.

მთავარი განსხვავება IP მისამართსა და ფიზიკურ მისამართს შორის არის ის, რომ ფიზიკური მისამართი გამოიყენება ლოკალურ ქსელში კადრების კომუტაციის დროს, ხოლო IP მისამართი გამოიყენება ჩვენი ქსელიდან პაკეტების მარშრუტიზირების დროს. კადრი არის მონაცემთა პაკეტი, მას ემატება დამისამართების ინფორმაცია თავსა და ბოლოში მას შემდგომ, რაც კადრი მოხვდება საჭირო ქსელში. მისი დანიშნულების ადგილამდე კომუტაცია მოხდება ფიზიკური მისამართის გამოყენებით.

თუ ლოკალური ქსელი მრავალი კომპიუტერისაგან შედგება, მაშინ ხელით კონფიგურირება თითოეული IP მისამართისა ჰოსტებზე დიდ დროს წაიღებს, შესაბამისად, დროის ეკონომიის მიზნით, შეგვიძლია გამოვიყენოთ ჰოსტების დინამიურად კონფიგურირების პროტოკოლი (DHCP) და სერვერი ავტომატიურად დაარიგებს IP მისამართებს, რაც დიდად გააადვილებს ამ პროცესს.

პროტოკოლები

პროტოკოლი (Protocol) არის იმ პროცედურების და წესების ერთობლიობა, რომელთა საშუალებითაც ხორციელდება თკავშირი კომპიუტერებს შორის. ერთდროულად შეიძლება მუშაობდეს რამდენიმე პროტოკოლი. მაშინ ამბობენ რომ ისინი ქმნიან პროტოკოლების სტეკს.

პროტოკოლების მთავარი ფუნქციებია:

- შეცდომების ამოცნობა
- მონაცემების შეკუმშვა (კომპრესაცია)
- გადაწყვეტილების მიღება მონაცემთა გადაცემის მეთოდის არჩევა
- მონცამეთა დამისამართება

თუმცაღა ბევრად მეტი პროტოკოლი არსებობს, მაგრამ ძირითადები წარმოდგენილია ცხრილში

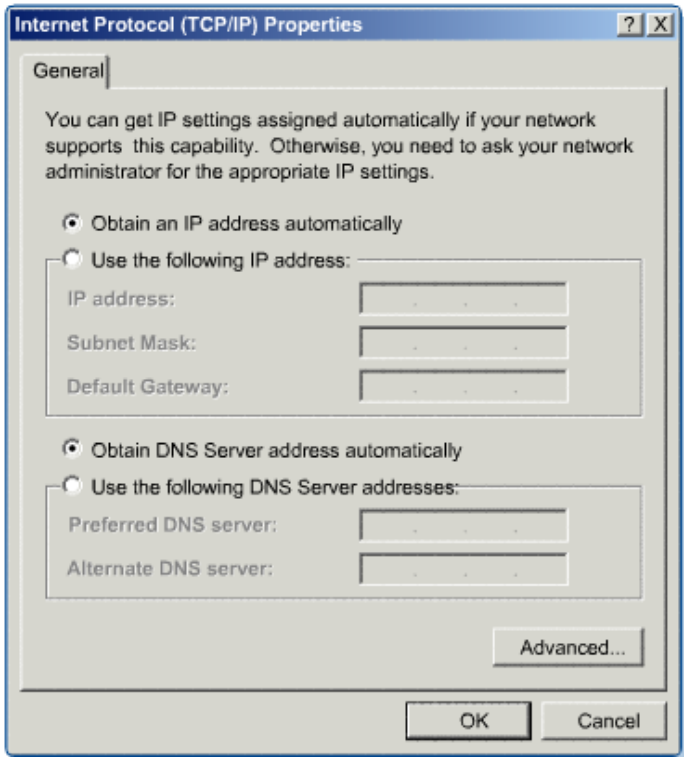
პროტოკოლი	აღწერა
TCP/IP	მონაცემთა გადასაცემად ინტერნეტში გამოიყენება
NETBEU\NETBIOS	მცირე, სწრაფი პროტოკოლი, შექმნილია სამუშაო ჯგუფებისათვის რომელთაც არ სჭირდებათ ინტერნეტთან წვდომა.
IPX/SPX	მონაცემთა გადასაცემად ნოველის Netware ქსელში გამოიყენება
HTTP/HTTPS	განსაზღვრავს, როგორ უნდა მოხდეს ფაილების მიმოსვლა ვებში
FTP	ფაილების გადემის პროტოკოლი
SSH	კომპიუტერების უსაფრთხოდ დაკავშირებისათვის გამოიყენება
TELNET	ბრძანებათა-ველის კავშირის დასამყარებლად დისტანციაზე მყოფ კომპიუტერთან
POP	საფოსტო პროტოკოლი, წერილების გადმოსაწერად სერვერიდან

IMAP	საფოსტო პროტოკოლი, წერილების გადმოსაწერად სერვერიდან
SMTP	საფოსტო პროტოკოლი, წერილების გასაგზავნად

ჰოსტის დინამურად კონფიგურირების პროტოკოლი(DHCP)

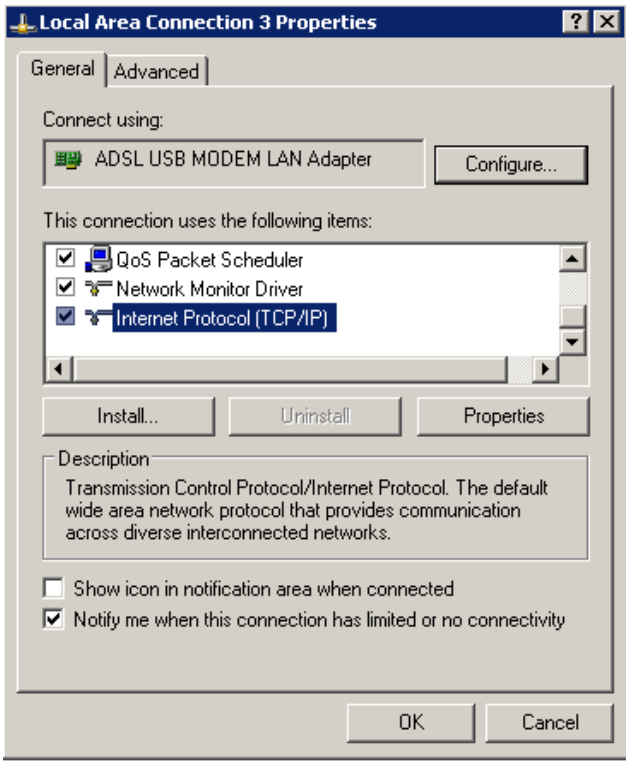
ეს არის პროგრამული უტილიტა რომელიც გამოიყენება ქსელური მოწყობილობებისათვის დინამიურად მისამართის მისანიჭებლად. ეს დინამიური პროცესი აღმოფხვრის საჭიროებას რომ ხელით მივანიჭოთ მისამართი ჩვენს მოწყობილობებს. DHCP სერვერის აწყობა შეიძლება და კომპიუტერების კონფიგურირება ავტომატიურად მისამართის შეკვეთის რეჟიმში. სერვერს აქვს სია მისამართებისა, რომელთა დარიგებაც შეუძლია და მართავს პროცესს იმისათვის, რომ ქსელში არსებულმა ყველა მოწყობილობამ მიიღოს ინდივიდუალური მისამართი, თითოეული მისამართის გამოყოფა ხდება გარკვეული დროით მას შემდეგ რაც ეს დრო ამოიწურება ხდება მისამართის მინიჭება ნებისმიერ ახალ მოწყობილობაზე რომელიც ჩაერთვება ქსელში. ეს არის სია ინფორმაციის რომლის მინიჭებაც შეუძლია DHCP სერვერს :

- IP address - აიპი მისამართი
- Subnet mask - ქვექსელის ნიღაბი
- Default Gateway – ”შლუზი”(კარიბჭე სხვა ქსელებში)
- Domain Name System Server Address- დომენური სახელების სისტემის სერვერის მისამართი



ასე გამოიყურება რეჟიმი როდესაც ავტომატიურად ხდება კონფიგურირება კომპიუტერის რომელზეც აყენია Windows-ი.

ამ ფანჯრის გასახსნელად შედით Control Panel/Network Connections/Local Area Network-ზე გამოიძახეთ დამატებითი მენიუ და აირჩიეთ Properties და გამოსულ ფანჯარაში აირჩიეთ TCP/IP და დააჭირეთ Properties.



თუ თქვენი კომპიუტერი ავტომატურად ვერ იღებს მისამართს სერვერიდან, მაშინ Windows-ი მიანიჭებს ავტომატიურად 169,254,0,0-დან 169,254,255,255-მდე. ამ ფუნქციას ეწოდება Automatic Private IP Addressing (APIPA). ის მაინც გააგრძელებს მოთხოვნების გაგზავნას სერვერთან IP მისამართისა იმისდა მიუხედავად, რომ უკვე ექნება მისამართი ზემოთ ხსენებული სიიდან.

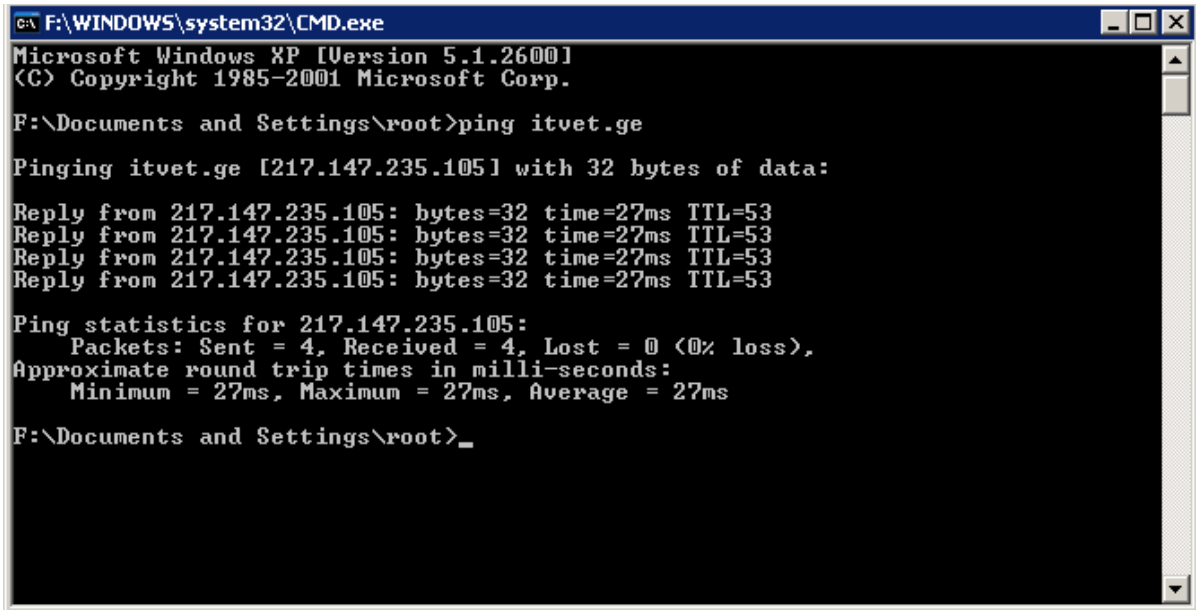
ICMP პროტოკოლი

Internet Control Message Protocol-ს მოწყობილობები იყენებენ კომპიუტერებისა და სერვერბისთვის საკონტროლო შეტყობინებებისა და შეცდომებზე ინფორმაციის გასაგზავნად. მას რამდენიმე ფუნქცია აქვს:

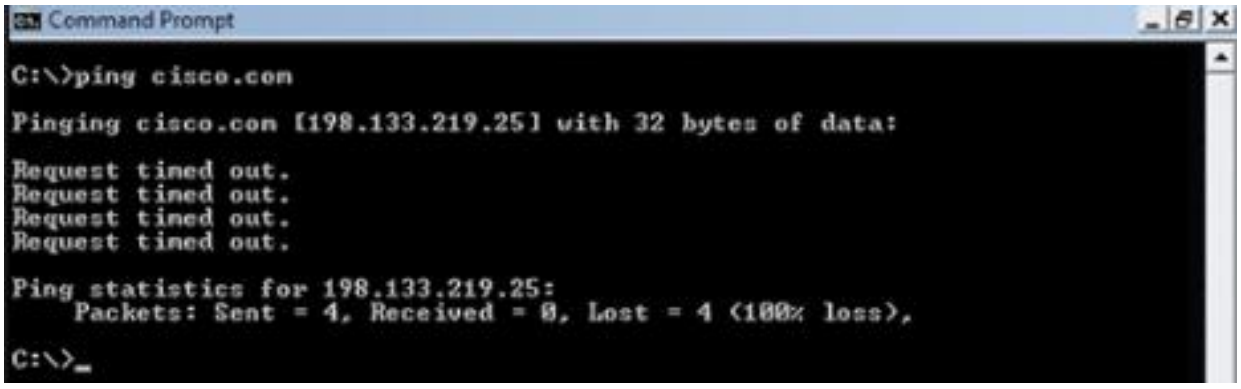
- ქსელში არსებული შეცდომების შეტყობეინება
- შეტყობინება ქსელის გადატვირთვის შესახებ
- დიაგნოსტიკისათვის

„პინგი“ (ბრძანება. პროგრამა) ხშირად გამოიყენება კავშირის გასასინჯად ორ კომპიუტერს შორის. ის გამოიყენება ბრძანებათა ველიდან (აკრიფეთ Ping /? დამატებითი ინფორმაციისათვის

ბრძანების შესახებ.) თქვენ შეგიძლიათ და პინგოთ IP მისამართი და შეამოწმოთ, არის თუ არა მასთან კავშირი. პინგის მუშაობის პრინციპი არის ძალიან მარტივი, ის აგზავნის მოთხოვნას დისტანციაზე მყოფ კომპიუტერთან პასუხის შესახებ და როდესაც კომპიუტერი იღებს ამ მოთხოვს, ის ასრულებს მას და პასუხს სცემს წყაროს. ხოლო თუ მოთხოვნა ვერ მივა დანიშნულების ადგილამდე, შესაბამისად, არ იქნება პასუხი და ჩვენ გამოგვივა შეტყობინება დროის ამოწურვის შესახებ (Request Timed Out). სურათზე მოცემულია წარმატებული პინგის მაგალითი:



როგორც მაგალითიდან შეამჩნევდით, დაპინგვა არა მარტო IP მისამართის შეიძლება, არამედ დომენური სახელისაც.



ამ სურათზე კი მოცემულია წარუმატებელი პინგის შედეგი:

ქსელური მოწყობილობების სახელები, დანიშნულება და მახასიათებლები
ქსელური კაბელების სახელები, დანიშნულება და მახასიათებლები
კონცენტრატორი

პაკეტი განკუთვნილი, ამიტომ შემოსულ პაკეტებს უგზავნის ყველა კომპიუტერს, მიუხედავად იმისა, არის თუ არა მისთვის განკუთვნილი. ამის გამო ხდება ქსელში მოძრაობის, იგივე ტრაფიკის (Trafic), გადატვირთვა. კომპიუტერთა რაოდენობის მიხედვით ჰაბს შეიძლება ჰქონდეს 6, 12 და მეტი RJ 45 პორტი. თუ ეს შესაერთებლები არ გვყოფნის, შეგვიძლია ორი ჰაბის ერთდროული ჩართვა, რისთვისაც გამოიყენება ასეთივე ტიპის შესაერთებელი Uplink Port. იმავე UTP კაბელით ამ პორტებით ვაერთებთ ჰაბებს ერთმანეთთან და ისინი ქსელის სრულუფლებიანი წევრები ხდებიან, ანუ პირველ ჰაბში შემოსული მონაცემთა

პაკეტები მიეწოდება უკლებლივ ყველა კომპიუტერს როგორც პირველ, ასევე მეორე ჰაბში მიერთებულებს. ამ დროს ორ ჰაბს შორის შემაერთებელი კაბელი ძალიან იტვირთება.

წარმოვიდგინოთ 12 კომპიუტერი მიერთებული ერთ ჰაბზე და ამდენივე მეორეზე. პირველ ჰაბზე მიერთებულმა რომელიმე კომპიუტერმა რომ გაუგზავნოს პაკეტი ამავე ჰაბზე მიერთებულ სხვა კომპიუტერს, ეს პაკეტი გაეგზავნება მეორე ჰაბზე მიერთებულ 12-ივე კომპიუტერსაც, თუმცა ეს მონაცემები იქ არავის არ სჭირდება. ჰაბების შემაერთებელი კაბელი მეტისმეტად გადაიტვირთება და თუ მეორე მხრიდანაც მოედინება მონაცემები, შეიძლება მოძრაობა შეფერხდეს, ამ მოვლენას კოლიზია ჰქვია. ტრაფიკის განტვირთვისათვის გამოიყენება მოწყობილობა ბრიჯი (Bridge), რომელიც დგება ჰაბებს შორის კაბელზე. იგი შიფრავს პაკეტების თავსართში მითითებულ მისამართებს და იმის მიხედვით ანაწილებს მათ, რომელი ჰაბისთვისაცაა განკუთვნილი. ანუ ბრიჯი ქსელს ყოფს ე.წ. ორ საკოლიზიო დომენად და ნაწილობრივ განტვირთავს ტრაფიკს.

UTP კაბელით მონაცემთა გადაცემა შესაძლებელია 100 მტრამდე მანძილზე, უფრო შორს სიგნალები ისე სუსტდება, რომ ჰაბსაც არ შეუძლია მათი გაძლიერება. ამიტომ შორ

მანძილზე კაბელის გაჭიმვის შემთხვევაში საჭიროა ყოველ 100 მეტრში ჩავაყენოთ ჰაბი, თუმცა 500 მეტრზე შორს ამ კაბელის გამოყენება აღარ შეიძლება, ანუ ერთ გზაზე შეგვიძლია ჩავაყენოთ მხოლოდ 4 ჰაბი.

კომუტატორი

ჰაბისაგან განსხვავებით კომუტატორს შეუძლია პაკეტის თავსართში ამოიკითხოს MAC მისამართი, გაარკვიოს რომელი ქსელის კარტას ეკუთვნის პაკეტი და გაუგზავნის ადრესატ კომპიუტერს. ანუ სვიჩი მონაცემებს უგზავნის იმ კომპიუტერს, რომლისთვისაცაა განკუთვნილი. არსებობს ორი სახის სვიჩი – გამჭოლი და შემნახველი. გამჭოლი სვიჩები ჩვეულებრივ მიიღებენ პაკეტებს და გადაუგზავნიან შესაბამის კომპიუტერებს, ხოლო შემნახველ სვიჩებს აქვთ საკუთარი პროცესორი და მეხსიერების ბუფერი. ისინი აგროვებენ შემოსულ პაკეტებს, ამოწმებენ შეცდომებს, შემდეგ ისევ ანაწილებენ და გადასცემენ შესაბამის კომპიუტერებს. მუშაობის პრინციპიდან გამომდინარე, სვიჩებს უფრო მეტი შესაერთებლები აქვთ და ჰაბების მსგავსად მათი ერთმანეთთან მიერთებაც შეიძლება.

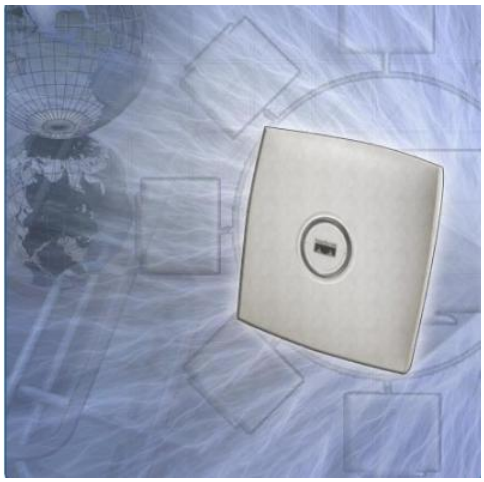
მარშრუტიზატორი(router)

სვიჩების გამოყენებით რამდენიმე ლოკალური ქსელის გაერთიანება შეიძლება და თუ ამ სვიჩებს მივუერთებთ მარშრუტიზატორს, ის შეძლებს პაკეტის თავსართში გაშიფროს ქსელში ჩართული ყველა კომპიუტერის IP მისამართი და გადაუგზავნოს იგი ქვექსელის გამაერთიანებელ

სვიჩს, რომელიც თავის მხივ მიაწვდის შესაბამის კომპიუტერს.

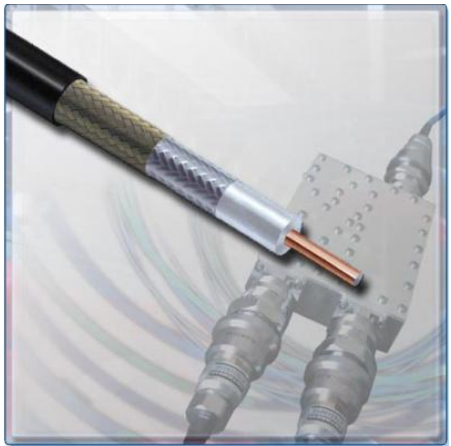
უკაბელო წვდომის წერტილები
(Wireless Access Point)

უკაბელო წვდომის წერტილებთან შესაძლებელია მოხდეს დაკავშირება კომპიუტერებით ან ლეპტოპებით, რომლებსაც აქვთ უკაბელო ქსელური ადაპტერი. ისინი კომუნიკაციისათვის რადიოტალღებს იყენებენ. მათი დაფარვის ზონა შეზღუდულია დიდი ქსელებს ესაჭიროებათ რამდენი ასეთი წერტილი ადეკვატური დაფარვისათვის.



მრავალფუნქციური მოწყობილობები

არსებობს მოწყობილობები, რომლებსაც ერთად რამდენიმე ფუნქცია აქვთ ჩაშენებული. გაცილებით მოხერხებულია ამგვარი მოწყობილობებით სარგებლობა, განსაკუთრებით საცხოვრებელ ბინებში. ერთ ამგვარ მოწყობილებას შეუძლია შეითავსოს მარშრუტიზატორის, კომუტატორის და უკაბელო წვდომის წერტილის ფუნქციები. ერთ-ერთი მათგანია LinkSys 300N.



კოაქსიალური კაბელი და მისი შეერთება ქსელის ადაპტერთან

კოაქსიალური კაბელი ყველაზე მეტად იყო გავრცელებული თავისი ფასის, წონისა და პრაქტიკულობის და ასევე დაყენების სიმარტივის გამო. მარტივი კოაქსიალური კაბელი შედგება სპილენძის გამტარისაგან, ირგვლივ შემოხვეული საიზოლაციო შრისაგან, მეტალის წნულისაგან (ეკრანისაგან) და გარე გარსისაგან. ზოგჯერ მეტალის წნულის გარდა აქვს ფოლგის ფენაც და ასეთს ეწოდება კაბელი ორმაგი ეკრანიზაციით. ძლიერი შეფერხებების დროს შეიძლება გამოყენებულ იქნას კაბელი ოთხმაგი ეკრანიზაციითაც. იგი შედგება ფოლგის ორი ფენისაგან და მეტალის წნულის ორი ფენისაგან. ელექტრული სიგნალები გადაიცემა სპილენძის გამტარში. ეს გამტარი გარშემორტყმულია დიალექტრიკული ფენით, რომელიც მას მეტალის წნულისაგან გამოყოფს. წნული მიწის როლს ასრულებს და იცავს გამტარს ელექტრული სიგნალისაგან და გადამკვეთი შეფერხებებისაგან. გადამკვეთი შეფერხებები ესაა ელექტრული დაზიანება, რომელსაც იწვევს სიგნალები მეზობელ გამტარებში. გამტარი და მეტალის წნული ერთმანეთს არ უნდა ეხებოდეს, რადგან შეიძლება წარმოიშვას მოკლე ჩართვა და მონაცემები დამახინჯდეს. კოაქსიალური კაბელი შეფერხებების მიმართ უფრო გამძლეა, ვიდრე ხვეულა წყვილი და სიგნალების მილევაც ნაკლებია მასში. სიგნალის მილევა არის კაბელში გავლისას სიგნალების შესუსტება.

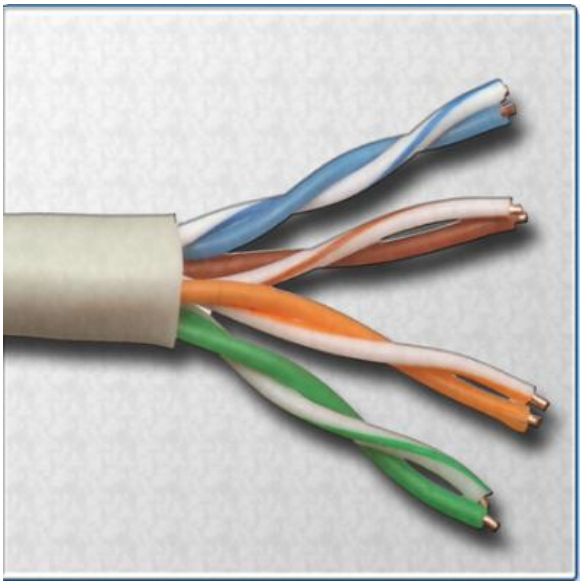
კოაქსიალური კაბელის ორი ტიპი არსებობს: წვრილი კოაქსიალური კაბელი (thinnet) და მსხვილი კოაქსიალური კაბელი (thicknet). წვრილი კაბელი მოქნილია, მისი კაბელია დიამეტრი 0.5 სმ-მდეა. იგი გამოიყენება ნებისმიერი ტიპის ქსელისთვის და უშუალოდ ერთვება ქსელის ადაპტერის პლატას. ასეთ კაბელებს ინფორმაციის დაუმახინჯებლად გადაცემა შეუძლია 185 მ-მდე. სქელი კოაქსიალური კაბელი შედარებით ხისტია, დიამეტრი 1 სმ-მდე აქვს. რაც მეტია სასიგნალო გამტარის სისქე, მით მეტ მანძილზე შეუძლია მას სიგნალების გადაცემა დაუმახინჯებლად. სქელ კოაქსიალური კაბელს მონაცემთა დაუმახინჯებლად გადაცემა შეუძლია 500 მ-დე მანძილზე. ამიტომ მას იყენებენ როგორც რამდენიმე პატარა ქსელის გამაერთიანებელ მაგისტრალს. ასეთი კაბელების მისაერთებლად ქსელის ადაპტერის პლატასთან გამოიყენება ტრანსივერი.

გრეხილი წყვილი –TP (Twisted Par)

არსებობს ამ კაბელის ორი სტანდარტი: არაეკრანირებული – UTP და ეკრანირებული – STP, რომელიც მთლიანად ლითონის ბადეშია ჩასმული.

ეკრანირებული კაბელის გამოყენება უმჯობესია, რადგანაც მონაცემები ნაკლებად შეიძლება დამახინჯდეს გარე ელექტრო-მაგნიტური ზემოქმედების დროს, თუმცა ეს კაბელები

საკმაოდ ძვირია და იმის გათვალისწინებით, რომ ლოკალურ ქსელებში კომპიუტერები მაინცდამაინც არ არის ერთმანეთისგან დაშორებული, მასიური გამოყენება UTP კაბელებს უფრო აქვთ.



კაბელი UTP

თავის მხრივ UTP კაბელები 4 კატეგორიისა: UTP 3, UTP 5, UTP 5e და UTP 6. პირველს შეუძლია მონაცემთა 10 მბტ/წმ სიჩქარით გატარება, ანუ იგი სტანდარტულ Ethernet სისტემებში შეგვიძლია გამოვიყენოთ, ხოლო Fast Ethernet და Gigabit Ethernet სტანდარტის აპარატურის შესაერთებლად გამოიყენება UTP 5 კაბელი, რომელსაც 100 მბტ/წმ და 1000 მბტ/წმ სიჩქარეების განვითარება შეუძლია. ამ კაბელებს ხვიურ წყვილებს იმიტომ უწოდებენ, რომ შედგებიან სადენთა 4 წყვილისაგან, რომელთაგან თითოეული ერთმანეთზეა დახვეული. ეს შემთხვევით არ არის ასე, ცნობილია, რომ სადენთა ერთმანეთზე გადახვევა ხელს უშლის ელექტრო-მაგნიტური ველის შექმნას, ე.ი. კაბელში მონაცემთა დამახინჯებას. თითოეული წყვილი განსხვავდება თავისი ფერით. ერთმანეთზე დახვეულია ლურჯი და თეთრი-ლურჯი ზოლით, მწვანე და თეთრი-მწვანე ზოლით, ნარინჯისფერი და თეთრი-ნარინჯისფერი ზოლით, ყავისფერი და თეთრი-ყავისფერი ზოლით. ფერთა ეს განლაგება ყველა კაბელში ერთნაირია და ამას თავისი მიზეზი აქვს, რასაც მოგვიანებით გავიგებთ. UTP 5e-ს განსხვავებით UTP 5-ისგან მეტი გრეხილი აქვს. ხოლო UTP 6 .კაბელი შეიცავს „პლასტიკურ გამყოფს“ წყვილებს შორის. რაც ხელს უშლის ხარვეზებს (დაბრკოლებებს).

ოპტიკურ-ბოჭკოვანი კაბელი

.

ოპტიკურ-ბოჭკოვან კაბელში მონაცემთა გადაცემა ხდება მოდულირებული სინათლის იმპულსების სახით. იგი მონაცემთა გადაცემის შედარებით დაცული ხერხია. ასეთი ტიპის ხაზები გამოიყენება დიდი

მოცულობის მონაცემების გადასაცემად დიდი სისწრაფით (10 გიგაბიტი/წამამდე). მათში სიგნალების მილევა და დამახინჯება თითქმის არ ხდება. ოპტიკური ბოჭკო წვრილი შუშის ცილინდრია (5-60 მიკრონი), რომელსაც ქვია შუშის ფენით დაფარული სასიგნალო გამტარი. ყოველი ოპტიკური ბოჭკო სიგნალს გადაცემს ერთი მიმართულებით, ამიტომ ყოველი კაბელი შედგება ორი ოპტიკური ბოჭკოსგან, რომლებსაც აქვთ დამოუკიდებელი კონექტორები; ერთი მათგანი გამოიყენება გადასაცემად, მეორე – მიმღებად. დღესდღეობით კომპიუტერულ ქსელებში გამოიყენება სამივე ტიპის კაბელი, მაგრამ ყველაზე პერსპექტიულია ოპტიკურ-ბოჭკოვანი, ის გამოიყენება მაგისტრალების ასაგებად.

ოპტიკურ-ბოჭკოვანი კაბელით ინფორმაციის გადაცემის დროს მასზე არ მოქმედებს ელექტრული შეფერხებები, არ ხდება სიგნალის დამახინჯება და მილევა, ამიტო გადაცემა ხდება ძალიან დიდი, წამში ასობით მეგაბიტი, სიჩქარით, რომლის თეორიული ზღვარი 200000 მგბტ/წმ-ის ტოლია. არსებობს ორი ტიპის ოპტიკურ-ბოჭკოვანი კაბელი:

- Multimode
  ამ ტიპის კაბელს სქელი „გული“ აქვს, შესაბამისად მისი დამზადება უფრო ადვილია. სინათლის წყაროდ შესაძლებელია გამოვიყენოთ უფრო მარტივი წყარო (შუქდიოდი). ის კარგად მუშაობს რამდენიმე კილომეტრზე.
- Singlemode.
  მას გააჩნია ძალიან თხელი „გული“ აქვს და შესაბამისად მისი დამზადებაც უფრო ძვირია. ის სინათლის წყაროდ იყენებს ლაზერს და თავისუფლად შეუძლია გადასცეს ინფორმაცია ათეულობით კილომეტრზე.

ლოკალური ქსელის ტოპოლოგიები. ლოკალური ქსელის არქიტექტურა

ტოპოლოგია ეწოდება ქსელის განლაგებას. ის შეიძლება იყოს ფიზიკურიც და ლოგიკურიც. ფიზიკური ტოპოლოგია გვატყობინებს, თუ როგორ არის განლაგებული კაბელი ხოლო ლოგიკური – თუ როგორ მოგზაურობენ მონაცემები ქსელში. ტოპოლოგიის სახეობის არჩევა არის მნიშვნელოვანი ნაბიჯი ქსელის დაპროექტებისას.

თითოეული მათგანი განსხვავადება ფასით, დანერგვის სირთულით, მგრძნობელობით ხარვეზებისადმი (მაგ., კაბელის გაწყვეტა) და სირთულით ხელახლა კონფიგურირებისას (მაგ., ახალი მანქანის დამატება ქსელში).

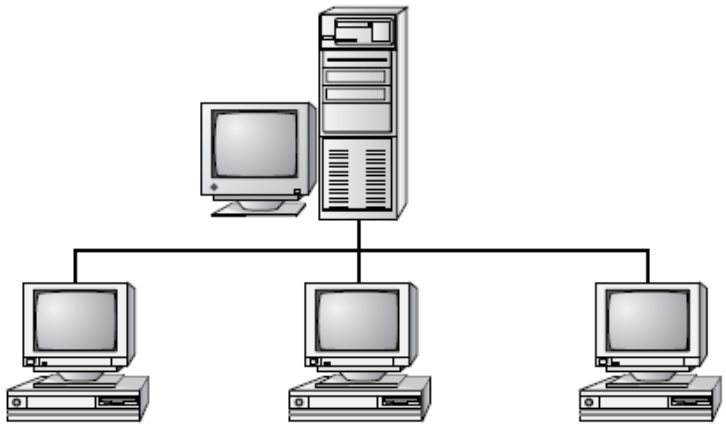
არსებობს ხუთი მთავარი სახეობის ტოპოლოგია (ზოგიერთი შეიძლება იყოს ორივენაირი – ლოგიკურიც და ფიზიკურიც):

- სალტური (BUS – შეიძლება იყოს ორივენაირი – ლოგიკურიც და ფიზიკურიც)
- ვარსკლავური (STAR – მხოლოდ ფიზიკური)
- წრიული (RING -შეიძლება იყოს ორივენაირი – ლოგიკურიც და ფიზიკურიც)
- ბადისებრი (MESH - შეიძლება იყოს ორივენაირი – ლოგიკურიც და ფიზიკურიც)
- ჰიბრიდული (HYBRID - როგორც წესი ფიზიკური)

თითოეულ ტოპოლოგიეს აქვს თავისი დადებითი და უარყოფითი მხარეები.

სალტური ტოპოლოგია (BUS)

სალტე არის უმარტივესი ფიზიკური ტოპოლოგია. ის შედგება მხოლოდ ერთი კაბელისაგან, რომელიც უერთდება ყველა კომპიუტერს. ქსელის ყველა კომპიუტერი ინაწილებს ერთსა და იმავე მონაცემებს და სამისამართო გზას. ყველა მონაცემი გადის ცენტრალურ მაგისტრალზე და თითოეული კომპიუტერი ამოწმებს, არის თუ არა ეს მონაცემი განკუთვნილი მისთვის. თუ არის, მაშინ ქსელური ადაპტერი გადმოიტანს თავის ჩაშენებულ მეხსიერებაში.



კაბელური სისტემები, რომლებიც გამოიყენებიან ამ ტოპოლოგიაში, ადვილად დასაინსტალირებელნი არიან – გააბამთ კაბელს პირველი კომპიუტერიდან ბოლომდე, ხოლო დანარჩენები მათ შორის სადმე ჩაირთვებიან. იმის გამო, რომ ადვილი დასამონტაჟებელია და კაბლის ფასიც არის დაბალია, ეს ტოპოლოგია არის ყველაზე იაფი.

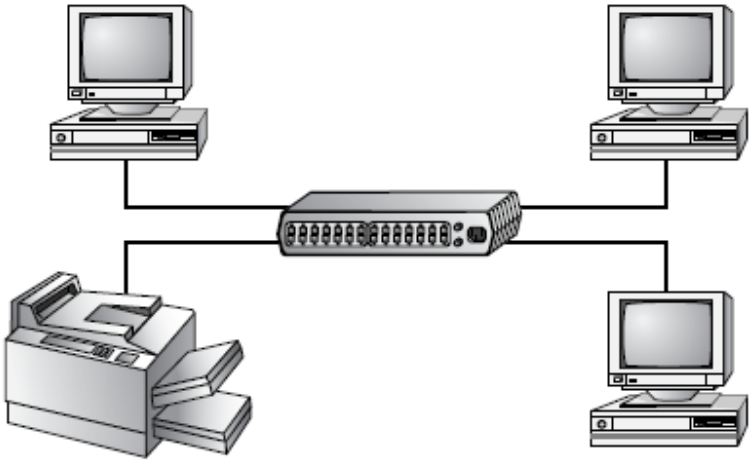
მართალია, სალტური ტოპოლოგია სხვებთან შედარებით ნაკლებ კაბელს საჭიროებს, მაგრამ ახალი სამუშაო მანქანის დამატების დროს ამ კაბელის სრულად გადამისამართება ხდება, ამიტომაც შესაძლოა ორჯერ მეტიც კი დაიხარჯოს. ასევე რომელიმე კაბელის გაწყვეტის შემთხვევაში მთელი ქსელი ზიანდება და წყვეტს მუშაობას. შესაბამისად, ასეთი ქსელის მომსახურება ძვირი ჯდება.

ვარსკვლავური ტოპოლოგია (STAR)

ვარსკვლავური ფიზიკური ტოპოლოგია აკავშირებს თითოეულ ქსელურ მოწყობილობას ცენტრალურ მოწყობილობასთან, რომელსაც ჰქვია ჰაბი (HUB). ახალი

სამუშაო მანქანების დამატება მასში ძალიან ადვილია, ხოლო თუ რომელიმე სამუშაო მანქანა გამოვა მწყობრიდან, არც ეს შეუშლის ხელს სხვა მანქანების მუშაობას, თუმცა როგორც, ალბათ, მიხვდით, თუ ცენტრალური მოწყობილობა დაზიანდა, მთელი ქსელი შეწყვეტს მუშაობას.

ზოგიერთი ტიპი Ethernet-ისა, ARCnet-ისა და Token Ring-ისა იყენებს ვარსკვლავურ ფიზიკურ ტოპოლოგიას, სურათი შეგიქმნით წარმოდგენას, თუ როგორ გამოიყურება ეს ტოპოლოგია.

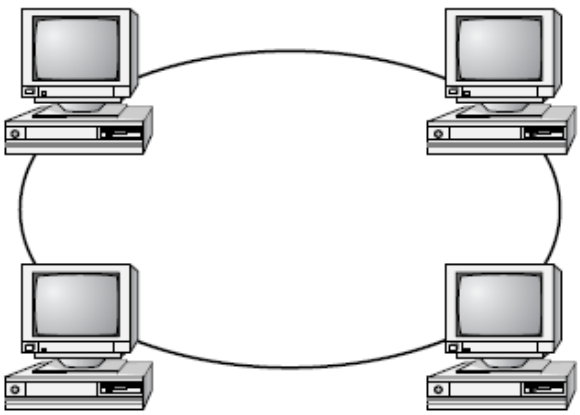


ვარსკვლავური ტოპოლოგია ადვილი დასამონტაჟებელია. კაბელები იჭიმება ჰაბიდან ყველა კომპიუტერამდე, ჰაბი კი მონტაჟდება ოფისის ცენტრალურ წერტილში. ამ ტოპოლოგიის დამონტაჟება სალტურ ტოპოლოგიასთან შედარებით უფრო ძვირი ჯდება, რადგანაც კაბელიც მეტია საჭირო და ჰაბიც შესაძენია, სანაცვლოდ ერთ-ერთი კაბელის გაფუჭებისას მთელი ქსელი აგრძელებს მუშაობას და ახალი სამუშაო მანქანები ადვილი დასამონტაჟებელია.

ხშირად კომპანიები ჰაბის მაგივრად იყენებენ მოწყობილობას, რომელსაც ჰქვია სვიჩი (Switch), განსხვავება ისაა, რომ სვიჩი ქმნის ვირტუალურ კავშირს გამგზავნსა და დანიშნულების კომპიუტერამდე. როდესაც ჰაბი უბრალოდ აგზავნის მანაცემებს ყველა პორტზე იმის გარდა, საიდანაც შემოვიდა ეს მონაცემები. შესაბამისად, სვიჩი გვთავაზობს უკეთეს მომსახურებას ჰაბთან შედარებით, პატარა ფასის მცირეოდენი გაზრდის ხარჯზე.

წრიული ტოპოლოგია (RING)

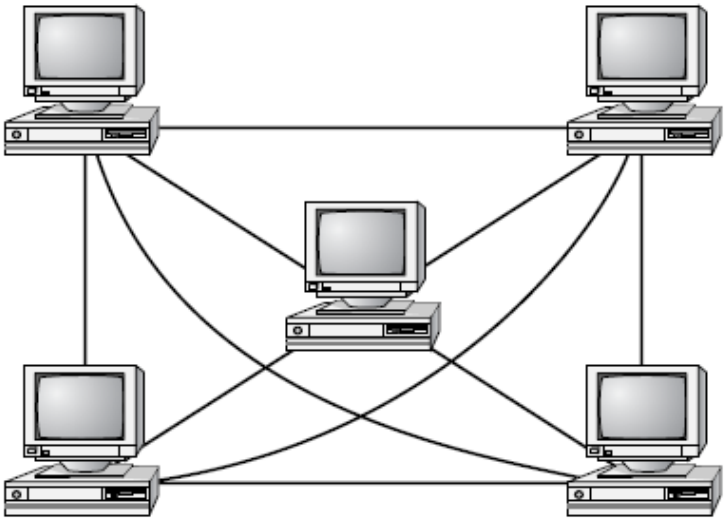
ფიზიკური წრიული ტოპოლოგია უნიკალური ტოპოლოგიაა – თითოეული კომპიუტერი უკავშირდება ორ სხვა კომპიუტერს და თითოეული, რომელიც იღებს მონაწილეობას ამ წრეში, იღებს მონაცემებს, კითხულობს მათ და შემდეგ აგზავნის თავის მეზობელთან მეორე ქსელური კაბელით. თვალსაჩინოებისთვის იხილეთ სურათი.



ამ ტოპოლოგიაში რთულია ახალი კომპიუტერის დამატება, განსხვავებით ვარსკვლავური ტოპოლოგიისაგან, წრიულში თუ ერთი კომპიუტერის გათიშვას მთელი ქსელის გათიშვა მოყვება. ფიზიკური წრიული ტოპოლოგია დღეს იშვიათად არსებობს. უმთავრესი მიზეზები ამისი არის ის, რომ მისი აპარატურული უზრუნველყოფა ძვირი ჯდება, თან მგრძნობიარეა ხარვეზებისადმი. თუმცა დღესდღეობით შემორჩენილია და გამოიყენება ლოგიკური წრიული ტოპოლოგიები. ერთ-ერთი მათგანი არის IBM-ის Token Ring-ი (წრედი მარკერით), ის მოგვიანებით იქნება განხილული „ქსელურ არქიტექტურაში“.

ბადისებრი ტოპოლოგია (MESH)

ეს ტოპოლოგია არის ყველაზე მარტივი მონაცემთა გადაცემის თვალსაზრისით, მაგრამ დიზაინი ყველაზე რთული აქვს ყველა კომპიუტერი ერთმანეთთან არის დაკავშირებული. ეს ტოპოლოგია იშვიათად გვხდება ლოკალურ ქსელებში, ამის მთავარი მიზეზი არის კაბელების გაყვანის სირთულე. თუ კი გვაქვს X კომპიუტერი ქსელში, მაშინ გვექნება (X*(X-1))/2. მაგ., თუ გვექნება 5 კომპიუტერი ქსელში, დაგვჭირდება 5 * (5-1) / 2 = 10 კაბელი. თუ დავამატებთ ერთ კომპიუტერს, 15 კაბელი გახდება საჭირო. წარმოიდგინეთ, 50 კომპიუტერისთვის ბადისებრ ტოპოლოგიაში დაგჭირდებათ 1225 კაბელი.

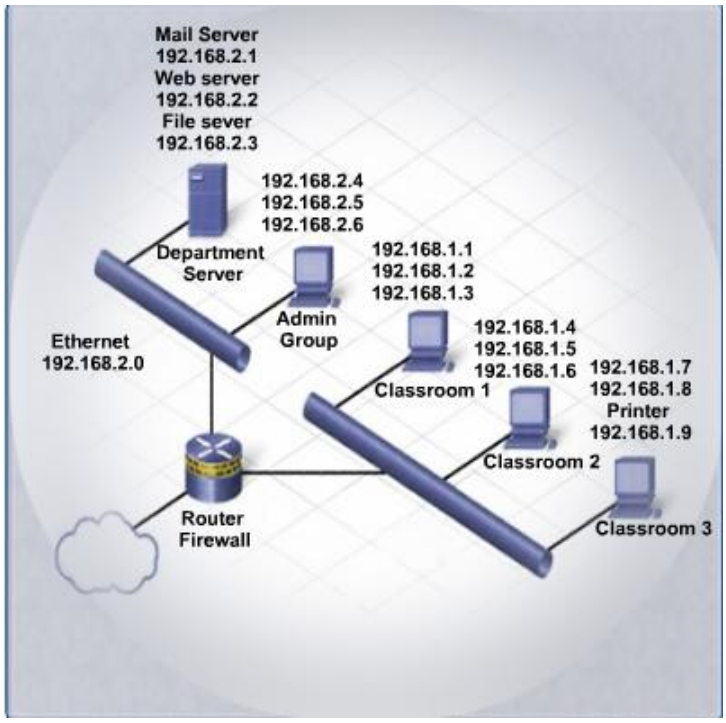


დიზაინიდან გამომდინარე, ფიზიკური ბადისებრი ტოპოლოგია ძალიან ძვირია დასამონტაჟებლადაც და შემდგომში მომსახურებისთვისაც, თუმცა დეფეკტებს ადვილად იტანს – აქ ყოველთვის არის საშუალება, რომ მონაცემი მივიდეს დანიშნულების ადგილამდე, მას შეუძლია პირდაპირის ნაცვლად ირიბი გზით მიაღწიოს მიზანს. ამის გამო ის ხშირად გვხდება გლობალურ ქსელებში (WANs), იმისთვის, რომ გადასაცემმა მონაცემმა რამდენიმე მარშუტიდან ოპტიმალური აირჩიოს, იყენებენ მოწყობილობა მარშუტიზატორს (Router). თუმცა ბადისებრი ტოპოლოგია ხდება არაეფექტური ხუთზე მეტი მოწყობილობის დაკავშირების შემთხვევაში.

ჰიბრიდული ტოპოლოგია (Hybrid)

ჰიბრიდული ტოპოლოგია მოიცავს ერთმანეთში შერეული სხვადასხვა ტოპოლოგიებს. ამის ჩვენება სურათით შეუძლებელია, რადგანაც ძალიან ბევრი ვარიანტი არსებობს. დღესდღეობით ფაქტიურად ყველა ქსელი არის შერეული და სხვადასხვაგვარი. ჰიბრიდული ტოპოლოგია შეიძლება სხვა დანარჩენ ტოპოლოგიებზე ძვირიანი იყოს, მაგრამ მას ყოველი მათგანიდან საუკეთესო თვისებები აქვს აღებული.

ლოგიკური ტოპლოგიები



ლოგიკური ტოპოლოგიების ორი ძირითადი ტიპი არსებობს, ფართო მაუწყებლობითი (broadcast) და ტოკენ რინგი.

ფართომაუწყებლობით ტოპოლოგიაში, თითოეული ჰოსტი ამისამართებს მონაცემებს ან ერთი კონკრეტული ჰოსტისადმი, ან ქსელით დაკავშირებული ყველა ჰოსტისადმი. არ არსებობს რიგითობა, რომელიც უნდა დაიცვან ჰოსტებმა ქსელში – მონაცემთა გადაცემა „დასწრებაზეა“, რომელიც პირველი მოინდომებს, ის გადასცემს პირველი.

ტოკენ რინგი აკონტროლებს ქსელში დაშვებას ელექტრო სიგნალით. სიგნალი რიგრიგობით გადაეცემა ყველა ჰოსტს ქსელში და როდესაც ჰოსტი მიიღებს ამ სიგნალს, ეძლევა უფლება, თვითონ გააგზავნოს მონაცემები ქსელში, მაგრამ თუ მას არა აქვს ქსელში გადასაცემი მონაცემები, ის სიგნალს გადასცემს მომდევნო ჰოსტს და პროცესი მეორდება.

Architecture	Physical Topology	Logical Topology
Ethernet	Bus Star Extended Star	Bus
Token Ring	Star	Ring
Fiber-Distributed Data Interface (FDDI)	Double Ring	Ring

ქსელური არქიტექტურა აღწერს როგორც ფიზიკურ ტოპოლოგიას, ასევე ლოგიკურს. სურათზე წარმოდგენილია სამი ყველაზე მეტად გავრცელებული ლოკალური ქსელის არქიტექტურა.

ეზერნეტი (Ethernet)

ეზერნეტი იყენებს ლოგიკურ სალტურ ტოპოლოგიას და ფიზიკურს – ვარსკვლავურს ან სალტურს. მონაცემთა გადაცემის სიჩქარე არის 10 მბტ/წმ და 100 მბტ/წმ, თუმცა ახალი ტექნოლოგიაა უკვე გავრცელებული, რომელსაც ეწოდება გიგაბიტ-ეზერნეტი და მისი სიჩქარე არის 1 გიგაბტ/წმ.

ტოკენ რინგი

ტოკენ რინგი თავდაპირველად IBM ფირმის მიერ იქნა შემუშავებული, როგორც საიმედო ქსელური არქიტექტურა, რომელშიც ეზერნეტის არქიტექტურაა დაფუძნებული IEEE 802.3 სტანდარტზე. ის გვაუწყებს, რომ ქსელი იყენებს Carrier Sense Multiple Access with Collision Detection-ს (CSMA/CD). ამ დროს მოქმედებს ამოქმედდება ქსელში მონაცემთა გადაცემის „დასწრებაზე: დაფუძვნებული წესის კონტროლი.

კონტროლი ხდებოდა სიგნალის (ტოკენი) გადაცემით ქსელში. ეს არქიტექტურა ხშირად არის ინტეგრირებული IBM ფირმის მეინფრეიმულ სისტემებში.

ტოკენ რინგი არის მაგალითი არქიტექტურისა, რომელშიც ფიზიკური ტოპოლოგია განსხვავდება ლოგიკურისაგან. ამ ტოპოლოგიაში კომპიუტერები უკავშირდებიან ცენტრალურ კონცენტრატორს, რომელსაც ეწოდება მრავალი მანქანის წვდომის ერთეული (MSAU). ამ მოწყობილობის შიგნით გამტარები წარმოქმნიან ერთგვარ წრედს, სიგნალი მიდის ამ წრედიდან გამავალი პორტის გზით კომპიუტერისაკენ და თუ კომპიუტერს არ გააჩნია ინფორმაცია გასაგზავნად, ის ბრუნდება უკან და აგრძელებს სვლას დანარჩენი კომპიუტერებისაკენ. ასე წრიულად გრძელდება ეს პროცესი და მართლაც წააგავს ფიზიკურ წრედს.

ამ ქსელში რამდენიმე მექანიზმია ქსელური დაზიანებების აღმოსაჩენად და გამოსასწორებლად. მაგ., ერთ-ერთი მანქანა ირჩევა როგორც „აკტიური მონიტორი“. ის იწყებს მუშაობას, როგორც ცენტრალიზებული წყარო სინქრონიზაციის ინფორმაციისა დანარჩენი ჰოსტებისათვის და წრედში რამდენიმე ფუნქციას ასრულებს, ერთ-ერთია: მუდმივად ჩაციკლული მონაცემებისა ამოღება წრიდან. როდესაც გამგზავნი მოწყობილობა გამოდის მწყობრიდან, მისმა მონაცემებმა შესაძლოა გააგრძელონ მოგზაურობა წრედში. ამან შეიძლება ხელი შეუშალოს სხვა ჰოსტებს მონაცემების გადაცემაში და დაბლოკოს ქსელი. აქტიურ მონიტორს შეუძლია აღმოაჩინოს ასეთი მონაცემები და მოაშოროს ისინი წრედს, თან წარმოქმნას ახალი ტოკენ-რინგი.

FDDI არის ტიპი ტოკენ რინგ ქსელისა. მისი ტოპოლოგია და გამოყენება განსხვავდება IBM არქიტექტურისაგან. ის ხშირად გამოიყენება რამდენიმე კორპუსის ერთმანეთთან დასაკავშირებლად საოფისე ან საუნივერსიტეტო კომპლექსში. კაბელი, რომელიც მასში გამოიყენება, არის ოპტიკურ-ბოჭკოვანი. ამ ტექონოლოგიაში თავმოყრილია მაღალი სიჩქარისა და საიმედოობის ტოპოლოგიები. მისი სიჩქარე არის 100 მბტ/წმ ორმაგი წრედის ტოპოლოგიაზე. გარეთა წრეს ეწოდება ძირითადი, ხოლო შიგას – მეორადი. ჩვეულებრივ მონაცემები მოგზაურობენ მხოლოდ გარე წრედზე, ხოლო იმ შემთხვევაში, თუ გარე წრე დაზიანდება, მონაცემთა გადაცემა გადაინაცვლებს შიგა წრედზე საპირისპირო მიმართულებით.

ამ ტოპოლოგიას შეუძლია 500 კომპიუტერის მუშაობის უზრუნველყოფა თითოეულ წრედზე. ხოლო მაქსიმალური მანძილი, რომელზეც თითოეული წრედი შეიძლება იშლებოდეს, არის 100 კილომეტრი. გამმეორებელი მოწყობილობა, რომელიც აძლიერებს სიგნალს არის საჭირო ყოველ ორ კილომეტრში. ბოლო ხანებში ამ ტიპის ქსელების შეცვლა ხდება უფრო სწრაფი ეზერნეტებით.

სტანდარტიზაციის ორგანიზაციები, ethernet-ის კაბელირებული სტანდარტები.
ethernet -ის უკაბელო სტანდარტები 802.11*(a,b,g,n)

CCITT

CCITT ადგენს სტანდარტებს ფაქსის გასაგზავნად და სატელეფონო ხაზის მეშვეობით მონაცემების გასაგზავნად (ისეთით, როგორიც არის V.90), რომელიც ავითარებს 56000 ბიტ/წმ-მდე სიჩქარეს.

1992 წელს ეს ორგანიზაცია გადაიქცა ITU.

IEEE

IEEE არის 150 ქვეყანაში მოქმედი არაკომერციული ტექნიკური ასოციაცია, შემდგარი 377 000 პროფესიონალისაგან. დაარსდა 1884 წელს. ორგანიზაციის წევრები არიან ინჟინრები, მეცნიერები, სტუდენტები. ის ლიდერია ისეთ სფეროებში, როგორიც არის კომპიუტერული ინჟინერია, ბიომედიცინის ტექნოლოგია, ტელეკომუნიკაციები და ა.შ.

ამ ორგანიზაციას აქვს 860-ზე მეტი აქტიური სტანდარტი, რომელთაგან 700 დამუშავების სტადიაშია. ორგანიზაცია კარგად არის ცნობილი იმითაც, რომ შეიმუშავა მრავალი სტანდარტი

კომპიუტერული და ელექტრონული ინდუსტრიებისათვის. მათ შორის IEEE 802 სტანდარტი, რომელიც არის ლოკალური ქსელებისათვისაა და ფართოდ გამოიყენება.

ISO

ISO საერთაშორისო სტანდარტიზაციის ორგანიზაციაა, მასში შესულნი არიან ეროვნული სტანდარტიზაციის ორგანიზაციები 140 ქვეყნიდან. მაგალითად, ANSI – ამერიკის ეროვნული სტანდარტების ინსტიტუტი. ეს არასამთავრობო ორგანიზაციაა. ის ახდენს გავრცელებას საერთაშორისო სტანდარტებისა. ამ ორგანიზაციამ რამდენიმე მნიშვნელოვანი კომპიუტერული სტანდარტი ჩამოაყალიბა, ყველაზე მნიშვნელოვანი, ალბათ, არის OSI მოდელი – სტანდარტული არქიტექტურა ქსელების ასაგებად. ISO-მ საერთაშორისო ელექტრო-ტექნიკურ კომისიასთან ერთად და საერთაშორისო სატელეკომუნიკაციო კავშირთან (ITU) ერთად დაამყარა სტრატეგიული პარტნიორობა მსოფლიო სავაჭრო ორგანიზაციასთან.

IAB

IAB – ინტერნეტ არქიტექტურის საბჭო არის კომიტეტი, რომელიც თვალყურს ადევნებს ტექნიკურ და ინჟინრულ განვითარებას ინტერნეტისა ინტერნეტსაზოგადოების (ISOC) მიერ. ასევე ის ზედამხედველობს IETF-სა და IRTF-ზე. ეს სახელი მას მიენიჭა 1992 წელს, როდესაც ინტერნეტი ყველასათვის ღია გახდა.

ANSI

ANSI არის ამერიკული ეროვნული სტანდარტების ინსტიტუტი. ის კერძო, არაკომერციული ორგანიზაციაა, რომელიც აკონტროლებს ამერიკულ ნებაყოფლობით სტანდარტიზაციის და შეთანხმების სისტემას. ის იკვლევს და ადგენს ინდუსტრიისა და საზოგადოების საჭიროებებს და ახდენს განვითარებას ამ სტანდარტებისა. ის არსებობს 1918 წლიდან და მის მიზნებში შედის ამერიკული ბიზნესის კონკურენტუნარიანობის გაზრდა მსოფლიო ბაზარზე და ცხოვრების დონის გაზრდა. ეს ორგანიზაცია თვითონ არ აყალიბებს სტანდარტებს, მისი მუშაობის პრინციპია ზრუნვა კონსესუსი მისაღწევად კომპეტენტურ ჯგუფებს შორის. ამის გამო მისი ლოგო ხშირად შეგხვდებათ მრავალ სტანდარტზე.

TIA/EIA

TIA/EIA ტელეკომუნიკაციის საერთაშორისო ასოციაციისა და ელექტრონულ ინდუსტრიათა ალიანსია, არიან სავაჭრო ასოციაციები, რომლებიც ერთად აყალიბებენ და აქვეყნებენ სტანდარტების ჯგუფს, მაგ., სტრუქტურირებული ხმისა და მონაცემებისათვის გაყვანილობა ლოკალურ ქსელში. ეს ინდუსტრიული სტანდარტები აღმოცენდა 1984 წელს მიღებული გადაწყვეტილებიდან, რომლის თანახმად, გაყვანილობაზე პასუხიმგებლობა შენობის მფლობელს დაეკისრა. მანამდე კი AT&T-ე დახურული ტექნოლოგიის კაბელებს იყენებდა გაყვანილობისათვის.

IEC

IEC საერთაშორისო ელტექნიკის კომისიაა, ის არის გლობალური ორგანიზაცია, რომელიც ამზადებს და აქვეყნებს საერთაშორისო სტანდარტებს ელექტრიკაში, ელექტრონიკასა და მსგავს ტექნოლოგიებში. ეს ორგანიზაცია ჩამოყალიბდა 1904 წელს ელექტრულ კონგრესზე მიღებული გადაწყვეტილებიდან გამომდინარე. კონგრესში მონაწილეობას იღებდა 60-მდე ქვეყანა. ეს ორგანიზაცია არის ერთ-ერთი იმათგანია, ვისაც ცნობს საერთაშორისო სავაჭრო ორგანიზაცია და მისი სტანდარტები ხშირად გამოიყენება როგორც ეროვნული სტანდარტები სხვადასხვა ქვეყნისთვის და ამით მიიღწევა მრავალი სავაჭრო შეთანხმება.

ეზერნეტი

Ethernet-ი დომინირებს ლოკალური ქსელების ტექნოლოგიებს შორის მთელ მსოფლიოში. ინტერნეტის ინჟინრულ ქმედებათა ძალა (IETF) ახდენს ფუნქციური პროტოკოლების და მომსახურებათა მხარდაჭერას TCP/IP პროტოკოლთა სტეკისათვის ზედა შრეებში. თუმცა მონაცემთა არხის შრის და ფიზიკური შრის ფუნქციური პროტოკოლები და მომსახურეობა არის აღწერილი სხვადასხვა ინჟინრული ორგანიზაციის (IEEE, ANSI, ITU) და კერძო კომპანიების მიერ (proprietary protocols – დახურული ტიპის პროტოკოლები), რადგანაც ეზერნეტი შედგება სტანდარტებისგან, რომლებიც არიან განთავსებულნი ქვედა შრეებზე.

IEEE სტანდარტები

მსოფლიოში პრიველი ლოკალური ქსელი იყო ეზერნეტის ორიგინალური ვერსია.

რობერტ მეტკალფმა და მისმა კოლეგებმა ქსეროქსში დააპროექტეს ის 30-ზე მეტი წლის წინ. პირველი Ethernet ტექნოლოგიის სტანდარტი იქნა გამოქვეყნებული 1980 წელს კონსორციუმის მიერ, რომელიც შედგებოდა Intel-ისაგან, Xerox-ისაგან და Digital Equipment Corporation-ისგან. (DIX). მეტკალფს უნდოდა, რომ Ethernet-ი ყოფილიყო განაწილებული სტანდარტი, ამიტომ ის იქნა გამოშვებული როგორც ღია სტანდარტი. პირველი პროდუქციები, რომლებიც შეიქმნა ეზერნეტ სტანდარტით, გასაყიდად გამოჩნდა ადრეულ 80-იან წლებში მე-20 საუკუნისა. 1985 წელს ელექტრონიკისა და ელექტროობის ინსტიტუტის (IEEE) სტანდარტების კომიტეტმა გამოაქვეყნა ლოკალური და ქალაქის ზომის ქსელების სტანდარტები, ციფრებით 802. Ethernet-ის სტანდარტია 802.3. ინსტიტუტს უნდოდა, რომ მათი სტანდარტი შეთავსებულიყო საერთაშორისო სტანდარტების ორგანიზაციასთან (ISO) და OSI მოდელთან. იმისთვის, რომ ეს

მომხდარიყო, IEEE 802.3 სტანდარტებს უნდა დაეკმაყოფილებინა მოთხოვნები პირველი შრისა და მეორე შრის ქვედა ნაწილის OSI მოდელისა. ამის შედეგად პატარა ცვლილებები განიცადა ორიგინალურმა ეზერნეტის სტანდარტმა (802.3-მა). ეზერნეტი მოქმედებს ოსი მოდელის ორ ქვედა შრეზე, მონაცემთა არხის და ფიზიკურ შრეებზე.

ტრაფიკის უდიდესი ნაწილი იწყება და მთავრდება ეზერნეტ კავშირებზე. თავისი დასაბამიდან, 70-იანი წლები, ეზერნეტმა განიცადა ევოლუცია, რომ ეპასუხა სწრაფი ლოკალური ქსელების გაზრდილი მოთხოვნებისთვის. როდესაც ოპტიკურბოჭკოვანი კაბელი შემოვიდა ხმარებაში, ეზერნეტმა ადაპტაცია განიცადა ამ ახალ ტექნოლოგიასთან და ახლა გამოიყნება მისი უპირატესობები როგორიც არის მაღალი გამტარობა და შეცდომების მცირე რაოდენობა. დღესდღეობით იგივე პროტოკოლი, რომელსაც გადაჰქონდა ინფორმაცია 3 მბიტით/წმ-ში, შეუძლია გადაიტანოს ის 10 გბიტით/წმ-ით.

ეზერნეტის წარმატება შემდეგმა პირობებმა გამოიწვია:

- სიმარტივე და ადვილი მომსახურება
- საშუალება შთანთქას ახალი ტექნოლოგიები
- საიმედოობა
- მისი ინსტალაცია და გაუმჯობესება იაფი ჯდება

საფუძველი ეზერნეტ ტექნოლოგიისთვის პირველად შეიქმნა 1970 წელს, პროგრამას ერქვა Alohanet და იყო ციფრული რადიოქსელი, შემუშავებული ისე, რომ გადაეცა ინფორმაცია განაწილებულ (shared) რადიოსიხშირეზე ჰავაის კუნძულებს შორის. საჭირო იყო, რომ ყველა მონაწილე მხარე დამორჩილებოდა პროტოკოლს, რომელშიც არაჭიარებული (unacknowledged) გადაცემა უნდა გამეორებულიყო პატარა ინტერვალის შემდეგ. განაწილებული მედიის გამოყენების გზები იქნა შემდგომში გამოყენებული კაბელურ გამტარებში ეზერნეტის ფორმით. ეზერნეტის დიზაინი იყო შექმნილი ისე, რომ განეთავსებინა რამდენიმე ურთიერთდაკავშირებული კომპიუტერი განაწილებულ სალტურ ტოპოლოგიაზე. ეზერნეტის პირველ ვერსიაში დაშვების მეთოდი იყო ცნობილი როგორც Carrier Sense Multiple Access with Collision Detection (CSMA/CD). ის მართავდა პრობლემებს, რომლებიც წარმოიქმნებოდა მაშინ, როდესაც რამდენიმე მოწყობილობა ერთდროულად შეეცდებოდა კავშირს განაწილებულ ფიზიკურ მედიაზე.

ეზერნეტის პირველი ვერსიები გამოიყენებდა კოაქსიალური კაბელის სალტურ ტოპოლოგიასთან დასაკავშირებლად. თითოეული კომპიუტერი პირდაპირ იყო

შეერთებული „მაგისტრალურ არხთან“ (backbone). ეს ვერსიები ცნობილი იყო როგორც Thicknet (10BASE5) და Thinnet (10BASE2).

10BASE5 გამოიყენებდა სქელ კოაქსიალურ კაბელში, რომელიც იძლეოდა საშუალებას 500 მეტრამდე კაბელის გაყვანისა, სანამ დასჭირდებოდა განმეორებელი (repeater). 10BASE2 კი იყენებდა თხელ კოაქსიალურ კაბელს, თუმცა უფრო ელასტიურს და მისი გაყვანა შეიძლებოდა 185 მეტრამდე სიგრძეზე.

შესაძლებლობა მიგრაციისა ორიგინალური ეზერნეტისა დღევანდელზე და სამომავლოზე გამოიწვია იმან რომ მეორე შრის კადრის სტრუქტურა პრაქტიკულად შეუჩვლელი რჩება. ფიზიკური მედია, მედიაზე დაშვება, და მედია კონტროლი ყველა განვითარდა და აგრძელებენ განვითარებას. თუმცა ეზერნეტის თავსართი და ბოლოსართი შეუცვლელი დარჩა. ეზერნეტი ადრინდელ ვარიანტებში იყო გამოყენებული დაბალი გამტარობის ლოკალური ქსელების გარემოში სადაც დაშვებას განაწილებულ მედიაზე. მართავდა CSMA ხოლო შემდგომ CSMA/CD. იმასთან ერთად რომ ის იყო ლოგიკური სალტური ტოპოლოგია ის მონაცემთა არხის შრეზე ის ასევე იყო სალტური ტოპოლოგიის ფიზიკურ დონეზეც. ეს ტოპოლოგია გახდა უფრო პრობლემატური როდესაც ლოკალური ქსელები გაიზარდნენ და მათი მომსახურეობებიც მომრავლდა. კოაქსიალური კაბელები ჩაანაცვლეს UTP aკაბელების ადრეულმა ვარიანტებმა. კოაქსიალურთან შედარებით ეს კაბელები მსუბუქები და უფრო იაფები, მათთან მუშაობა უფრო მარტივი იყო. ფიზიკური ტოპოლოგიაც შეიცვალა ვარსკვალურ ტოპოლოგიაზე კონცენტრატორების(hub) გამოყენებით. ისინი კავშირებს აკონცენტრირებდნენ, სხვასიტყვებით რომ ვთქვათ, ისინი იღებდნენ კაბელების ჯგუფს და აძლევდნენ დაშუალებას ქსელს რომ აღექვა ისინი როგორც ერთი. როდესაც კადრი მოვა ერთ პორტზე, მისი გადაკოპირება ხდება ყველა დანარჩენ პორტზე, და შესაბამისად ქსელის ყველა სეგმენტი იღებს კადრს. კონცენტრატორის გამოყენებამ ამ სალტურ ტოპოლოგიაში შემატა საიმედოობა, და ერთი კონკრეტული კაბელის მდგომარეობიდან გამოსვლის შემთხვევაში არ გაითიშება მთელი ქსელი. თუმცა ყველა დანარჩენი პორტისთვის კადრის გამეორებამ არ გადაწყვიტა კოლიზიების პრობლემა.

Legacy ეზერნეტი

ტიპიურად 10BASE-T ქსელებში ცენტრალური წერტილი ქსელის სეგმენტისა იყო კონცენტრატორი. ამან წარმოშვა განაწილებული მედია. იმის გამო, რომ მედია არის განაწილებული, მხოლოდ ერთ მხარეს შეეძლო წარმატებით ინფორმაციის გადაცემა დროის ნებისმიერ მონაკვეთში. ამ კავშირს ეწოდება ნახევარ-დუპლექსური კავშირგაბმულობა. ქსელში მოწყობილობების დამატებასთან ერთად კადრების კოლიზიების რიცხვი მატულობდა. როდესაც კოლიზიების რიცხვი დაბალი იყო CSMA/CD-ს მართვის შედეგად მომხმარებელს არ ექმნდებოდა დისკომფორტი. მაგრამ მათ მატებასთან ერთად გაჩნდა

დისკომფორტიც. მაგალითისთვის გეტყვით, როდესაც დილით ადრე მიემგზავრებით სადმე, მანქანები ცოტაა, გზა თავისუფალია და სწრაფად და თავისუფლად მოძრაობთ, მაგრამ საღამოს იმავე გზაზე გაცილებით ჭირს მოძრაობა, იმიტომ რომ გადატვირთულია მანქანებით.

დღევანდელი ეზერნეტი

ლოკალური ქსელების განვითარების გზაზე ერთ-ერთი უმნიშვნელოვანესი ეტაპი იყო სვიჩების გამოჩენა, რომლებმაც ჩაანაცვლეს კონცენტრატორები. ეს 100BASE-TX ეზერნეტის შექმნიდან მალე მოხდა. სვიჩებს შეუძლიათ აკონტროლონ მონაცემთა ნაკადი და გააგზავნონ კადრი მხოლოდ იმ პორტზე, რომლისთვისაცაა ის განკუთვნილი. სვიჩი ამცირებს რაოდენობას მოწყობილობებისა, რომლებიც იღებენ კადრს და ამით ამცირებენ კოლიზიების რაოდენობას. ამან და შემდეგ სრული დუპლექსის კავშირგაბმულობის გამოჩენამ (ერთდროულად გადაცემის და მიღების საშუალება) გამოიწვია 1გბტ/წმ და უფრო სწრაფი ეზერნეტის შექმნა.

პროგრამები, რომლებიც იყენებენ ქსელს, ყოველდღიურად ტვირთავენ ყველაზე ჯანმრთელ ქსელებსაც კი. მაგალითად, VoIP ტექნოლოგიის გამოყენების ზრდამ და მულტიმედიური მომსახურებები საჭიროებამ უფრო სწრაფ კავშირებს ვიდრე არის 100მბტ/წმ-ში ეზერნეტი.

გიგაბიტ ეზერნეტი გამოიყენება იმისთვის, რომ განვსაზღვროთ 1000 მბტ/წმ-ის გამტარობის ან მეტის ეზერნეტი. ის მიიღება სრული დუპლექსის და UTP ოპტიკურ-ბოჭკოვანი ტექნოლოგიების გამოყენებით.

როდესაც ხდება ქსელის განახლება 100 მბტ/წმ-ის გამტარობიდან 1 გბტ/წმ-მდე ან მეტით, განსხვავება საგრძნობია.

განახლება ქსელისა 1 გბტ/წმ-მდე ყოველთვის არ ნიშნავს მთელი ქსელის ინფრასტრუქტურის გამოცვლას. ზოგიერთი მოწყობილობა თანამედროვე ქსელებში შეიძლება ძალიან პატარა დანახარჯებით ამუშავდეს უფრო მაღალ სიჩქარეებზე.

ოპტიკურ-ბოჭკოვანი კაბელის შემოსვლასთან ერთად ზღვარი ლოკალურ ქსელსა და ფართო ტერიტორიის ქსელს შორის წაიშალა. ეზერნეტი თავდაპირველად შემოისაზღვრებოდა ერთი შენობით და შემდეგ გავრცელდა შენობებს შორის. დღეს ის შეიძლება მთელ ქალაქს ფარავდეს და მას. საქალაქო ქსელი ეწოდება (Metropolitan Area Network (MAN)).

CSMA/CD დაშვების მეთოდში ყველა ქსელურმა მოწყობილობამ, რომელსაც აქვს გასაგზავნი ინფორმაცია, უნდა მოისმინოს გაგზავნამდე.

როდესაც ტრაფიკის აღმოჩენა არ ხდება, მოწყობილობა იწყებს მონაცემის გადაცემას. ეს გადაცემა გრძელდება, მოწყობილობა უსმენს ტრაფიკს ან კოლიზიებს ლოკალურ ქსელში. როდესაც მონაცემი გაგზავნილია, მოწყობილობა ბრუნდება საწყისი სმენის მდგომარეობაში.

მრავალი დაშვება

თუ მანძილი მოწყობილობებს შორის იმდენად დიდია, რომ როდესაც ერთი მოწყობილობა იწეყებს გადაცემას, მეორეს ეს ჯერ არ „ესმის“, შეიძლება მოხდეს ისე, რომ მეორემაც დაიწყოს გადაცემა, მაშინ ეს სიგნალები სადმე გზაში ერთმანეთს დაეჯახება და მონაცემი დამახინჯდება, თუმცა სიგნალი მთლიანად არ გაქრება და ასე დამახინჯებული გააგრძელებს მოგზაურობას.

კოლიზიის აღმოჩენა

როდესაც მოწყობილობა სმენის რეჟიმშია, მას შეუძლია აღმოაჩინოს, თუ როდის მოხდება კოლიზია. კოლიზიის აღმოჩენა არის შესაძლებელი იმიტომ, რომ ყველა მოწყობილობას შეუძლია აღმოაჩინოს სიგნალის ამპლიტუდა. მას შემდეგ, რაც მოხდება კოლიზია, ყველა მოწყობილობა აღმოაჩენს ამას. აღმოჩენის შემდეგ ყველა მოწყობილობა, რომლებიც აგზავნიდნენ ინფორმაციას, აგრძელებს გაგზავნას იმისთვის, რომ დარწმუნდეს, რომ ყველამ აღმოაჩინა კოლიზია.

დახშობის სიგნალი და უკან დახევა

მას შემდეგ, რაც კოლიზიას აღმოაჩენენ გადამცემი მოწყობილობები, ისინი გააგზავნიან დამხშობ სიგნალს, ის გამოიყენება იმისთვის, რომ შეატყობინონ სხვა მოწყობილობებს კოლიზიის შესახებ, რათა მათ გაააქტიურონ უკან დახევის ალგორითმი. ეს ალგორითმი გამოიწვევს ყველა მოწყობილობის გაგზავნის შეჩერებას შემთხვევითი დროით, როცა კოლიზიურ სიგნალებს ჩაცხრომის ნებას რთავს. დროის გავლის შემდეგომ მოწყობილობა გადავა მოსმენა გაგზავნამდე მდგომარეობაში. შემთხვევითი დრო გვეხმარება იმაში, რომ გამოვრიცხოთ იმ მოწყობილობების, რომლებიც იყვნენ ჩართულნი კოლიზიაში, გამეორება ამ კოლიზიისა. თუმცა ეს ასევე ნიშნავს, რომ გადაცემა შეიძლება დაიწყოს სხვა მოწყობილობამ უფრო ადრე, ვიდრე ამას შეძლებენ კოლიზიაში ჩართული მოწყობილობები.

კონცენტრატორები და კოლიზიური დომენები

იმის გამო, რომ კოლიზიები მოხდება ნებისმიერ განაწილებული ტოპოლოგიის მედიაზე, მაშინაც, როდესაც გამოიყენება CSMA/CD მეთოდი, ამიტომ უნდა დავაკვირდეთ პირობებს, რომელთა დროსაც შესაძლებელია მოიმატოს კოლიზიების რაოდენობამ. ინტერნეტის სწრაფი გაზრდის გამო:

- ქსელში უფრო მეტი მოწყობილობა ერთვება.
- მოწყობილობები უფრო ხშირად უკავშირდებიან ერთმანეთს.
- მოწყობილობათა შორის მანძილი იზრდება.

კონცენტრატორები საშუამავლო მოწყობილობები რომლებიც უფრო მეტ მოწყობილობას აძლევდნენ საშუალებას ჩართულიყვნენ ისინი ასევე ცნობილი არიან როგორც მრავალპორტიანი გამმეორებლები. კონცენტრატორები აგზავნიან მათთან მისულ სიგნალს ყველა პორტში იმის გარდა, საიდანაც სიგნალი მოვიდა. კონცენტრატორები არ ასრულებენ ქსელურ ფუნქციებს, ისეთებს როგორიც არის მონაცემების გადამისამართება. კონცენტრატორები და გამმეორებლები არიან მოწყობილობები, რომლებიც აგრძელებენ დისტანციას, რომელზეც შეიძლება ეზერნეტის კაბელების გაყვანა. იმის გამო რომ კონცენტრატორები მოქმედებენ პირველ შრეზე და მუშაობენ მხოლოდ ელექტრულ სიგნალებთან, კოლიზიები შეიძლება მოხდეს იმ მოწყობილობებს შორის, რომლებსაც ისინი აერთებენ, და თვით მათშიც.

კონცენტრატორების გამოყენება ქსელში მომხმარებლების მომატებისთვის აუარესებს უკვე არსებული მომხმარებლების მომსახურეობას იმიტომ, რომ გასაყოფი მედია არ იცვლება.

მოწყობილობები, რომლებიც არიან დაკავშირებული კონცენტრატორების მეშვეობით, საერთო გამტარზე წარმოადგენენ კოლიზიურ დომეინს. მას ასევე უწოდებენ ქსელის სეგმენტს. კონცენტრატორები და გამმეორებლები ზრდიან ზომას კოლიზიური დომეინებისა. თუ გამოვიყენებთ გაფართოებული ვარსკვლავის ფიზიკურ ტოპოლოგიას კონცენტრატორების გამოყენებით, ჩვენ შევქმნით ძალიან დიდ კოლიზიურ დომეინს. კოლიზიების გაზრდილი რაოდენობა ძლიერ ამცირებს ქსელის ეფექტურობას იმისდა მიუხედავად, რომ CSMA/CD არის კადრების კოლიზიის მართვისთვის შექმნილი. ის იყო შექმნილი მცირე რაოდენობის მოწყობილობისთვის და ნაკლებად დატვირთული ქსელებისთვის. ამიტომ უნდა მოინახოს სხვა გზა, რათა შესაძლებელი გახდეს ბევრი მოწყობილობის ჩართვა ქსელში და უფრო დიდი დატვირთვის ქსელის ოპერირება.

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

დაყოვნება

როგორც ვთქვით, თითოეული მოწყობილობა, რომელსაც სურს მონაცემის გადაცემა, უნდა ჩაირთოს სმენის რეჟიმში, რათა შეამოწმოს ტრაფიკი ქსელში. თუ ტრაფიკი არ არსებობს, მაშინ მოწყობილობა იწყებს გადაცემას. ელექტრული სიგნალის გადაცემას სჭირდება გარკვეული დრო (დაყოვნება), თითოეული კონცენტრატორი ან გამმეორებელი სიგნალის გზაზე ზრდის ამ დაყოვნებას და ეს ზრდის კოლიზიების რაოდენობას. იმიტომ რომ თუ სიგნალი მუშავდებოდა კონცენტრატორით ან გამმეორებელით, იმ მომენტში რომელშიც ის მოისმინა მოწყობილობამ, ის ჩათვლის რომ ქსელი თავისუფალია და დაიწყებს გადაცემას.

ჩამხშობი სიგნალი

ეზერნეტი რთავს ნებას მოწყობილობებს, რომ შეეჯიბრონ გადაცემის დროისთვის, ხოლო იმ დროს თუ ორი მოწყობილობის გადაცემა ერთდროულად მოხდება, ქსელის CSMA/CD a შეეცდება გამოასწოროს პრობლემა. თუმცა გახსოვთ ალბათ, რომ მოწყობილობების რაოდენობის ზრდასთან ერთად, შესაძლებელია კოლიზიები ძალიან რთულად გასასწორებელი გახდეს.

კოლიზიის აღმოჩენისთანავე გადამცემი მოწყობილობები გადაცემა 32-ბიტიან ჩამხშობ სიგნალს, რათა ყველა მოწყობილობას შაეტყობინონ კოლიზიის შესახებ. მნიშვნელოვანია რომ ჩახშობის სიგნალი არ ჩაითვალოს როგორც მუშა კადრი, თორემ ვერ მოხდება კოლიზიის აღმოჩენა, ყველაზე გავრცელებული ჩამხშობი სიგნალი არის უბრალოდ 1,0,1,0 ... როგორც პრეამბულა. დამახინჯებულ მონაცემებს ხშირად უწოდებენ კოლიზიის ფრაგმენტებს. ნორმალური კოლიზიები 64 ოქტეტზე მოკლეებია, ამიტომ ადვილია მათი ამოცნობა, ისინი არ აკმაყოფილებენ მინიმალურ ზომას და საკონტროლო (FCS) ტესტს.

უკან დახევის დრო

კოლიზიის შემდეგ ხდება და მოწყობილობების სრული კადრთაშორისი დაყოვნება. მოწყობილობები, რომელთა გამოც მოხდა კოლიზია, დამატებით შემთხვევით დროს იცდიან. ეს დრო შემთხვევითია შეგნებულად, იმის გამო, რომ მათ არ დაიწყონ გადაცემა ისევ ერთდროულად, რაც გამოიწვევდა კიდევ მეტ კოლიზიას. ეს მიიღწევა ნაწილობრივ იმით, რომ ხდება გაზრდა ინტერვალისა, რომლიდანაც ხდება არჩევა შემთხვევითი დროის ამორჩევა. ლოდინის დრო განისაზღვრება სლოტის დროის პარამეტრებით.

იმ შემთხვევაში, თუ მოხდება ისე, რომ ვერ გაიგზავნება კადრი ზედიზედ 16-ჯერ, მოხდება შეცდომის შეტყობინება ქსელური შრისთვის. ეს იშვიათად ხდება სწორად გამართულ ქსელში, და უფრო ხშირად მაშინ როდესაც ფიზიკურ შრეზე დაზიანებაა. ამ მეთოდმა დართო ნება ეზერნეტს უკეთესი მომსახურება გაეწია კონცენტრატორებზე თაფუძნებულ განაწილებული მედიის ტოპოლოგიაში. სვიჩების შემოსვლასთან ერთად CSMA/CD-სადმი მოთხოვნილებამ იკლო, ზოგიერთ შემთხვევაში, საერთოდაც აღარ არის.

განსხვავებები ეზერნეტის სტანდარტებს შორის არის ფიზიკურ შრეზე, ეზერნეტი არის აღწერილი IEEE 802.3 სტანდარტებში. ამჟამად, ოპტიკურ-ბოჭკოვან და გრეხილი წყვილის კაბელებში 4 მონაცემთა გამტარობაა აღწერილი:

10 მბტ/წმ-ში – 10Base-T ეზერნეტი

100 მბტ/წმ-ში – ჩქარი ეზერნეტი

1000 მბტ/წმში – გიგაბიტ ეზერნეტი

10 გბტ/წმ-ში – 10 გიგაბიტ ეზერნეტი

10მბტ/წმ-ში ეზერნეტი შეიცავს:

10BASE5 Thicknet კოაქსიალური კაბელის გამოყენებით.

10BASE2 Thinnet კოაქ სიალური კაბელის გამოყენებით.

10BASE-T Cat3/Cat5 არაეკრანირებული გრეხილი სწყვილის კაბელის გამოყენებით.

ეზერნეტის ადრინდელ ვარიანტებში 10BASE5-სა და 10BASE2-ში, ფიზიკური სალტის შესაქმნელად გამოიყენებოდა კოაქსიალური კაბელი. თუმცა ეს ვარიანტები ახლა აღარ გამოიყენება და არ არის გათვალისწინებული ახალი 802.3 სტანდარტით.

10 მბტ/წმშ-ი ეზერნეტი – 10BASE-T

	10BASE-T	100BASE-TX	1000BASE-T
Media	EIA/TIA Category 3, 4, 5 UTP, four pair	EIA/TIA Category 5, 5e UTP, two pair	EIA/TIA Category 5, 5e UTP, four pair
Maximum Segment Length	100 m (328 feet)	100 m (328 feet)	100 m (328 feet)
Topology	Star	Star	Star
Connector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)

10BASE-T იყენებს მანჩესტერი კოდირებას ორ არაეკრანირებულ გრეხილ წყვილზე. ადრინდელ ვარიანტებში 10BASE-T-სი გამოიყენებოდა Cat3 კაბელი, თუმცა დღესდღეობით მხოლოდ Cat5 ან უფრო ახალი ტიპის კაბელები გამოიყენება. 10მბიტ/წამში ეზერნეტი ითვლება კლასიკურ

ეზერნეტად და გამოიყენებს ვარსკვლავის ფიზიკურ ტოპოლოგიას. ეზერნეტი 10BASE-T-ის კაბელები, სანამ მათ დასჭირდებათ კონცენტრატორი ან გამმეორებელი, შეიძლება იყვოს 100 მეტრამდე 10BASE-T იყენებს ორ წყვილს ოთხ წყვილიანი კაბელისა და terminated 8-გასართიანი RJ-45 კონეკტორით. წყვილები, შეერთებულები პირველ და მეორე გასართთან, გამოიყენებიან ინფორმაციის გადასაგზავნად, ხოლო მე-3 და მე-6-თან – ინფორმაციის მისაღებად. ახალი ქსელის შექმნისას 10BASE-T-ს აღარავინ ირჩევს, თუმცა ჯერჯეროზით არსებობს ბევრი ქსელი, აგებული მისი მეშვეობით. კონცენტრატორების სვიჩებით შეცვლამ ძალიან გაზარდა გამტარობა ამ ქსელებისა და გაუხანგძლივა მათ სიცოცხლე. სვიჩთან შეერთებულ მის კაბელებს აქვთ მხარდაჭერა ნახევარ-დუპლექსისაც და სრული დუპლექსისაც.

100 მბიტ/წამში სწრაფი ეზერნეტი

20 საუკუნის 90-იან წლების შუა პერიოდში რამდენი ახალი 802.3 სტანდარტი იქნა ჩამოყალიბებული ინფორმაციის გადასაცემად 100მბიტ/წამში სიჩქარით. ეს სტანდარტები იყენებენ განსხვავებულ კოდირებას, რათა მიაღწიონ გაზრდილ გამტარუნარიანობას. ამ ეზერნეტის გამართვა შეგვიძლია გრეხილი წყვილი კაბელის მეშვეობით ან ოპტიკურ-ბოჭკოვან გამტარზე. ყველაზე გავრცელებული ვარიანტებია:

100BASE-TX Cat5 კაბელის გამოყენებით

100BASE-FX ოპტიკურ-ბოჭკოვანი კაბელის გამოყენებით

იმის გამო, რომ უფრო მაღალი სიხშირის სიგნალები, რომლებიც გამოიყენება სწრაფ ეზერნეტში, უფრო მეტად ზიანდება ხარვეზებისგან, ორი განცალკევებული კოდირების სისტემა გამოიყენება სიგნალის სრულფასოვნების გასამუჯობესებლად.

100BASE-TX

იქნა შემუშავებული გადაცემის უზრუნველსაყოფად მეხუთე კატეგორიის UTP კაბელზე. ის იმავე ორ წყვილის იყენებს და ისეთივე გასართი აქვს, როგორიც 10BASE-T-ს. თუმცა მას ესაჭიროება კატეგორია ხუთის ან უფრო ახალი UTP კაბელი. 4B/5B კოდირება გამოიყენება 100BASE-T ეზერნეტისთვის. ის დაკავშირებულია როგორც ფიზიკური ვარსკვლავი, თუმცა 10BASE-T-ისგან განსხვავებით ჩვეულებრივ აქ კონცენტრატორის მაგივრად გამოიყენება სვიჩი. 100BASE-TX ტექნოლოგია და სვიჩები ერთდროულად გახდნენ გავრცელებულნი და ამან გამოიწვია მათი ბუნებრივი შერწყმა 100BASE-TX ქსელებში.

100BASE-FX

ეს ტექნოლოგია იყენებს იმავე ხერხს სიგნალების გადაცემისა, რასაც 100BASE-TX, თუმცა მისგან განსხვავებით აქ გამოიყენება ოპტიკურ-ბოჭკოვანი გამტარი. კოდირება, დეკოდირება და საათის გამოჯანმრთელების პროცედურები ერთნაირია ორივე ტექნოლოგიაში, თუმცა სიგნალის გადაცემა 100BASE-TX-ში ხდება ელექტრული იმპულსების გამოყენებით, ხოლო 100BASE-FX-ში სინათლის იმპულსებით. 100BASE-FX იყენებს ეგრეთ წოდებულ დუპლექსურ SC კონექტორებს.

1000მბიტ/წამში – გიგაბიტ ეზერნეტი

გიგაბიტ ეზერნეტის ქსელებში ბიტები ჩნდებიან წილადში იმ დროის რომელიც არის საჭირო სრაფ ეზერნეტში და კლასიკურ ეზერნეტში. და სიგნალების უფრო მოკლე დროში გაჩენის გამო, ბიტები უფრო მგრძნობიარენი ხდებიან ხარვეზებისადმი და, შესაბამისად, სინქრონულობა კრიტიკულია. შესრულება არის დამოკიდებული იმაზე, თუ რამდენად სწრაფად შეუძლია ქსელის ადაპტრეს შეცვალოს ვოლტაჟის დონეები და რამდენად კარგად შეიძლება ამ ვოლტაჟის ცვლილების აღმოჩენა 100 მეტრის მანძილზე მიმღები ქსელის ადაპტერზე ან ინტერფეისზე.

ამ მაღალ სიჩქარეებზე მონაცემების კოდირება და დეკოდირება უფრო კომპლექსურია. გიგაბიტ ეზერნეტში გამოიყნება ორი განცალკევებული კოდირების ნაბიჯი. მონაცემთა გადაცემა უფრო ეფექტურია, როდესაც კოდები გამოიყენება ორობითი ნაკადის აღნიშვნისთვის. კოდირებული მონაცემები უფლებას იძლევა სინქრონიზაციისა და გამტარუნარიანობის უფრო ეფექტურად გამოყენებისა, აგრეთვე გაუმჯობესებულ მოთმინების უნარს ხარვეზებისადმი სიგნალისთვის.

გვაწვდის სრულ-დუპლექსურ გადაცემას ოთხივე წყვილის გამოყენებით კატეგორია 5 ან უფრო ახალი კაბელისა. გიგაბიტ ეზერნეტი იძლევა გაუმჯობესებას 100მბიტ/წამიდან თითოეული წყვილის 125მბიტ/წამამდე, ან 500მბიტ/წამამდე ოთხივე წყვილისთვის. თითოეული წყვილი სრულ-დუპლექსურ რეჟიმში და აორმაგებს 500მბიტ/წამს 1000მბიტ/წამამდე. 1000BASE-T იყენებს 4D-PAM5 ხაზის კოდირებას რათა მიიღოს 1გიგაბიტ/წამში გამტარუნარიანობა. ეს კოდირების სქემა იძლევა საშუალებას გადაცემისა სიგნალის 4-ივე წყვილზე ერთდროულად. ის თარგმნის 8ბიტიან ბაიტს ერთდროულ გადაცემაში 4 კოდური სიმბოლოსი. რომლებიც იგზავნებიან გამტარზე, თითოეულ წყვილზე, როგორც 5 დონიან პულსის ამპლიტუდის მოდუალირებულ სიგნალს.ეს ნიშნავს რომ თითოეული სიმბოლო აღნიშნავს ორ ბიტ ინფორმაციას იმის გამო რომ ინფორმაცია მოგზაურობს ერთდროულად 4 განსხვავებულ მარშრუტზე, უნდა მოხდეს კადრების დაყოფა გადამცემთან და შეერთება მიმღებთან.

1000BASE-T გვაძლევს საშუალებას ერთდროულად ერთი და იმავე კაბელით გავაგზავნოთ და მივიღოთ ინფორმაცია. ეს ტრაფიკი მუდმივად იწვევს კოლიზიებს, კოლიზიების შედეგები

არის კომპლექსური ვოლტაჟის მიმდევრობები, მიმღები იყენებს გამოცდილ ხერხებს, როგორიც არის ექოს გაუქმება, პირველი შრის გადამისამართების შეცდომის გამოსწორება (FEC) და წინდახედული არჩევანი ვოლტაჟის დონნებისა, ამ ხერხების გამოყენებით სისტემა აღწევს 1 გიგაბიტ გამტარუნარიანობას. სინქრონიზაციის დასახმარებლად ფიზიკური შრე ენკაპსულაციას უკეთებს თითოეულ კადრს ნაკადის დამწყები და დამამთავრებელი მსაზღვრელით. წრიული სინქრონიზაცია მიიღწევა უმოქმედობის სიმბოლოების შეუწყვეტელი გადაცემით, რაც ხდება თითეულ წყვილზე კადრთაშორის დაყოვნებისას. განსხვავებით სხვა ციფრული აპარატურისგან, სადაც, როგორც წესი, წყვილი კეთილგონიერი ვოლტაჟი გამოიყენება, 1000BASE-T იყენებს მრავალი ვოლტაჟის დონეს, უმოქმედობისას 9-მდე დონეს ვოლტაჟისა და მონაცემების გადაცემისას 17-მდე ვოლტაჟის დონეს. ამდენი განსხვავებული მდგომარეობის გათვალისწინებით და ხარვეზებთან ერთად სიგნალი უფრო ჰგავს ანალოგურს, ვიდრე ციფრულს და როგორც ანალოგური, ის უფრო მგრძნობიარეა ხარვეზებზე.

1000BASE-SX და 1000BASE-LX ეზერნეტი ოპტიკურ-ბოჭკოვანი გამტარის გამოყენებით. ამ გამტარში, UTP-სგან განსხვავებით, გვაქვს იმუნიტეტი ხარვეზებზე, პატარა ზომა და მეტი დისტანცია (რომელიც არ საჭიროებს გამმეორებლებს) და გამტარუნარიანობა. ორივეს აქვს უზრუნველყოფა სრულ დუპლექსური ორობითი გადაცემისა 1250მბიტ/წამში ერთ წყვილზე. კოდირება დაფუძნებულია 8B/10B კოდირების სქემაზე. თუმცა ამ კოდირების ზედნადებისგან სიჩქარე მაინც 1000მბიტ/წამია. თითოეული მონაცემთა კადრი არის ენკაპსულირებული ფიზიკურ შრეზე გადაცემამდე, არხის სინქრონიზაცია მიიღწევა უწყვეტი ნაკადის გაგზავნით უმოქმედობის კოდის ჯგუფებისა კადრთაშორის დაყოვნების პერიოდში.

1000BASE-SX-სა და 1000BASE-LX-ს შორის პრინციპული განსხვავებაა არხის გამტარი, კონექტორები და ოპტიკური სიგნალის ტალღის სიგრძე.

IEEE 802.3ae სტანდარი იყო ადაპტირებული 10გბიტ/წამში, სრულ დუპლექსური გადაცემისთვის ოპტიკურ კაბელში. ეს სტანდარტი ძალიან ჰგავს 802.3 სტანდარტს (ეზერნეტის ორიგინალური სტანდარტი). 10გბ-იანი ეზერნეტი ვითარდება არა მხოლოდ ლოკალურ ქსელებში გამოსაყენებლად არამედ გლობალურ ქსელებშიც. იმის გამო, რომ კადრის ფორმატი და სხვა ეზერნეტის მეორე შრის სპეციფიკაციები წინა სტანდარტების შესაბამისია, მას შეუძლია უზრუნველყოს მეტი გამტარუნარიანობა უკვე არსებულ ქსელურ ინფრასტრუქტურაში. მისი შედარება სხვა ეზერნეტბთან ამგვარად შეიძლება:

კადრის ფორმატი იგივე, კლასიკურ ეზერნეტთან შესაბამისობა, სწრაფ ეზერნეტთან, გიგაბიტ ეზერნეტთან და 10-გიგაბიტიან ეზერნეტთან, კადრების ან საუბრების პროტოკოლების კონვერტაციის გარეშე. ბიტ დრო არის 0.1 ნანოწამი. რადგან მხოლოდ ოპტიკური გამტარი გამოიყენება, არ არის საჭიროება CSMA/CD-ში. 802.3 ქვეშრეები პირველი და მეორე შრეებისა

უმეტესად დაცულია, რამდენი დანამატით, მხარდაჭერისათვის 40კილომეტრიანი ოპტიკური არხებისთვის და თავსებადობა სხვა ოპტიკურ ტექნოლოგიებთან.

მომავალი ეზერნეტის სიჩქარეები

1 გიგაბიტიანი ეზერნეტი უკვე ფართოდაა გავრცელებული და 10-გიგაბიტიანი ეზერნეტის პროდუქციის აჩევანიც არის. მიმდინარეობს მუშაობა 40, 100 და 160 გიგაბიტიან სტანდარტებზე. ტექნოლოგიების დანერგვა დამოკიდებულია რამდენიმე ფაქტორზე, მათ შორის ტექნოლოგიის და სტანდარტების დაღვინებასა და ბაზარზე მათ გავცელებასა და ფასზე.

კლასიკური ეზერნეტი იყენებს კონცენტრატორს. ის არ ახდენს არავითარ ფილტრაციას მონაცემებისა, ის უბრალოდ გადაამისამართებს მონაცემებს ყველა მოწყობილობაზე, რომლებიც არის ჩართული მათში. ამის გამო ყველა მოწყობილობა ქსელში ინაწილებს გამტარუნარიანობას და დამატებით მათში ხშირად ხდება კოლიზიები. ამ პრობლემებიდან გამომდინარე მას შეზღუდული გამოყენება აქვს დღევანდელ ქსელებში. კონცენტრატორები გამოიყენებზ ან მარტო პატარა ქსელებში, ან იმ ქსელებში, რომლებსაც დაბალი გამტარუნარიანობის მოთხოვნა აქვთ. გამტარის განაწილება იწვევს დიდ პრობლემებს ქსელის გაზრდასთან ერთად.

კონცენტრატორის ქსელში არის ზღვარი გამტარუნარიანობაზე რომელიც მოწყობილობებს შეუძლიათ გამოიყენონ, თითოეული ახალი მოწყობილობის დამატებასთან ერთად, საშუალო გამტარუნარიანობა რომელიც არის ხელმისაწვდომი თითოეული მოწყობილობისათვის მცირდება. თითოეული ნამატით მოწყობილობების რიცხვში ქსელში, შესრულების ხარისხი მცირდება.

დაყოვნება

ქსელური დაყოვნება არის დრო, რომელიც სჭირდება სიგნალს, რომ მიაღწიოს ყველა დანიშნულების ადგილს გამტარზე, თითოეულ მოწყობილობას უწევს ლოდინი კონცენტრატორით აგებულ ქსელში, შესაძლებლობისა სიგნალის გადაცემისთვის, რათა აარიდოს თავი კოლიზიებს. დაყოვნება შეიძლება ძლიერ გაიზარდოს, როცა მანძილი მოწყობილობებს შორის იზრდება. დაყოვნებაზე ასევე მოქმედებს დაყოვნება სიგნალისა გამტარზე და დაყოვნება დამატებული გამოთვლითი ოპერაციებით სიგნალზე, კონცენტრატორის ან გამმეორებლის გავლის დროს. გამტარის სიგრძის მომატება კონცენტრატორების ან გამმეორებლების რაოდენობის მომატება იწვევს დაყოვნების მომატებას. რაც დიდია დაყოვნება, მით დიდია შანსი კოლიზიისა.

ქსელის მარცხი იმიტომ რომ კლასიკური ეზერნეტი იყენებს განაწილებულ გამტარს, ერთი მოწყობილობა შეერთებული კონცენტრატორზე, რომელიც შეიძლება გამოვიდეს მწყობრიდან და დაიწყოს მავნე ტრაფიკი გაგზავნე, შეწყვეტს მუშაობას ყველა

მოწყობილობისთვის გამტარზე. ამ ტრაფიკის მიზეზი შეიძლება იყოს არასწორი სიჩქარის გამო ან სრული-დუპლაქსის რეჟიმის გამო ქსელურ ადაპტერზე.

კოლიზიები

CSMA/CD-ს შესაბამისად, მოწყობილობამ არ უნდა გაგზავნოს პაკეტი, თუ ქსელი თავისუფალი არ არის. თუ ორი მოწყობილობა ერთდროულად გააგზავნის პაკეტებს, კოლიზია მოხდება და პაკეტები გაფუჭდება. შემდგომ ორივე მათგანი გააგზავნის ჩამხშობ სიგნალს, დაიცდიან შემთხვევით დროის რაოდენობას და შემდგომ დაბრუნდებიან მოსმენის რეჟიმში გაგზავნამდე. ქსელის ნებისმიერი ნაწილის, სადაც პაკეტებს შეუძლიათ ერთმანეთთან შეჯახება, კოლიზიური დომეინი ეწოდება. ქსელი, რომელსაც ბევრი მოწყობილობა აქვს ერთ სეგმენტში, წარმოადგენს დიდ კოლიზიურ დომეინს და როგორც წესი, აქვს მეტი ტრაფიკი. ტრაფიკის რაოდენობის გაზრდასთან ერთად იმატებს კოლიზიების რაოდენობაც, სვიჩები წარმოადგენენ ალტერნატივას შეჯიბრზე დაფუძნებული კლასიკური ეზერნეტისა.

ბოლო რამდენიმე წელიწადში სვიჩები გახდნენ უმეტესი ქსელის, ფუნდამენტური ნაწილი სვიჩები ახდენენ სეგმენტაციას ლოკალური ქსელისა კოლიზიურ დომეინებად, თითოეული პორტი სვიჩისა წარმოადგენს განცალკევებულ კოლიზიურ დომეინს და უზრუნველყოფს მოწყობილობას სრული გამტარუნარიანობით. რაც ნაკლებია მოწყობილობა თითოეულ კოლიზიეურ დომეინში, მით მეტია ზრდა საშუალო გამტარუნარიანობისა თითოეული მოწყობილობისათვის და კოლიზიების რიცხვიც მცირდება.

ლოკალურ ქსელს შეიძლება ჰქონდეს ცენტრალური სვიჩი, რომელსაც უკავშირდებიან კონცენტრატორები და მათი მომხმარებლები. ან ლოკალური ქსელში შეიძლება ყველა კოპმიუტერი იყოს შეერთებული სვიჩში. ქსელში, სადაც კონცენტრატორები უკავშირდებიან სვიჩს, კოლიზიები მაინც მოხდება, თუმცა სვიჩი მოახდენს მათ იზოლაციას.

მოწყობილობები პირდაპირ არიან ჩართულნი

ლოკალურ ქსელში, სადაც ყველა მოწყობილობა პირდაპირ არის ჩართული სვიჩში. ქსელის გამტარუინარიანობა ძლიერ იზრდება. ამის სამი ძირითადი მიზეზია:

- თითოეული პორტისათვის გამოყოფილი გამტარუნარიანობა
- უკოლიზიო გარემო
- სრული დუპლექსის რეჟიმი
- გამოყოფილი გამტარუნარიანობა

თითოეულ მოწყობილობას მედიის სრული გამტარუნარიანობა აქვს კავშირში მოწყობილობასა და სვიჩს შორის. კონცენტრატორი ყველა მოწყობილობას რომ უგზავნის მიღებულ სიგნალებს, ეს ნიშნავს, რომ სალტის მთლიანი გამტარუნარიანობა უნდა

განაწილედეს ყველა მოწყობილობას შორის სვიჩებში თითოეულ მოწყობილობას აქვს გამოყოფილი კავშირი მოწყობილობასა და სვიჩს შორის. გამტარზე შეჯიბრის გარეშე.

მაგალითისთვის შევადაროთ ორი სწრაფი ეზერნეტის ლოკალური ქსელი, თითოეულზე 10 მოწყობილობით, ქსელის სეგმენტი ა-ში, 10 მოწყობილობა არის ჩართული კონცენტრატორში. და თითოეული მოწყობილობა ინაწილებს ამ 100მბიტ/წამს. ეს იძლევა საშუალო10მბიტ/წამს. ქსელის სეგმენტ ბ-ში. 10 მოწყობილობა ჩართულია სვიჩში, ამ სეგმენტში 10-ვე მოწრობილობას აქვს სრული 100მბიტ/წამ გამტარუნარიანობა მათ შორის.

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

უკოლიზიო გარემო

მიძღვნილ კავშირში(წეტილიდან-წერტილამდე) სვიჩთან ასევე აუქმებს ნებისმიერი სახის შეჯბრს მოწყობილობათა შორის. და ნებას რთავს მოწყობილობას იმუშაოს ცოტა ან საერთოდ კოლიზიების გარეშე. საეშუალო ზომის კლასიკური ეზერნეტის ქსელებში კონცენტრატორების გამოყენებით 40%-დან 50%-მდე არის კოლიზიებიდან გამოსვლა. სვიჩიან ეზერნეტ ქსელში ეს თითქმის 0-ის ტოლია. და ეს ანიჭებს სვიჩიან ქსელებს საგრძნობლად უკეტესს გამტარუნარიანობას.

ეზერნეტის უკაბელო სტანდარტები

IEEE 802.11 არის სტანდარტი, რომელშიც არის აღწერილი უკაბელო ქსელების კავშირგაბმულობა, 802.11 კი – სტანდარტების ჯგუფი, რომელიც შედგება შემდეგი სტანდარტებისგან : 802.11a, 802.11b, 802.11g და 802.11n. ეს პროტოკოლები აღწერეს ხვადასხვა უკაბელო სტანდარტის სიხშირეებს, სიჩქარეებს და სხვა შესაძლებლობებს.

802.11a
ამ სტანდარტით მომუშავე მოწყობილობები 54 მბ/წმ სიჩქარეს აღწევენ. და მოქმედებენ 5გიგაჰერც სიხშირეზე, მათი მაქსიმალური დაფარვის ზონა 45.7 მეტრია.
802.11b
ეს მოწყობილობები მოქმედებენ 2.4 გიგაჰერც სიხშირეზე მაქსიმალური თეორიული სიჩქარით. და მათი მაქსიმალური დაფარვის ზონა არის 91მეტრი.
802.11g
ამ სტანდარტს ისეთივე თეორიული მაქსიმალური სიჩქარე აქვს, როგორ 802.11a-ს, რაც არის 54მბ/წმ, მაგრამ მუშაობის სიჩქარე ისეთივე აქვს, რაც 802.11b-ს 2.4 გიგაჰერცზე. თუმცა ზემოთ ხსენებული ორი სტანდარტისგან განსხვავებით ეს სტანდარტი თავსებადია 802.11b სტანდარტთან და მისი მაქსიმალური დაფარვის ზონა არის 91 მეტრია.

802.11n
ეს სტანდარტი არის უფრო ახალია, და აქვს მაქსიმუმ 540 მბ/წმ თეორიული სიჩქარე, მუშაობს ან 2.4, ან 5 გიგაჰერც სიხშირეზე, 250 მეტრი მაქსიმალური დაფარვის ზონით.

OSI მოდელი, TCP/IP მოდელი.
OSI და TCP/IP მოდელების შედარება

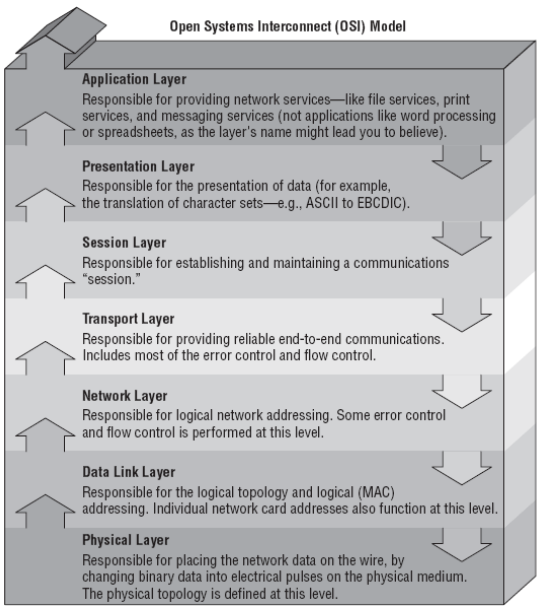
OSI მოდელი

სტანდარტიზაციის საერთაშორისო ორგანიზაციამ (ISO) წარმოადგინა ღია სისტემების ურთიერთდაკავშირება (Open Systems Interconnection), რათა მოეწოდებინა საერთო გზა ქსელის პროტოკოლების განმარტებისთვის. მათ წარმოადგინეს 7-დ შრიანი მოდელი, ურთიერთობა კომუნიკაციის ეტაპებს შორის თითო შრის მიერ ხდება მონაცემის დამატება ზედა ან ქვედა შრისთვის.

OSI მხოლოდ მოდელია მისი გამოყენება შეუძლებელია, ვერ იპოვით ქსელს, რომელიც მუშაობს ამ პროტოკოლით.

ეს მოდელი შემდეგში მდგომარეობს: როდესაც ხდება გადაცემა, მონაცემი მოგზაურობს ზედა შრიდან ქვედა შრეებისკენ, როდესაც მონაცემი გადის შრეში, ის ამატებს თავსართს (Header) მასსზე, ხოლო ზოგიერთ შრეს შეუძლია დაამატოს ბოლოსართიც (Trailer). ასე გრძელდება ბოლო შრემდე და შემდეგ ხდება მონაცემების გადაცემა კაბელში.

მიმღებ წერტილში ყველაფერი უკუღმა ხდება, მონაცემის მიღების შემდეგ პირველი შრე აშორებს მონაცემს თავსართსა და ბოლოსართს და გადასცემს დარჩენილს ზედა შრეზე და ასე გრძელდება, სანამ მონაცემი არ მიაღწევს ბოლო შრეს.



OSI მოდელის შრეები ჩამოთვლილია ზემოდან – ქვემოთ.

- Application Layer – პროგრამული შრე
- Presentation Layer – წარმომადგენლობითი შრე
- Session Layer – სასესიო შრე
- Transport Layer – სატრანსპორტო შრე
- Network Layer – ქსელური შრე
- Data Link Layer – არხული შრე
- Physical Layer – ფიზიკური შრე

ფიზიკური შრე

ფიზიკური შრე განსაზღვრავს, თუ როგორ იგზავნება მონაცემები ფიზიკურ გარემოში. ეს შრე განსაზღვრავს, რა სიგბრის უნდა იყოს თითოეული გადაცემული მონაცემის ნაჭერი, და თარგმნის მას ელექტრულ პულსებში კაბელში გასაგზავნად. ის წყვეტს, მან ერთმხარეს უნდა იმოგზაუროს, თუ ორ მხარეს აპარატურაში. ის ასევე აკავშირებს ელექტრულ, ოპტიკურ, მექანიკურ და ფუნქციურ ინტერფეისებს კაბელზე.

არხული შრე

არხული შრე მონაცემებს აწყობს ნაჭრებში, რომლებსაც ჰქვიათ ფრეიმები (Frames). ამ ნაჭრებში არის განთავსებული საკონტროლო ინფორმაცია, რომელიც აღნიშნავს ნაკადის დასაწყისსა და დასასრულს. ეს ძალიან მნიშვნელოვანი შრეა, რადგან გვაძლევს საშუალებას შევამოწმოთ შეცდომების არსებობა მონაცემებში და ამარტივებს მათ გადაცემას. არხული შრე ასევე ახასიათებს ქსელური ადაპტერის უნიკალურ ფიზიკურ მისამართს (ასევე ცნობილს როგორც MAC მისამართი).

ქსელური შრე

ქსელური შრე ამისამართებს შეტყობინებებს და თარგმნის ლოგიკურ მისამართებს ფიზიკურ მისამართებად. ამ შრეზე მონაცემები პაკეტების (Packets) სახით არის წარმოდგენილი, მას აქვს საშუალება განსაზღვროს საუკეთესო გზა პაკეტების გასაგზავნად, ამისთვის იყენებს ისეთ მონაცემებს, როგორიც არის ქსელის დატვირთვის მდგომარეობა, პრიორიტეტი და ა. შ. იგი შემდეგი ხერხებით ახორციელებს ტრეფიკის მართვას: პაკეტების კომუტაციით, მარშრუტიზაციით და მონაცემთა გადატვირთვის კონტროლით.

სატრანსპორტო შრე

ეს შრე გამოსცემს სიგნალს „ყველაფერი კარგად არის“ მას შემდეგ, რაც შეამოწმებს, რომ მონაცემთა სეგმენტებში არ არის შეცდომები. ასევე ის აკონტროლებს მონაცემთა ნაკადს და აღმოაჩენს და ასწორებს შეცდომებს გადასაცემ ან მიღებულ მონაცემთა დიაგრამებში (DATAGRAM). მისი უმთავრესი დანიშნულება არის შეცდომების არსებობის შემოწმება და წერტილიდან-წერტილამდე საიმედო კომუნიკაციაა.

სასესიო შრე

სასესიო შრე საშუალებას აძლევს პროგრამებს სხვადასხვა კომპიუტერიდან დაამყარონ კავშირი, შემდეგ გამოიყენონ ეს კავშირი და ბოლოს დაამთავრონ ურთიერთობა. მას შემდეგ, რაც სესია დამთავრდება, ახალი პროცესი იწყება, ეს შრე შესაძლებელს ხდის ქსელის პროცედურებს როგორიც არის პაროლების იდენტიფიცირება და ქსელის მონიტორინგი. მას ასევე შეუძლია მართოს აღდგენა ქსელის დაზიანებიდან.

წარმომადგენლობითი შრე

ეს შრე განსაზღვრავს „გარეგნობას“ ან ფორმატს მონაცემებისა, ქსელური უსაფრთხოებისა და ფაილების გადაცემისა. ეს შრე უზრუნველყოფს პროტოკოლის გარდაქმნას და მართავს მონაცემთა შეკუმშვას, თარგმნას და დაშიფრვას.

პროგრამული შრე

პროგრამული შრე ნებას რთავს ქსელის მომსახურებებთან შეღწევას, ის არის შრე, რომელზეც ფაილურე და საბეჭდი მომსახურებები მუშაობენ, ის ასევე არის შრე, რომელზეც სამუშაო მანქანები ურთიერთქმედებენ.

სურათზე ნაჩვენებია მთელი ოსი მოდელი. დააკვირდით ურთიერთობას შრეებს შორის და მათ ფუნქციებს.

TCP/IP Model	Layer	Description
Application	4	Where high-level protocols such as SMTP and FTP operate
Transport	3	Where flow-control and connection protocols exist
Internet	2	Where IP addressing and routing take place
Network Access	1	Where MAC addressing and physical components of network exist

TCP/IP მოდელი

არის საერთო სამუშაო მოდელი რომლის მიხედვითაც არის აგებული ინტერნეტი. ის შეიცავს შრეებს რომლებიც არიან აუცილებელნი მონაცემების მოსამზადებლად ქსელში გადასაცემად.

სურათზე შეგიძლიათ იხილოთ ამ მოდელის ოთხი შრე.

მესიჯი იწყება ზედა შრეზე და მოგზაურობს ქვევით TCP/IP მოდელის შრეებზე, სანამ არ მიაღწევს უკანასკნელს. ქსელური წვდომის შრე, თავსართი ემატება მესიჯს თითოეულ შრეზე, როდესაც ის მოგზაურობს და შემდგომ ხდება მისი გაგზავნა. მას შემდეგ, რაც ის მიაღწევს დანიშნულების ადგილს, ის მოგზაურობს ქვემოდან ზემოთ TCP/IP მოდელის შრეებზე, ამ დროს ხდება თავსართის, რომელიც მესიჯზე იქნა დამატებული, მოშორება.

გამოყენებითი შრის პროტოკოლები

ამ შრის პროტოკოლები გვაწვდიან ქსელურ მომსახურეობებს სამომხმარებლო პროგრამებზე გამოსაყენებლად, ასეთი პროგრამების მაგალითია ვებ ბრაუზერები, მეილის გასაგზავნი/მისაღები პროგრამები.

ტრანსპორტის შრის პროტოკოლები

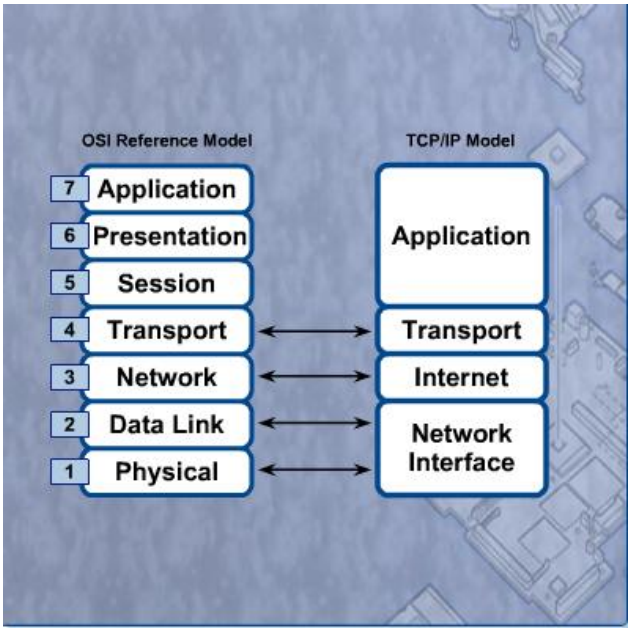
ამ შრის პროტოკოლები გვთავაზობენ საუშუალებას მონაცემის მართვის წერტილიდან-წერტილამდე. მისი ერთ-ერთი ფუნქცია არის მონაცემების დაყოფა უფრო მართვად სეგმენტებად, რომელთა გაგზავნაც უფრო ადვილია ქსელში.

ინტერნეტის შრის პროტოკოლები

ამ შრის პროტოკოლები არიან ზემოდან მესამე შრეზე TCP/IP მოდელში. ეს პროტოკოლები გვეხმარებიან უზრუნველვყოთ კავშირგაბმულობა ქსელში ჰოსტებს შორის.

ქსელური წვდომის პროტოკოლები

ეს პროტოკოლები აღწერენ სტანდარტებს, რომლებიც ჰოსტებმა უნდა გამოიყენონ ფიზიკურ გამტართან კავშირისთვის. ეზერნეტის ისეთი სტანდარტები და ტექნოლოგიები, როგორებიც არის CSMA/CD და 10BASE-T, აღიწერებიან ამ შრეში.



ოსი მოდელი და TCP/IP მოდელი ორივე არის მოდელი, რომელიც გამოიყენება მონაცემთა კავშირგაბმულობის პროცესის აღწერისათვის. TCP/IP მოდელი გამოიყენება კონკრეტულად TCP/IP პროტოკოლთა ნაკრებთან სამუშაოდ. ხოლო OSI მოდელი გამოიყენება სტანდარტული კავშირგაბმულობის ჩამოყალიბებისათვის სხვადასხვა მწარმოებლის აპარატურულ უზრუნველოყოფას შორის.

TCP/IP მოდელი ასრულებს იმავე პროცესს, რომელსაც OSI მოდელი, თუმცა იყენებს ოთხ შრეს შვიდი შრის მაგივრად. სურათზე ნაჩვენებია, რომელი შრე რომელ შრეს შეესაბამება.

ქსელის ადაპტერის ინსტალაცია ან განახლება, კომპიუტერის დაკავშირება არსებულ ქსელთან, მოდემის ინსტალაცია სატელეფონო ტექნოლოგიების აღწერა, ძაბვის გადამცემი ხაზის კავშირგაბმულობა, Broadband კავშირი და VOIP-ი

ინტერნეტთად დასაკავშირებლად საჭიროა ქსელური ადაპტერი. ის შეიძლება იყოს ინტეგრირებული ან გაფართოების ადაპტერის სახით. ზოგიერთ შემთხვევაში შეიძლება დაგჭირდეთ დრაივერის განახლება, ამისათვის შეგიძლიათ გამოიყენოთ დისკი, რომელიც მოყვა დედაპლატას ან ვიდეო ადაპტერს, ან მოიძიოთ ინტერნეტით მოწყობილობის მწარმოებლის ვებგვერდზე.

მას შემდეგ, რაც მოხდება ქსელური ადაპტერის და დრაივერის დაყენება, თქვენ შეგიძლიათ დაუკავშირდეთ ქსელს.

ამას გარდა, ინტერნეტთან დასაკავშირებლად შეიძლება დაგჭირდეთ მოდემის დაყენება.

ზოგჯერ მწარმოებელი გამოაქვეყნებს ახალ დრაივერს ქსელური ადაპტერისთვის. ახალმა დრაივერმა შეიძლება გააუმჯობესოს მოწყობილობის ფუნქციები ან შეუთავსოს ახალ ოპერაციულ სისტემას.

ახალი დრაივერის დაყენებისას გათიშეთ ანტივირუსი, რათა ყველა ფაილის კოპირება სწორად მოხდეს. ზოგიერთი ანტივირუსი აღიქვამს ქსელური ადაპტერის განახლებას როგორც ვირუსს.

ასევე მხოლოდ ერთი დრაივერის დაყენება უნდა მოხდეს დროის ერთ მომენტში. რადგანაც წინააღმდეგ შემთხვევაში შესაძლებელია რამდენიმე პროცესს ერთმანეთთან კონფლიქტი მოუვიდეს.

გამოცდილებიდან გირჩევთ, რომ დახუროთ ყველა პროგრამა დრაივერის დაყენების წინ, რათა არ მოხდეს რომელიმე პროგრამის მიერ იმავე ფაილის გამოყენება და ხელის შეშლა დრაივერის დაყენების პროცესისთვის. განახლების წინ აუცილებლად ნახეთ მწარმოებლის ვებ გვერდი, რადგან მასში ხშირად გვხდება ავტომატურად დაყენებადი (self-extracting executable) ფაილი, რომელიც ავტომატურად დააყენებს ან განაახლებს დრაივერს. ალტერნატიულად თქვენ შეგიძლიათ შეხვიდეთ device manager-ში და იქ აირჩიოთ Update Driver ღილაკი.

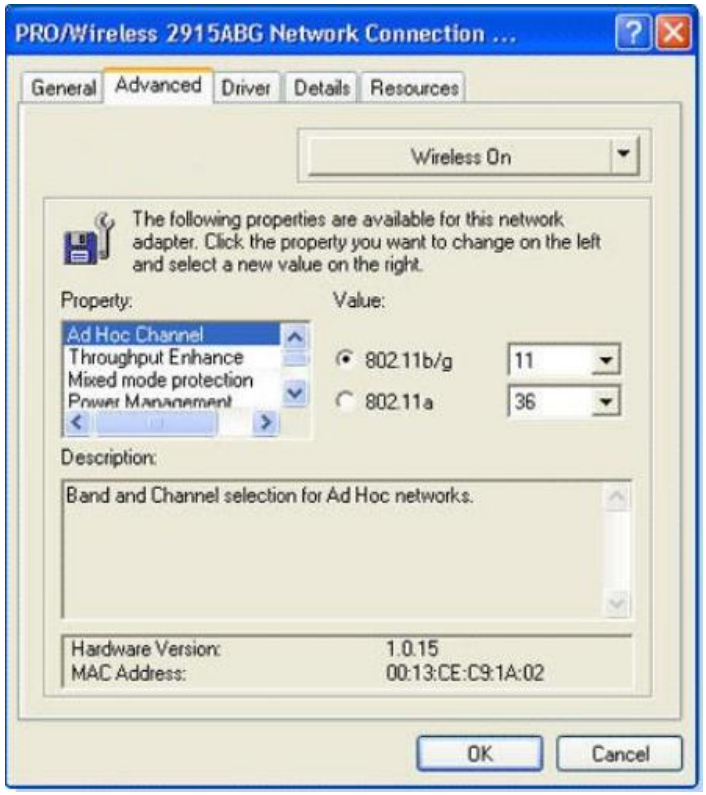
ქსელური ადაპტერების წინ მდება „+“ გაძლევთ საშუალებას ჩამოშალოთ სია ყველა ადაპტერისა, რომლებიც არის დაყენებული თქვენს კომპიუტერზე. იმისთვის, რომ დაათვალიეროთ ან შეცვალოთ ქსელური ადაპტერის პარამეტრები, ორჯერ დააჭირეთ მას.

მას შემდეგ, რაც დასრულდება განახლება, კარგი იქნებოდა გადაგეტვირთათ კომპიუტერი იმისდა მიუხედავად, გამოვა თუ არა ეკრანზე შესაბამისი მოთხოვნა. გადატვირთვის შემდეგ დარწმუნდებით, რომ თქვენ მიერ განხორციელებული განახლება წარმატებით იქნა დაყენებული და ახალი დრაივერი სწორად მუშაობს. როდესაც აყენებთ რამდენიმე დრაივერს, გადატვირთეთ კომპიუტერი თითოეული დრაივერის დაყენების შემდეგ რათა დარწმუნდეთ, რომ არ არის წინააღმდეგობა

განახლებებს შორის. ამ ნაბიჯით თქვენ უზრუნველყოფთ სუფთა ინსტალაციას იმისდა მიუხედავად, რომ ცოტა მეტი დრო დაგჭირდათ.

ქსელური მოწყობილობის დრაივერების წაშლა ან ძველ მდგომარეობაში დაბრუნება. ამისთვის უნდა შეხვიდეთ Device Manager-ში, შედით ადაპტერის პარამეტრებში და აირჩიეთ დრაივერი და Roll Back Driver. თუმცა თუ დრაივერი არ იყო დაყენებული მანამდე, მაშინ ეს ფუნქცია არ იქნება გააქტიურებული. ამ შემთვევაში მოგიწევთ დრაივერის მოძებნა და დაყენება, თუ ოპერაციულმა სისტემამ ვერ იპოვა თვითონ.

მას შემდეგ, რაც ქსელური ადაპტერის დრაივერს დააყენებთ, თქვენ ხართ მზად დაუკავშირდეთ ქსელს. შეაერთეთ ქსელური კაბელი, ასავე წოდებული ეზერნეტის straight-though კაბელად, კომპიუტერის ქსელურ პორტში, მეორე ბოლო შეაერთეთ ქსელურ მოწყობილობაში ან კედელზე არსებული აუტლეტში.



ქსელური კაბელის და შევხედავთ შუქდიოდს, ეზერნეტის პორტის გვერძე, და ის გვატყობინებს ქსელში აკტივობის შესახებ, თუ არ არის აკტივობა ქსელში. შესაძლო პრობლემა შეიძლება იყოს კაბელში. დაზიანებულ პორტში ან გაფუჭებულ ქსელურ ადაპტერში. პრობლემის აღმოსაფხვრელად შეიძლება მოგიწოთ ზემოთ ხსენებული ერთი რომელიმე ან რამდენიმე მოწყობილობის შეცვლა.

ამ პრობლემის აღმოიფხვრს შემდეგ უნდა გადახვიდეთ კომპიუტერზე IP მისამართის დაყენებაზე, ქსელების უმეტესობა შეიცავს DHCP სერვერს, რომლის მეშვეობითაც ავტომატურად მოხდება პარამეტრების მინიჭება კომპიუტერზე. სხვა შემთხვევაში უნდა დააყენოთ პარამეტრები ხელით. ამის შემდეგ შეამოწმეთ კავშირი ბრძანება PING-ის მეშვეობით. პირველ რიგში დაპინგეთ default gateway, თუ მასთან კავშირი იქნება და ჩვენ უნდა გვქონდეს კავშირი ინტერნეტთან მასინ სცადეთ დაპინგოთ რაიმე ცნობილი ვებ გვერდი.

მრავალი გზა არსებობს ინტერნეტთან დასაკავშირებლად: სატელეფონო, კაბელური, სატელიტური და კერძო კომპანია გვთავაზობენ ინტერნეტ კავშირს ბიზნესისთვის და სახლისთვის.

1990-იან წლებში ინტერნეტი, როგორც წესი, გამოიყენებოდა მონაცემების გადასაცემად. გადაცემის სიჩქარე დღევანდელთან შედარებით ნელი იყო. ინტერნეტთან დასაკავშირებლად ყველაზე ხშირად გამოიყენებოდა ანალოგური მოდემები, რომლებიც იყენებდნენ ჩვეულებრივ სატელეფონო ქსელს (POTS) ინფორმაციის გადასაცემად და მისაღებად. უკანასკნელ წლებში მრავალი მომხმარებელი გადაერთო სწრაფ ინტერნეტ კავშირზე, რაც იძლევა დამატებით გამტარუნარიანობას, რომლითაც შეგვიძლია გადავცეთ ხმოვანი და ვიდეო მონაცემებიც.

სატელეფონო ტექნოლოგიები

არსებობს რამდენიმე ტექნოლოგია ინტერნეტთან დასაკავშირებლად. სხვადასხვა ტექნოლოგიას სხვადასხვა სიჩქარე და მომსახურების დონე აქვს. სანამ გადაწყვეტდეთ რომელიმეს არჩევას, კარგად გამოიკვლიეთ ყველა არსებული და განსაზღვრეთ, რომელი იქნება საუკეთესო თქვენთვის.

ანალოგური სატელეფონო კავშირი

ეს ტექნოლოგია იყენებს სტანდარტულ სატელეფონო ხაზებს, ეს ტექნოლოგია იყენებს მოდემს, რათა დაუკავშირდეს მეორე მოდემს (რომელიც დგას ატს-ში ან ნებისმიერ სხვა ადგილას). რამდენიმე ნაკლი კი აქვს მას – პირველი ის არის რომ იმ დროს როდესაც გვაქს დამყარებული კავშირი, არ შეიძლება ტელეფონით დარეკვა, ხოლო მეორე ის არის დაბალი სიჩქარე, რომელიც არის შეზღუდვა ამ ტექნოლოგიის გამოყენებისას, 56კბ/წამი. თუმცა რეალურად როგორც წესი ეს უფრო დაბალი ციფრია. ანალოგური მოდემი არ არის კარგი გამოსავალი დატვირთული ქსელებისათვის.

ინტერგრირებული მომსახურებების ციფრული ქსელი (ISDN)

შემდეგი ნაბიჯია ჩვენი ტექნოლოგიის განვითარებაში. ეს სტანდარტი გამოყენება ხმის, ვიდეოს და მონაცემების გადასაცემად ჩვეულებრივი სატელეფონო სადენების მეშვეობით. იმისდა მიუხედავად, რომ გამტარი ისეთივეა, როგორიც ანალოგურ ქსელში, ის ციფრულ მეთოდს იყენებს ინფორმაციის გადაცემისთვის და ამის გამო გვთავაზობს უფრო სწრაფ და ხარისხიან კავშირს ანალოგურ კავშირთან შედარებით.

არსებობს სამი ტიპი ამ კავშირისა: Basic Rate Interface (BRI), Primary Rate Interface (PRI) და Broadband ISDN (BISDN). ეს ტექნოლოგია იყენებს 2 არხს გადასაცემად. B არხი

გამოიყენება ინფორმაციის გადასაცემად (ხმა, ვიდეო და ა.შ.), ხოლო D არხი – კონტროლისათვის, თუმცა მისი გამოყენება მონაცემების გადასაცემადაც შეიძლება.

DSL

ამ ტექნოლოგიის შემთხვევაში კავშირი ყოველთვის დამყარებულია, შესაბამისად ჩვენ არ გვჭირდება დაკავშირება (dial up) ყოველ ჯერზე, როდესაც მოგვინდება ინტერნეტში შესვლა. ამას ეწოდება Always On. ეს ტექნოლოგია გვთავაზობს სწრაფ კავშირს არსებული სატელეფონო გამტარის გამოყენებით. თუმცა ISDN-ისგან განსხვავებით ანალოგური სიგნალი არ იცვლება ციფრულით, არამედ ხდება შეთავსება ციფრულის და ანალოგური სიგნალის. სატელეფონო კომპანია ადებს ლიმიტს გამტარუნარიანობას, რომლის გამოყენებაც შეუძლია ანალოგურ ხმას. რაც გვაძლევს საშუალებას ციფრული სიგნალისათვის გამოვიყენოთ დარჩენილი ნაწილი და ერთდროულად ვისარგებლოთ ტელეფონითაც და ინტერნეტითაც.

ამ ტექნოლოგიას შეზღუდვებიც აქვს, სატელეფონო სადგურიდან დიდი მანძილით არ უნდა იყოს დაცილებული. იმის გამო, რომ სატელეფონო კაბელი იყო შექმნილი ანალოგური სიგნალის გასატარებლად, ციფრული სიგნალის მილევადობა ხდება გარკვეული მანძილის შემდგომ. ასევე არის გასათვალისწინებელი ის ფაქტიც, რომ მომხმარებლის მხარეს უნდა მოხდეს განცალკევება ინტერნეტ კავშირისა და ხმოვანი ზარების, ეს ხდება მოწყობილობის მეშვეობით, რომელსაც ეწოდება splitter-ი.

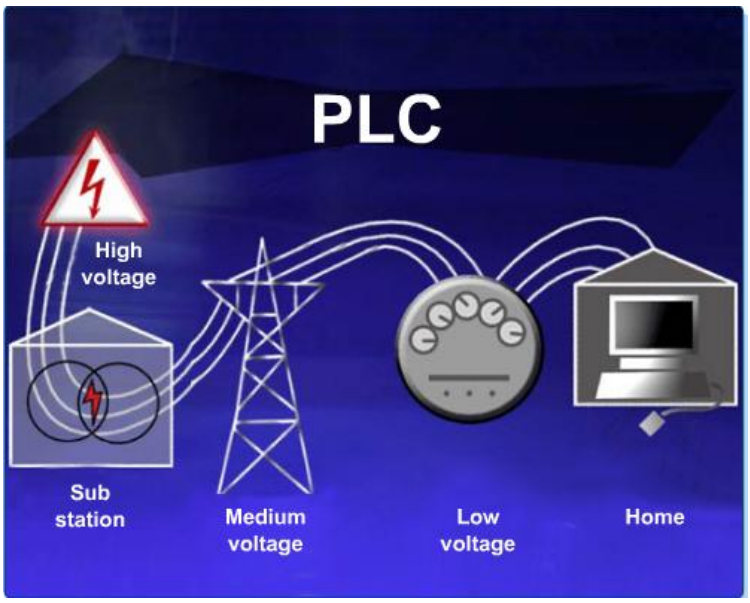
ასიმეტრიული DSL

დღესდღეობით ყველაზე ხშირად ამ ტექნოლოგიას იყენებნ. მას განსხვავებული შესაძლებლობები აქვს მიმართულებით ინფორმაციის გადაგზავნისას. უფრო სწრაფად მიიღებთ ინფორმაციას, ვიდრე გააგზავნით. ეს ტექნოლოგია ხელსაყრელია მათთვის, ვინც იწერს დიდი რაოდენობით ინფორმაციას, მაგრამ ვისაც აქვს რაიმე სერვერი, რომელთანაც კავშირი მყარდება ინტერნეტიდან და შემდეგ ამ სერვერიდან ტვირთავენ ინფორმაციას, ეს ტექნოლოგია გამოუსადეგარია.

ძაბვის გადამცემი ხაზის კავშირგაბმულობა

ეს მეთოდი იყენებს ძაბვის გადამცემ ხაზებს ინფორმაციის მისაღებად და გადასაცემად.

ამ ტექნოლოგიის მეშვეობით თელასის ტიპის კომპანიას შეუძლია დაადოს ანალოგური სიგნალი



სტანდარტულ 50 ან 60 ჰერციან ცვლად დენს, რომელიც მოგზაურობს გამტარში. ანალოგურ სიგნალს შეუძლია გადასცეს ხმოვანი და მონაცემთა სიგნალები. ეს ტექნოლოგია შესაძლებელია იქ იყოს ხელმისაწვდომი, სადაც სხვა ტექნოლოგია არ არის ხელმისაწვდომი. ეს ტექნოლოგია უფრო სწრაფი ანალოგურ მოდემთან შედარებით და გაცილებით იაფის სხვა სწრაფ გადაწყვეტილებებთან შედარებით. ამ ტექნოლოგიის განვითარებასთან ერთად მისმა სიჩქარემ შესაძლოა იმატოს და ჰპოვოს მეტი გავრცელება. მისი გამოყენება კომპიუტერების ერთმანეთთან დასაკავშირებლად ბინებშიც შეიძლება, რადგან ყველგან მუშაობს, სადაც არის დენის აუტლეტი (გასართი).

Broadband არის მეთოდი ერთი გამტარის მეშვეობით რამდენიმე სიგნალის გაგზავნისა და მიღების. მაგალითად, კაბელს, რომლითაც ტელევიზია შემოდის თქვენთან სახლში, შეუძლია ამავდროულად დაგაკავშიროთ ინტერნეტთანაც, რადგანაც ეს ორი გადაცემის ტიპი იყენებს სხვადასხვა სიხშირეს და ერთმანეთს არ უშლის. რამდენიმე მაგალითი ასეთი კავშირის მეთოდისა არის კაბელური, DSL, ISDN და სატელიტური კავშირი.

კაბელური

კაბელური მოდემი თქვენს კომპიუტერს კაბელურ კომპანიასთან იმავე კოაქსიალური კაბელის გამოყენებით აკავშირებს, რომელიც ერთდება თქვენს ტელევიზორში. თქვენ პირდაპირ შეგიძლიათ შეაერთოთ თქვენი კომპიუტერი კაბელურ მოდემში ან მარშრუტიზატორში, კომუტატორსა ან მსგავს მოწყობილობაში, რათა გამოიყენოთ კავშირი მრავალ კომპიუტერთან.

DSL

ამ ტექნოლოგიის გამოყენების დროს გვესაჭიროება ფილტრი რათა DSL-ის სიგნალებმა არ შეუშალონ ტელეფონის სიგნალებს. DSL მოდემი შეიძლება პირდაპირ უკავშირდებოდეს კომპიუტერს ან ქსელურ მოწყობილობას, რომელზეც იქნება დაკავშირებული რამდენიმე მოწყობილობა.

ISDN

იმის გამო, რომ ეს ტექნოლოგია იყენებს რამდენიმე არხს და შეუძლია სხვადასხვა ტიპის მომსახურების გადაცემა. ისიც შედის ამ ჯგუფში.

სატელიტური კავშირი

სატელიტური კავშირი გამოიყენება მაშინ, როდესაც მომხმარებელს ესაჭიროება სწრაფი ინტერნეტი, მაგრამ ვერც DSL-ით და ვერც კაბელური კავშირით სარგებლობს. ამ ტექნოლოგიის დროს გადმოწერის სიჩქარე აღწევს 500კბ/წმ-ს, ხოლო უტვირთვის 56კბ/წმ-ს.

ვოიპი (Voice over IP)

ამ მეთოდის წყალობით სატელეფონო კავშირი მტარდება მონაცმთა ქსელების და ინტერნეტის გამოყენებით. ეს ტექნოლოგია ანალოგურ სიგნალს რომელიც არის ჩვენი ხმა, გარდაქმნის ციფრულ სიგნალად და აგზავნის მას IP პაკეტების მეშვეობით. ამ ტექნოლოგიის გამოყენებისას თქვენ ხართ დამოკიდებულნი ინტერნეტზე და თუ ის არ არის სტაბილური და ხარისხიანი, არ გირჩევთ მის გამოყენებას.

DOS შეტევა, სპამი და სარეკლამო ფანჯრები, social engineering, TCP/IP შეტევები

არსებული საფრთხეების (Viruses, Worms, Trojans) აღწერა, ვებ უსაფრთხოება, adware, spyware, grayware-ის აღწერა

DOS შეტევა (Denial of service – მომსახურეობაზე უარის თქმა) არის შეტევის ფორმა, რომელიც ხელს უშლის მომხმარებლების ისარგებლონ, მაგ., იმეილით ან ვებ სერვერით. ეს ხორციელდება დიდი რაოდენობით მოთხოვნების გაგზავნით სისტემურ რესურსებზე და იწვევს მათ გადატვირთვას, რასაც ჩვეულებრივი მომხმარებლის უგულვებელყოფა მოყვება.

ფართოდ გავრცელებული DOS შეტევების ტიპებია:

- Ping of death – სიკვდილის პინგი, ეს არის ჩვეულებრივზე დიდი ზომის გარკვეული რაოდენობა პინგების გაგზავნის მეთოდი.
- E-mail bomb – იმეილის ბომბი, ეს არის დიდი რაოდენობით იმეილის გაგზავნა სერვერზე, რათა ხელი შეეშალოს მომხმარებლების სერვერთან დაკავშირებას.

Distributed DoS (DDoS) არის განსხვავებული სახეობა შეტევისა, ის იყენებს მრავალ ინფიცირებულ კომპიუტერს, რომლებსაც ეწოდება zombies, რათა განახორციელოს შეტევა. იმის გამო, რომ კომპიუტერები გეოგრაფიულად დაცილებულ ადგილებში მდებარეობენ, ძალიან რთულია პოვნა შეტევის წყაროსი.

სპამი, როგორც წესი, არის გადასაყრელი წერილები, ძირითადად სარეკლამოა, თუმცა ზოგჯერ გამოიყენება ისეთი ლინკების გასაგზავნად, რომლებზეც თქვენ შეხვდებით მომატყუებელ შიგთავსს.

როდესაც ის გამოიყენება როგორც შეტევის მეთოდი, შეიძლება შეიცავდეს, დაინფიცირებული ვებ გვერდების ლინკებს. ეს ლინკები ისეა შემუშავებული, რომ მიიპყრონ თქვენი ყურადღება და მიგიყვანონ სარეკლამო ვებ გვერდებზე. ამ ფანჯრებს ეწოდებათ პოპაპები (popups). უკონტროლო პოპაპებმა შეიძლება სწრაფად დაფაროს ეკრანი და არ მოგვცენ მუშაობის გაგრძელების საშუალება. მრავალი ანტივირუსული და საფოსტო პროგრამული უზრუნველყოფა ავტომატურად ამოიცნობს და შლის სპამს შემომავალი ყუთიდან, თუმცა ზოგიერთი სპამ წერილი შესაძლოა მაინც გამოეპაროს ამა თუ იმ ფილტრს. ამიტომ თქვენ, უნდა დააკვირდეთ შემდეგ პუნქტებს:

- წერილს არა აქვს სათაური
- პასუხის გასაცემი მისამართი არასრულია
- კომპიუტერის მიერ გენერირებული წერილები
- უკან მოსული წერილები, რომლებიც არ გაგიგზავნიათ

„სოციალური ინჟინერი“ ეწოდება ადამინს, რომელმაც ტყუილებითა და ხრიკებით მიაღწია აპარატურამდე ან მოხვდა ქსელში. ის ახერხებს თანამშრომლის ნდობის მოპოვებას, დაარწმუნებს მომხმარებლის სახელის და პაროლის გამხელის აუცილებლობაში. მას შეუძლია თავი წარადგინოს როგორც ტექნიკოსმა, რათა შეაღწიოს დაწესებულებაში. მას შემდეგ, რაც მოხვდება შენობაში, შეუძლია მოიპოვოს ინფორმაცია ბევრი გზით, მაგ., დახედოს მაგიდებზე გაშლილ ქაღალდებს და თუ წერია პაროლები ან სატელეფონო ნომრები, შეუძლია ხელთ ჩაიგდოს სია თანამშრომლების საფოსტო ყუთების მისამართებისა. და ა.შ.

ჩამოთვლილი ქმედებები დაგეხმარებათ თავიდან აიცილოთ ამგვარი საფრთხე:

- არასოდეს არავის გაუმხილოთ თქვენი პაროლი
- ყოველთვის მოითხოვეთ საიდენტიფიკაციო ბარათი უცნობი პირებისაგან
- შეზღუდეთ მოულოდნელ სტუმრების შემოსვლა
- მარტო ნუ დატოვებთ სტუმარს
- არასოდეს არ დაწეროთ თქვენი პაროლი თქვენს სამუშაო სივრცეში
- დაბლოკეთ კომპიუტერი, როდესაც ტოვებთ მას
- არ დართო ნება არავის, შემოგყვეთ კარში, რომელსაც ესაჭიროება ელექტრონული გასაღები

TCP/IP არის პროტოკოლების ნაკრები, რომელიც გამოიყენება მთელი კომუნიკაციის გასაკონტროლებლად ინტერნეტზე. თუმცა ასევე მას შეუძლია გახდეს სუსტი წერტილი ქსელში.

ზოგიერთი ყველაზე გავრცელებული შეტევის ტიპები:

- SYN Flood – შემთხვევითი წესით ხსნის TCP-ს პორტებს, ცრუ მოთხოვნების დიდი რაოდენობის შედეგად სესიებზე უარს იღებენ ლეგიტიმური მომხმარებლები.
- DoS – აგზავნის დიდი რაოდენობით მოთვოხნებისა სისტემისადმი, რაც იწვევს მომსახურების შეზღუდვას.
- DDoS – იყენებს zombies-ებს, რათა შეტევის წყაროს მოძებნა რთული გახადოს.
- Spoofing – ახერხებს მოწყობილობებსა და რესურსებთან შეღწევას როგორც სანდო კომპიუტერი.
- Man-in-the-Middle – იპარავს ან ანაცლებს ინფორმაციას ორ ჰოსტს შორის.
- Replay – იყენებს ქსელურ sniffer-ებს, რათა გაიგოს მომხმარებლის სახელი და პაროლი მოგვიანებით გამოსაყენებლად.
- DNS Poisoning – ცვლის DNS ჩანაწერებს სისტემაზე, რათა ცრუ სერვერებზე გადამისამართება მოახდინოს.

კომპიუტერული და ქსელური უსაფრთხოება გვეხმარება მონაცემების და მოწყობილობების ფუნქციუნალურობის და წვდომადობის შენარჩუნებაში.

ორგანიზაციის ყველა წევრმა უნდა მიანიჭოს დიდი პრიორიტეტი უსაფრთხოებას რადგანაც უსაფრხოებაში წარმოქმნილი პრობლემა ყველაფერზე ახდენს ზეგავლენას.

ქურდობა, ქსელში შეღწევა და მოწყობილობის დაზიანება იწვევს მწყობრიდან გამოსვლას. ქსელის ან კომპიუტერის აპარატურის დაზიანება ან დაკარგვა შეიძლება ნიშნავდეს პროცესის შეჩერებას. რემონტი და გამოცვლა აპარატურის შეიძლება სერიოზულ თანხას დას დრო დაუჯდეს კომპანიას. ხოლო ქსელის არაავტორიზებულმა გამოყენებამ შეიძლება გამოიწვიოს საიდუმლო ინფორმაციის დაკარგვა და ქსელური რესურსების შემცირება.

თავდასხმა, რომელიც მიზანმიმართულად აუარესებს კომპიუტერის ან ქსელის წარმადობას, ასევე შეიძლება გახდეს ორგანიზაციაში პროცესების შეჩერების მიზეზი. უკაბელო ქსელში არასრულფასოვნად განხორციელებულმა უსაფრხოებამ შეიძლება მისცეს საშუალება არაავტორიზებულ შეღწევას ფიზიკური კავშირის გარეშე.

ტექნიკოსის ძირითადი პასუხისმგებლობა არის მონაცემთა და ქსელის უსაფრთხოება. კერძო პირის ან ორგანიზაციის კომპიუტერული აპარატურის და მონაცემების უსაფრთხოებ შეიძლება თქვენზე იყოს დამოკიდებული. თქვენ შეიძლება შეაკეთოთ, დააინსტალიროთ ან ერთმანეთს მოარგოთ აპარატურა. თქვენ უნდა იცოდეთ, როგორ დააკონფიგურიროთ პარამეტრები, რომ შეინარჩუნოთ ქსელი უსაფრთხოდ და ამავდროულად ნება დართოთ კავშირისა მათ, ვისთვისაც ეს ნებადართულია. თქვენ უნდა უზრუნველყოთ, რომ პროგრამული განახლებები, ანტივირუსები, და anti-spyware პროგრამები იყვნენ დაინსტალირებულნი. თქვენ ასევე შეიძლება დაგეკითხონ, თუ რა წესები დაიცვან მომხმარებლებმა, რათა არ დაირღვეს უსაფრთხოება.

იმისთვის, რომ წარმატებულად დაიცვათ კომპიუტერები და ქსელები, უნდა გესმოდეთ ორივე ტიპის საფრთხეები:

- ფიზიკური – მოვლენები ან თავდასხმები, რომლებიც იპარავს, აზიანებს ან ანადგურებს აპარატურას, ისეთებს, როგორიცაა სერვერები, კომუტატორები და კაბელური გაყვანილობა.
- მონაცემთა – მოვლენები ან თავდასხმები, რომლებიც შლიან, აზიანებენ, ზღუდავენ კავშირს ან რთავენ და იპარავენ ინფორმაციას.

საფრთხეები შეიძლება მოდიოდეს შიგნიდან ან გარედან და პოტენციური ზიანი შეიძლება დიდად განსხვავდებოდეს:

- შიგა – თანამშომლებს ხელი მიუწვდებათ მონაცემებზე, აპარატურასა და ქსელზე.

- წინასწარ განზრახული საფრთხე არის მაშინ, როდესაც თანამშრომელი ცდილობს ზიანის მიყენებას
- შემთხვევითი არის საფრთხეები, როდესაც მომხმარებელი აზიანებს მონაცემებს ან აპარატურას წინასწარი განზრახვის გარეშე.

- გარე – მომხმარებელები ორგანიზაციის გარედან, რომელთაც არ აქვთ ავტორიზირებული წვდომის უფლება, აღწევენ ქსელში ან მის რესურსებზე.

  - არასტრუქტურირებული – თავდამსხმელები იყენებენ არსებულ რესურსებს, როგორებიც არიან პაროლები და სკრიპტები, რათა განახორციელონ წვდომა და გაუშვან პროგრამები რომლებიც განკუთვნილნი არიან დაზიანებისათვის
  - სტრუქტურირებული – თავდამსხმელები იყენებენ კოდს, რათა მოახდინონ წვდომა ოპერაციულ სისტემასთან ან პროგრამულ უზუნველყოფასთან.

ფიზიკური დანაკარგი ან დაზიანება ჩვენი აპარატურის შეიძლება იყოს ძვირად ღირებული ხოლო მონაცემების დაკარგვა შეიძლება იყოს დამღუპველი კომპანიის საქმიანობისათვის და რეპუტაციისათვის. საფრთხეები მონაცემების მიმართ მუდმივად იცვლება, რადგან თავდასხმელები მუდმივად პოულობენ ახალ მეთოდებს მათი განხორციელებისათვის.

კომპიუტერული ვირუსები მიზანდასახულად იქმნებიან და იგზავნებიან თავდამსხმელების მიერ. ვირუს არის მიმაგრებული კომპიუტერული კოდის პატარა ნაწილზე, პროგრამულ უზრუნველყოფასა ან დოკუმენზე. ვირუსი გაიშვება მაშინ, როდესაც პროგრამული უზრუნველყოფა გაიშვება კომპიუტერზე. თუ ვირუსი გავრცელდება სხვა კომპიუტერზე, ის თავის მხრივ გააგრძელებს ამ ვირუსის გავრცელებას.

ვირუსი არის ბოროტი განზრახვით დაწერილი პროგრამა და იგზავნება თავდამსხმელის მიერ. ვირუსი ვრცელდება კომპიუტერიდან კომპიუტერზე იმეილის, ფაილების მიმოცვლის, და მესიჯის პროგრამების საშუალებით. ვირუსი იმალება რომელიმე ფაილზე თავისი თავის მიბმით. როდესაც ფაილზე ხორციელდება წვდომა, ვირუსი გაიშვება და აინფიცირებს მთლიან კომპიუტერს. ვირუსს აქვს პოტენციალი დააზიანოს და წაშალოს ფაილები, გამოიყენოს იმეილი, რათა გავრცელდეს სხვა კომპიუტერებზე, ან თუნდაც წაშალოს მთელი მყარი დისკი.

ზოგიერთი ვირუსი შეიძლება განსაკუთრებით საშიში იყოს, ერთ-ერთი ასეთი შემთხვევაა, როდესაც ვირუსი იმახსოვრებს ყველა დაჭერილ ღილაკს ჩვენს კლავიატურაზე, ის გამოიყენება თავდამსხმელების მიერ ინფორმაციის მოსაპარად, იქნება ეს პაროლი თუ საკრედიტო ბარათის ნომერი. მათ ასევე შეუძლიათ

შეცვალონ და გაანადგურონ ინფორმაცია კომპიუტერზე. სტელს ვირუსებს შეუძლიათ დააინფიცირონ კომპიუტერი, მაგრამ იყვნენ დამალულნი სანამ არ იქნებიან გააქტიურებულნი თავდამსხმელის მიერ.

worm ანუ ჭია ეს არის თვითკოპირებადი პროგრამა, რომელიც არის საზიანო ქსელებისათვის, ის იყენებს ქსელს, რათა მოახდინოს კოპირება თავისი თავის სხვა ჰოსტებზე ქსელში, ხშირად მომხმარებლის ქმედებების გარეშე. ის განსხვავდება ვირუსისაგან, რადგანაც არ ესაჭიროება პროგრამაზე მიბმა, რათა დააინფიციროს ჰოსტები. იმ შემთხვევაშიც კი, თუ ის არ ახდენს მონაცემების და პროგრამების დაზიანებას, ის აზიანებს ქსელს, რადგანაც ითვისებს გამტარუნარიანობას.

ტროიანი ტექნიკურად იგივეა, რაც worm. მას არ ესაჭიროება მიბმა სხვა პროგრამულ უზრუნველყოფაზე, ის იმალება პროგრამაში, რომელიც თქვენ სხვა დანიშნულების გგონიათ. ტროიანს შეუძლია გავრცელდეს როგორც ვირუსს სხვა კომპიუტერებზე, კომპიუტერული მონაცემებზე ზიანი და წარმადობის დაკარგვა შეიძლება იყოს მნიშვნელოვანი. ტექნიკოსი შეიძლება იყოს საჭირო, რათა განახორციელოს შესწორებები და თანამშორმელბმა შეიძლება დაკარგონ მონაცემები. დაინფიცირებული კომპიუტერი შეიძლება აგზავნიდეს მნიშვნელოვან ინფორმაციას მეტოქეებთან და ამავდროულად აინფიცირებდეს სხვა კომპიუტერებს ქსელში.

ვირუსებისაგან დამცავი პროგრამული უზრუნველყოფა, რომელიც ცნობილია როგორც ანტივირუსი, არის სპეციალურად შექმნილი იმისთვის, რომ იპოვოს, გაანეიტრალოს და წაშალოს ვირუსები, worms-ები და ტროიანები მანამ, სანამ ისინი დააინფიცირებენ კომპიუტერს. თუმცა ეს პროგრამული უზრუნველყოფა ძალიან სწრაფად ძველდება, თუმცა მწარმოებლები ქმნიან განახლებებს, და ტექნიკოსის მოვალეობაა ამ განახლებების გადმოწერა და დაინსტალირება. უმეტეს ორგანიზაციას აქვს დაწერილი წესების კრებული, რომელშიც არის მითითებული, რომ თანამშრომლებს არ აქვთ უფლება დააყენონ პროგრამული უზრუნველყოფა, რომელიც არ იქნა ნებადართული და მოწოდებული კომპანიის მიერ. ორგანიზაციები ასევე ამცნობენ მომხმარებლბებს, თუ რა ტიპის საფრთხეები არსებობენ იმეილების მიმაგრებების გახსნის.

უსაფრთხოების პროცედურები და წესები, აპარატურის ფიზიკური დაცვის გზები, მონაცემების დაცვის ხერხები და უკაბელო ქსელების უსაფრთხოება

კრიტიკულ სიტუაციაში სამოქმედოდ უსაფრთხოების გეგმას უნდა იყენებდნენ, თან მუდმივად უნდა ხდებოდეს მისი განახლება, რათა უფრო ზუსტად ასახოს ის საფრთხეები, რომლებიც ემუქრება ქსელს. უსაფრთხოების გეგმა, სწორად

ჩამოყალიბებული პროცედურებით, ტექნიკოსის ქმედებების განმსაზღვრელია. მისი მოხდეს ყოველწლიურად განხილვა უნდა.

უსაფრთხოების უზრუნველყოფის ნაწილი არის ასევე ტესტების ჩატარება, რათა გამოვლინდეს მისი „სუსტი წერტილები“. ტესტირება რეგულარულად უნდა ჩატარდეს. ყოველდღიურად ახალ-ახალი საფრთხე ვრცელდებ და რეგულარულ ტესტირებას შეუძლია შეგვატყობინოს, თუ სად არის სისუსტე ამჟამინდელ უსაფრთხოების წესში და რა უნდა გამოსწორდეს.

არსებობს რამდენიმე შრე ქსელურ უსაფრთხოებაში – ფიზიკური, უკაბელო და მონაცემთა. შესაძლებელია თითოულ შრეზე მოხდეს თავდასხმა. ტექნიკოსმა უნდა იცოდეს, თუ როგორ განახორციელოს უსაფრთხოების პროცედურები, რათა დაიცვას აპარატურა და მონაცემები.

იმისდა მიუხედავად, რომ უსაფრთხოების გეგმები შეიძლება განსხვავდებოდნენ სხვადასხვა ორგანიზაციაში, არსებობს ყველასთვის საერთო შეკითხვები.

- რა ქონება არის დასაცავი?
- რა შესაძლო საფრთხეები არსებობს?
- რა უნდა გაკეთდეს უსაფრთხოების წესის დარღვევის შემთხვევაში?

უსაფრთხოების გეგმა უნდა აღწერდეს უსაფრთხოებასთან დაკავშირებული პრობლემების გადაწყვეტას:

- განსაზღვროს პროცესი ქსელური უსაფრთხოების ინციდენტების მართვისა
- განსაზღვროს არსებული ქსელური უსაფრთხოების აუდიტის პროცესი
- განსაზღვროს რა არის დაშვებული ქმედებები
- განსაზღვროს რა არის დაუშვებელი ქმედებები
- განსაზღვროს, რა ქმედებების და მოვლენების დამახსოვრებაა საჭირო და სად უნდა მოხდეს მათი შენახვა
- განსაზღვროს ქსელურ რესურსებთან შეღწევის შესაძლებლობა მომხმარებლის უფლებების მიხედვით
- განსაზღვროს აუტენტიფიკაციის ტექნოლოგიები

ფიზიკური უსაფრთხოება იმდენადვე მნიშვნელოვანია, რამდენადაც მონაცემთა უსაფრთხოება. როდესაც იპარავენ კომპიუტერს, იმავდროულად მონაცემების მოპარვასაც აქვს ადგილი.

კომპიუტერული აპარატურის ფიზიკური დაცვის რამდენიმე მეთოდი არსებობს:

- ადგილმდებარეობის კონტროლი
- კაბელის საკეტების გამოყენება
- სატელეკომუნიკაციო ოთახების ჩაკეტვა
- აპარატურაზე უსაფრთხოების ხრახნისი
- გისოსები აპარატურის გარშემო
- სენსორები, მაგ., RFID ჩიპები აპარატურაზე

ადგილმდებარეობის კონტროლის რამდენიმე ხერხია:

- ელექტრონული გასაღები. რომელიც ინახავს ინფორმაციას პატრონის და მისი უფლებების შესახებ
- ბიომეტრიული სენსორები, რომლებიც ახდედენენ იდენტიფიცირებას ფიზიკური პარამეტრების, მაგ. თითის ანაბეჭდების მეშვეობით და სხვ.
- დაცვის თანამშრომელი

როგორც წესი, ფიზიკური აპარატურის ფასი იმ ინფორმაციაზე ბევრად უფრო დაბალია, რომელიც მასში ინახება. თუ ეს მონაცემები ჩაუვარდება ხელთ კონკურენტ ფირმას ან კრიმინალებს, შეიძლება ძვირად დაუჯდეს კომპანიას. ასეთმა დანაკარგმა შეიძლება გამოიწვიოს კომპანიისადმი ნდობის დაქვეითება და უსაფრთხოების დარგში მომუშავე ტექნიკოსის სამსახურიდან დათხოვნა. მონაცემების დასაცავად არსებობს რამდენიმე.

პაროლით დაცვა
პაროლით დაცვამ შეიძლება აღკვეთოს არასანქცირებული შეღწევა ქსელში.

თავდამსხმელმა შეიძლება შეაღწიოს დაუცველ კომპიუტერულ მონაცემებში. ამიტომ ყველა კომპიუტერი უნდა იყოს პაროლით დაცული. რეკომენდირებულია ორი დონის პაროლით დაცვა:

- BIOS-ის პაროლი არ დაუშვებს ნებას არასანქცირებულ შეღწევას ბიოსში და მისი პარამეტრების შეცვლას
- LOGIN არ დაუშვებს ქსელში არასანქცირებულ შეღწევას

ქსელური login-ი გვაძლევს საშუალებას შევინახოთ ინფორმაცია ქსელში მომხმარებლების რესურსებთან შეღწევის შესახებ. როგორც წესი, სისტემური ადმინისტრატორი დაადგენს მომხმარებლების login-ებს. მომხმარებლის სახელის მაგალითი შეიძლება იყოს მოხმარებლის სახელის პირველი ასო და მას მიყოლებული მისივე გვარი. მომხმარებლის სახელი უნდა იყოს ადვილი დასამახსოვრებელი, რომ მომხმარებელს არ დაავიწყდეს ის.

როდესაც ვირჩევთ პაროლს, გვახსოვდეს, რომ მისი კონტროლის მექანიზმი უნდა უტოლდებოდეს უსაფრთხოების საჭირო დონეს. კარგი უსაფრთხოების პოლიტიკა მკაცრად უნდა მოქმედებდეს და შეიცავდეს შემდგომ წესებს:

- პაროლებს უნდა გაუვიდეთ ვადა დროის გარკვეული პერიოდის შემდგომ
- პაროლები უნდა შეიცავდნენ როგორც ასოებს, ასევე ციფრებს, რათა იყვნენ რთულად გასატეხი
- პაროლების სტანდარტებმა უნდა აუკრძალონ მომხმარებლებს მათი ქაღალდზე დაწერა და დაუცველად დატოვება იმ ადგილებში, სადაც შესაძლოა ვინმემ წაიკითხოს
- წესები პაროლის ვადის გასვლის და ბლოკირების შესახებ უნდა იყოს განსაზღვრული. ბლოკირება უნდა მოხდეს როდესაც წარუმატებელი შეღწევის მცდელობებს ექნება ადგილი ან როდესაც სპეციფიური ცვლილება განხორციელდება სისტემაში

უსაფრთხოების ადმინისტრირების გასაადვილებლად ამ ჯგუფებისთვის ხშირად ხდება მომხმარებლების ჯგუფებად გაერთიანება და შემდგომ ამჯგუფებისთვის გარკვეული უფლებების მინიჭება. ეს გვიმარტივებს რომელიმე მომხმარებლისათვის უფლებების შეცვლას, რამეთუ მარტივად გადავიყვანთ ერთი ჯგუფიდან მეორე და მისი უფლებები შეიცვლება. ეს ძალიან გამოსადეგია, როდესაც გვყავს დროებითი თანამშრომელი ან კონსულტანტი და გვსურს შევზღუდოთ მისი უფლებები რომელიმე რესურსთან შეღწევისა.

მონაცემების დაშიფვრა დაშიფვრისათვის გამოიყენება კოდები და გასაღებები. ინფორმაცია, რომელიც მოგზაურობს ქსელში, შეიძლება ამ მეთოდით იქნას დაცული თავდამსხმელებისგან, რომლებიც თვალყურს ადევნებენ ინფორმაციას ქსელში. მოპოვებული მონაცემების გაშიფვრისათვის საჭირო დრო უნდა აღემატებოდეს დროს, როდესაც შეიძლება ამ

ინფორმაციის გამოყენება. ანუ, მას შემდეგ, რაც თავდამსხმელი გაშიფრავს ინფორმაციას, ის უკვე გამოუსადეგარი უნდა იყოს.

Virtual Private Network (VPN) იყენებს დაშიფვრას მონაცემების დასაცავად. A VPN კავშირი საშუალებას აძლევს მომხმარებელს დისტანციიდან ის დაამყაროს კავშირი ქსელში არსებულ რესურსებთან, თითქოს იმავე ქსელში იყოს.

Port-ის უსაფრთხოება ყოველ კავშირგაბმულობას, რომელიც იყენებს TCP/IP-ის, აქვს პორტის ნომერი, რომელზეც ახდენს ინფორმაციის დამისამართებას, მაგ., HTTPS იყენებს 443 პორტს. Firewall-ი არის მეთოდი, საშუალება ჩვენი ქსელის დაცვისათვის პორტების, გამოყენებით არასანქცირებული კავშირისაგან. მომხმარებელს ამა თუ იმ პორტის დახურვა-გახსნის საშუალებით შეუძლია აკონტროლოს მონაცემების შეშვება კომპიუტერში. მონაცემებს, რომლებიც მოგზაურობენ ქსელში, ეწოდება ტრაფიკი.

მონაცემთა დარეზერვება მონაცემთა და რეზერვების პროცედურები აღწერილი უნდა იყვოს უსაფრთხოების გეგმაში. ქურდობის, წყალდიდობის, ხანძრის ან სხვა შემთხვევაში მონაცემები შეიძლება დაზიანდეს ან დაიკარგოს. მათი დაცვის ერთ-ერთი ეფექტური გზა დარეზერვებაა. ამ დროს უნდა გაითვალისწინოთ შემდეგი:

- **დარეზერვების სიხშირე** – დარეზერვებამ შესაძლებელია დიდი დრო წაგვართვას. ზოგჯერ უფრო მარტივია, განვახორციელოთ სრული რეზერვირება თვეში ან კვირაში ერთხელ და შემდგომ მოვახდინოთ ხშირი ნაწილობრივი განახლებები იმ მონაცემებისა, რომლებიც შეიცვალნენ მას შემდეგ, რაც მოვახდინეთ სრული რეზერვირება.
- **რეზერვების შენახვა** – უფრო მეტი უსაფრთხოებისათვის სარეზერვო ასლები უნდა იყვნენ გადატანილნი და შენახულნი სხვა ადგილას. მათი ტრანსპორტირება უნდა ხდებოდეს კონკრეტული ორგანიზაციის მოთხოვნების შესაბამისად.
- **სარეზერვო ასლების უსაფრთხოება** – სარეზერვო ასლები შეიძლება იყოს დაცული პაროლის მეშვეობით. ამ პაროლების მოთხოვნა მოხდებოდა მანამ სანამ მოხდებოდა ამ სარეზერვო კოპიების აღდგენისას.

ფაილური სისტემის უსაფრთხოება ყველა ფაილური სისტემა ადევნებს თვალყურს რესურსებს, მაგრამ მხოლოდ იმ ფაილურ სისტემებს, რომლებასც აქვთ ჟურნალი, შეუძლიათ დაიმახსოვრონ, თუ რომელი მომხმარებელი და რა დროს იყო ქსელში. FAT 32 ფაილურ სისტემას, რომელიც გამოიყენება ვინდოუსის რამდენიმე ვერსიაში, აკლია ორივე – როგორც, ჟურნალი, ასევე დაშიფვრის ფუნქცია. შედეგად, როდესაც არის საჭირო საიმედო უსაფრთხოება, გამოიყენება ისეთი ფაილური სისტემა, როგორიც არის NTFS, ის არის ვინდოუს 2000-ის და XP-ს ნაწილი. საჭიროების შემთხვევაში შესაძლებელია გარდაქმნა არსებული FAT 32 ფაილური სისტემისა NTFS ფაილურ სისტემად. ამ ცვლილების შემდეგ უკან ვეღარ დაბრუნდებით გაითვალისწინოთ.

იმის გამო, რომ ტრაფიკი ჰაერში რადიოტალღების სახით მოგზაურობს, თავდამსხმელებისათვის ადვილია მონაცემებზე თავდასხმა და მოპარვა ფიზიკური

კავშირის უქონლობის შემთხვევაშიც. თავდამსხმელები მიახლოებით შეაღწევენ დაუცველ უკაბელო ქსელში. ტექნიკოსმა უნდა იცოდეს, როგორ დააკონფიგურიროს წვდომის წერტილები და უკაბელო ქსელის ადაპტერები სწორი უსაფრთხოების პარამეტრებით.

როდესაც ვაინსტალირებთ უკაბელო მომსახურებებს, მაშინათვე უნდა მოვახდინოთ უსაფრთხოების კონფიგურირება, რათა თავიდან ავიცილოთ არასანქცირებული შეღწევა ქსელში. უკაბელო წვდომის წერტილების კონფიგურირება ბაზისური უსაფრთხოების პარამეტრებით უდნა მოხდეს ისე, რომ შესაბამისი იყოს არსებულ ქსელურ უსაფრთხოებასთან.

თავდამსხმელს შეუძლია შეღწევა იმ მონაცემებთან, რომლებიც გადაიცემიან რადიოსიგნალით. ამიტომ უკაბელო ქსელის მეშვეობით გაგზავნილი მონაცემების მოპარვის თავიდან ასაცილებლად შიფრი უნდა გამოვიყენოთ კავშირის ორივე ბოლოს ერთანირი შიფრაციის მეთოდი უნდა იქნას გამოყენებული.

- **Wired Equivalent Privacy (WEP) –** პირველი თაობის უსაფრთხოების სტანდარტი უკაბელო ქსელებისათვის. თავდამსხმელებმა უცბად აღმოაჩინეს, ამ შიფრაციის გატეხვის მეთოდი – მარტივად მიაგნეს შიფრაციის გასაღებს, ამის შემდეგ კი მონაცემებიც გაშიფრეს.
- **Wi-Fi Protected Access (WPA) –**WEP-ს გაუმჯობესებული ვერსია. ის შეიქმნა როგორც დროებითი გადაწყვეტილება, სანამ მოხდებოდა 802.11i სტანდარტის სრულად დამტკიცება. ამჟამად 802.11i სტანდარტი არის დამტკიცებული და გამოშვებულია WPA2. ის სრულად შეიცავს 802.11i სტანდარტს.
- **Lightweight Extensible Authentication Protocol (LEAP)**, ასევე მოიხსენიება როგორც **EAP-Cisco –** უკაბელო უსაფრთხოების პროტოკოლი შექმნილი Cisco-ს მიერ, რათა გამოესწორებინა WEP-ის და WPA-ის სისუსტეები. LEAP-ი არის კარგი არჩევანია, როდესაც ვიყენებთ Cisco-ს აპარატურას ვინდოუსის და ლინუქსის ოპერაციულ სისტემებთან ერთად.

Wireless Transport Layer Security (WTLS) არის უსაფრთხოების შრე, რომელიც გამოიყენება მობილურ მოწყობილობებში, რომლებიც იყენებენ Wireless Applications Protocol (WAP)-ს. ამ მოწყობილობებს არ გააჩნიათ დიდი რაოდენობით გამტარუნარიანობა, შედეგად პროტოკოლი ეკონომიურად გამოეყენებს გამტარუნარიანობას.

უსაფრთხოების გაზრდა მუდმივად ცვალებადი ტექნოლოგიური პროცესია. ახალი „სუსტი წერტილების“ (exploits) აღმოჩენა ხდება ყოველდღიურად. თავდამსხმელები მუდმივად ახალი გზების ძიებაში არიან. პროგრამული უზრუნველყოფის მწარმოებლებმა რეგულარულად უნდა გამოუშვან განახლებები და patche-ები თავიანთი პროდუქციისათვის. თუ ტექნიკოსი გამუდმებით არ იზრუნებს კომპიუტერის დაცვაზე,,

თავდამსხმელი ადვილად შეაღწევს მასში. დაუცველი კომპიუტერები ინტერნეტში შეიძლება რამდენიმე წუთში დაინფიცირდნენ.

იმის გამო, რომ უსაფრთხოებას სულ ახალ-ახალი რისკი ექმნება, ტექნიკოსმა ძალიან კარგად უნდა იცოდეს, როგორ დააინსტალიროს patche-ები და განახლებები. მას ასევე უნდა შეეძლოს გაიგოს, როდის არის ესა თუ ის განახლება ან patche გადმოსაწერი. ზოგიერთი მწარმოებელი ავრცელებს განახლებებს ყოველთვიურად ერთსა და იმავე რიცხვში. თუმცა ასევე აგზავნიან სასწრაფო განახლებებს, როდესაც საჭიროა. სხვა მწარმოებლები გვთავაზობენ ავოტმატური განახლების საშუალებებს და პროგრამული უზრუნველყოფა განახლდება კომპიუტერის ყოველი ჩართვისას, ან იმეილით გვატყობინებენ ახლის გამოსვლას.

ვირუსების, spyware-ის და adware-ის აღმომჩენი პროგრამები მიმდევრობით ეძებენ შაბლონურ კოდებს პროგრამულ უზრუნველყოფაში, ეს შაბლონები მოპოვებულია ვირუსების ანალიზის შედეგად, მათ უწოდებენ signatures-ს. მრავალი ასეთი შაბლონის ერთად ჩაწერა ხდება ცხრილში, ანტივირუსის და მსგავსი პროგრამების ცხრილები ვრცელდება განახლებების მეშვეობით. სანამ შევეცდებოდეთ განახლებას, უნდა გადავამოწმოთ, მოძველებული ხომ არ არის ჩვენი ცხრილი. ამისათვის შედით მენიუში About ჩვენი პროგრამული უზრუნველყოფისა და თუ ცხრილები უკვე დაძველდა, შეგიძლიათ გაუშვათ განახლების პროცესი „Update Now“ ღილაკზე დაჭერით (უმეტეს პროგრამულ უზრუნველყოფაში).

ცხრილები უნდა გადმოიწეროთ მხოლოდ ოფიციალური მწარმოებლის ვებგვერდიდან, რომ თავი დაიზღვიოთ დაზიანებული ცხრილებისაგან (დაზიანების გამომწვევი შეიძლება იყოს ვირუსი). მაგრამ ამას შესაძლებელია მოჰყვეს მწარმოებლის ვებგვერდის მეტისმეტი გადატვირთვა ახალი ვირუსის გავრცელებისას. ამის თავიდან ასაცილებლად, უმეტესი მწარმოებელი იყენებს მრავალ ვებგვერდს ამ ცხრილების გასავრცელებლად. მათ ეწოდებათ mirror-ები.

ვირუსები და სხვა საზიანო პროგრამული უზრუნველყოფა შეიძლება იყოს რთული წასაშლელი კომპიუტერიდან, მაგრამ წაშლა უნდა მოხდეს და იმ ზიანის აღმოფხვრა, რომელიც მოხდა ვირუსის გამო აუცილებელია. ეს პროგრამული უზრუნველყოფა შეიძლება მოგვაწოდოს ოპერაციული სისტემის მწარმოებელმა ან უსაფრთხოების პროდუქციაზე სპეციალიზებულმა პროგრამული უზრუნველყოფის კომპანიამ. ეს პროგრამები ოფიციალური ვებგვერდიდან გადმოიწერეთ.

ოპერაციული სისტემების და პროგრამული უზრუნველყოფის მწარმოებლები ზოგჯერ შემოგვთავაზებენ განახლებებს, რომლებსაც ეწოდება patche-ები. გარკვეული დროის შემდგომ, როდესაც დაგროვდება ეს patche-ები და სხვა ტიპის განახლებები, მწარმოებლები მათ აერთიანებენ ე.წ. service pack-ის სახით. ვინდოუსის ოპერაციული სისტემა დადგენილი გრაფიკით ათვალიერებს ვინდოუსის განახლების ვებგვერდს და

ამოწმებს, ხომ არ გამოვიდა გამოვიდა რაიმე მაღალი პრიორიტეტის განახლება, რომელსაც შეუძლია გააუმჯობესოს ჩვენი კომპიუტერის უსაფრთხოება. თქვენ მიერ დაყენებული პარამეტრების თანახმად მოიქცევა ვინდოუსი მას შემდგომ, რაც აღმოაჩენს განახლებას.

განახლებები უნდა დაინსტალირდნენ და არა უბრალოდ იქნან გადმოწერილნი, თუ თქვენ გამოიყენებთ ავოტმატური განახლების პარამეტრს, მაშინ საამისოდ შეგიძლიათ აირჩიეოთ დღე და დრო. თუ იმ დროს თქვენი კომპიუტერი გათიშული იქნება, განახლების ინსტალირება მოხდება მომავალი ჩართვისას. თქვენ ასევე შეგიძლიათ აირჩიოთ, პარამეტრი რომლის თანახმადაც მოგივათ შეტყობინება, რომ განახლება გამოვიდა, თუმცა გადაწყვეტილება მისი დაინსტალირების შესახებ თქვენი გადასაწყვეტი იქნება.

Troubleshooting-ის პროცესი გამოიყენება უსაფრთხოების სისტემაში არსებული პრობლემების აღმოსაჩენად და აღმოსაფხვრელად. პრობლემა შეიძლება იყვოს ძალიან მარტივი, ვთქვათ, როდესაც ვინმე, თქვენს უკან მდგომი ცდილობს დაინახოს პაროლი, რომელსაც თქვენ კრეფთ და გაცილებით რთული, კომპლექსურიც. მაგალითად, დაინფიცირებული ფაილების ხელით წაშლა.

ტექნიკოსებს უნდა შეეძლოთ გააანალიზონ საფრთხეები და აღმოაჩინონ ადექვატური მეთოდი დაცვისა და პრობლემის აღმოფხვრისა.

პირველი ნაბიჯი troubleshooting-ში არის ინფორმაციის მოგროვება კლიენტისაგან.

მას შემდგომ, რაც მიიღებთ ინფორმაციას კლინეტისაგან, გადაამოწმეთ მისი სიზუსტე, ამის შემდგომ სცადეთ სწრაფი გადაწყვეტები ამ პრობლემებისა. თუ სწრაფმა გადაწყვეტებმა არ უშველა, უნდა გადახვიდეთ ინფორმაციის მოძიებაზე კომპიუტერიდან. მას შემდგომ, რაც მოახდენთ პრობლემის იდენტიფიცირებას, მოახდინეთ მისი ანალიზი და მონახეთ გზა გამოსწორებისათვის.

ქსელის Troubleshooting-ი

ქსელური პრობლემები შეიძლება იყოს მარტივები და კომპლექსურები. იმისთვის, რომ შეაფასოთ რამდენად რთულია პრობლმა, უნდა დაადგინოთ, ქსელში რამდენ კომპიუტერს შეექმნა ეს პრობლემა.

თუ პრობლემა მხოლოდ ერთ კომპიუტერს აქვს ქსელში, დაიწყეთ troubleshooting-ის პროცესი იმ კომპიუტერთან, და თუ პრობლემა არაერთ კომპიუტერს აქვს, ქსელში troubleshooting-ს შეუდექით ქსელურ ოთახში. როგორც ტექნიკოსმა, თქვენ უნდა ჩამოაყალიბოთ მეთოდი, რომლითაც მოახდენთ პრობლემის დიაგნოსტირებას. თითო-

თითო უნდა მოსინჯოთ შესაძლო მიზეზები, უნდა მიმართოთ გამორიცხვის მეთოდს, სანამ არ აღმოაჩენთ პრობლემის მიზეზს.

მიყჰყევით შემდგომ ნაბიჯებს:

- მოაგროვეთ ინფორმაცია კლიენტისაგან
- გადაამოწმეთ ყველა ძირითადი შესაძლო პრობლემა
- სცადეთ სწრაფი გადაწყვეტები
- მოაგროვეთ ინფორმაცია კომპიუტერიდან
- შეაფასეთ პრობლემა და განახორციელეთ გადაწყვეტა
- მოახსენეთ კლიენტს

ქსელური პრობლემები შეიძლება წარმოიშვას პრობლემათა კომბინაციით აპარატურულ და პროგრამულ უზრუნველყოფებში. ტექნიკოსს უნდა შეეძლოს ამ პრობლემების ამოცნობა და აღმოფხვრა. ამ პროცესს ეწოდება Troubleshooting-ი. კლიენტთან საუბარი დაიწყეთ ამ შეკითხვებით:

- რა ტიპის პრობლემები გექმნებათ თქვენს კომპიუტერთან?
- უახლოეს პერიოდში რომელი პროგრამული უზრუნველყოფის დაყენება მოხდა კომპიუტერზე?
- რას აკეთებდით, როდესაც გადააწყდით პრობლემას?
- რა ტიპის შეცდომაზე შეტყობინება გამოვიდა თქვენს კომპიუტერზე?
- რა ტიპის ქსელურ კავშირს იყენებს კომპიუტერი?
- ვინმე სხვას ხომ არ გამოუყენებია თქვენი კომპიუტერი ბოლო ხანებში?
- ხედავთ რაიმე გაზიარებულ ფაილებს ან პრინტერებს?
- პაროლი ხომ არ შეგიცვლიათ ამ ბოლო დროს?
- ინტერნეტთან კავშირი გაქვთ?
- ხართ თუ არა ამჟამად ქსელში ჩართული?

მას შემდგომ, რაც გაესაუბრებით კლიენტს, უნდა მოიძიოთ ძირითადი შესაძლო პრობლემები:

- სადმე კაბელი ხომ არ არის გამოერთებული
- არასწორად ხომ არ არის დაყენებული ქსელური ადაპტერი
- შეამოწმეთ ქსელური ადაპტერის შუქდიოდი
- ხომ წესრიგშია უკაბელო სიგნალის სისტემა
- არასწორი IP მისამართი ხომ არ არის მიცემული

ამის შემდგომ სცადეთ სწრაფადრეალიზებადი გადაწყვეტილებები:

- დარწმუნდით, რომ ყველა კაბელი სწორად არის შეერთებული
- გამოაერთეთ და თავიდან შეაერთეთ კაბელები

- გადატვირთეთ კომპიუტერი ან ქსელური მოწყობილობა
- გამოიყენეთ სხვა მომხმარებლის სახელი და პაროლი
- გამორთეთ და ჩართეთ ქსელური კავშირი, ან დააჭირეთ Repair ღილაკს
- დაუკავშრიდით ქსელურ ადმინისტრატორს

თუ ამ გადაწყვეტილებებმა ვერ გამოასწორეს პრობლემა, მაშინ მოიძიეთ დამატებითი ინფორმაცია, ამისთვის შეგიძლიათ გამოიყენოთ:

- Ping – გამოიყენება ქსელური კავშირის არსებობის შესამოწმებლად. იგზავნება პაკეტი კონკრეტულ მისამართზე და ელოდებიან პასუხს
- NsLookup – გამოიყენება დომენური სახელები შესაბამისი IP მისამართების დასადგენად
- Tracert – გამოიყენება იმ გზის დასადგენად, რომელზეც გადის პაკეტი და ის გვაჩვენებს, სად იქმნება პრობლემა კავშირგაბმულობაში
- Net View – გმაოიყენება სამუშაო ჯგუფში არსებული ყველა კომპიუტერის სიის სანახავად, ის ასევე გვაუწყებს, თუ რომელი რესურსები არის გაზიარებული.

ის შემდეგ გექნებათ საკმარისი ინფორმაცია, რომ შეაფასოთ პრობლემა, გამოიკვლიოთ ის და მიიღოთ გადაწყვეტილება.

- პრობლემების აღმოფხვრის გამოცდილება
- სხვა ტექნიკოსები
- ინტერნეტში ძიება
- ახალი ამბების ჯგუფები
- მწარმოებლის FAQ დოკუმენტი
- კომპიუტერის ინსტრუქცია
- მოწყობილობის ინსტრუქცია
- ონლაინ ფორუმები
- ტექნიკური ვებგვერდები

ეს ყველაფერი დაგეხმარებათ გადაწყვეტილების პოვნაში.

მას შემდგომ, რაც პრობლემა აღმოიფხვრება, შეასრულეთ შემდეგი:

- მომხმარებელთან განიხილეთ გადაწყვეტილება, რომლის განხორციელებაც მოხდა
- სთხოვეთ მომხმარებელს დაადასტუროს, რომ პრობლემა აღმოიფხვრა
- მიეცით კლიენტს ყველა საჭირო დოკუმენტი
- შეკვეთის ბლანკსა და ტექნიკოსის ჯურნალში აღწერეთ, რა ნაბიჯები გადადგით პრობლემის აღმოსაფხვრელად

- ჩამოწერეთ ყველა კომპონენტი, რომელთა გამოყენებაც მოხდა პრობლემის აღმოფხვრის დროს
- აღნიშნეთ, რა დრო დაგჭირდათ პრობლემის აღმოსაფხვრელად.

მუშაობისას ზოგიერთ პრობლემას უფრო ხშირად წააწყდებით, ვიდრე სხვას. წარმოიდგინეთ ამ გავრცელებულ პრობლემებსა და მათი მოგვარების გზებს:

- კომპიუტერს აქვს IP მისამართი 169.254.X.X – შეამოწმეთ, მუშაობს თუ არა DHCP სერვერი
- კომპიუტერი ვერ უკავშირდება ქსელს – შეამოწმეთ კაბელები
- კომპიუტერი ვერ ბეჭდავს ქსელურ პრინტერზე – შეამოწმეთ მომხმარებლის უფლებები და ქსელური პრინტერის მდგომარეობა
- კომპიუტერი ვერ შედის ვებგვერდებზე – შეამოწმეთ DNS პარამეტრები, აპარატურული ან პროგრამული პარამეტრები და Firewall-ის პარამეტრები.

ქსელის შემუშავება კლიენტის მოთხოვნის შესაბამისად. კაბელებთან უსაფრთხოდ მუშაობის წესები, ქსელის დიზაინის შემუშავება კლიენტის მოთხოვნების თანახმად. საჭირო ტოპოლოგიის დადგენა და რომელი პროტოკოლები და პროგრამები უნდა მუშაობდედნენ ქსელში. ქსელის კომპონენტების და კაბელის დადგენა, ინტერნეტპროვაიდერთან კავშირის, ქსელის ადაპტერის და ქსელური მოწყობილობების ტიპების არჩევა

ქსელი უკეთ მუშაობს როდესაც მორგებულია მომხმარებლის მოთხოვნებს. ქსელის ასაგებად საჭიროა გარემოს ანალიზი და ქსელური გადაწყვეტილებების ცოდნა. თქვენ უნდა გამოკითხოთ კლიენტი და სხვა ნებისმიერი პირი, ჩართული პროექტში. მნიშვნელოვანია გქონდეთ წარმოდგენა იმის შესახებ, თუ რა ტიპის პროგრამული და აპარატურული უზრუნველყოფა იქნება გამოყენებული ქსელში. აგრეთვე უნდა გაითვალისწინოთ კომპანისს და ქსელის სამომავლო ზრდის პერსპექტივები.

ქსელის ტოპოლოგიის დასადგენად საჭიროა კლიენტის მოთხოვნების გაგება და ქსელის ზოგადი სახის განსაზღვრა. ამისათვის ქვემოთ მითითებული მნიშვნელოვანი საკითხები უნდა განიხილოთ კლიენტთან:

- კაბელის ტიპები და უკაბელო გადაწყვეტები
- ქსელის ზრდის პერსპექტივა - Expandability
- მომხმარებლების რაოდენობა და განლაგება

მომხმარებლების რიცხვი და მათი პროგნოზირებული ზრდა განსაზღვრავს ქსელის ლოგიკურ ტოპოლოგიას. კარგი იქნება, თუ შექმნით კლიენტის მოთხოვნების შესამოწმებელ სიას (checklist).

ინსპექცია, ანუ ადგილმდებარეობის დათვალიერება უნდა მოხდეს პროექტის დასაწყისშივე. შენობის დათვალიერება დაგეხმარებათ საბაზისო ლოგიკური ტოპოლოგიის შემუშავებაში. მომხმარებლების რაოდენობა და სამომავლო ზრდა განსაზღვრავს ქსელის პირვანდელ ფიზიკურ და ლოგიკურ ტოპოლოგიას. უნდა გაითვალისწინოთ შემდეგი:

- სად იქნება განთავსებული მომხმარებლების კომპიუტერები
- კომუტატორებისა და მარშრუტიზატორებს.
- სერვერების განთავსების ადგილი, ეს შეიძლება იყოს იგივე ოთახი, სადაც ქსელური აპარატურაა ან სხვაგან. გადაწყვეტილება, როგორც წესი, ეფუძნება თავისუფალ ადგილს, უსაფრთხოებას, ჰაერის კონდიცირებას და კვების (დენის) მოწოდებას.

იმ სართულის გეგმა ან ნახაზი, სადაც ქსელი იგება, დაგეხმარებათ აპარატურის და კაბელირების განაწილებაში. თუ სართულის გეგმა ან ნახაზი არ არის ხელმისაწვდომი, თქვენ თვითონ დახატეთ, სად იქნება განთავსებული ქსელური მოწყობილობები, სასერვერო ოთახი, პრინტერები, მომხმარებლების კომპიუტერები და კაბელის გაყვანილობა. ეს ნახატი შეიძლება გამოსადეგი გახდეს, როდესაც კლიენტი თქვენთან ერთად დააპირებს საბოლოო გადაწყვეტილების მიღებას. ქსელის დიზაინისთვის უნდა გადაწყვიტოთ, თუ რომელი პროტოკოლები იმუშავებენ ქსელში, რადგანაც ზოგიერთი პროტოკოლი არის დახურული და მუშაობს მხოლოდ კონკრეტული ფირმის აპარატურაზე, და ამავდროულად არსებობს ღია პროტოკოლები, რომლებიც მუშაობენ სხვადასხვა ტიპის აპარატურაზე.

- TCP/IP – პროტოკოლების ეს ნაკრები ყველაზე მეტად გავრცელებულია მსოფლიოში. ის ღია პროტოკოლია, რომელიც განსაზღვრავს, თუ როგორ იგზავნება ინფორმაცია ქსელში კომპიუტერებს შორის ან თუნდაც რამდენიმე ქსელით დაშორებულ კომპიუტერებში.
- IPX/SPX – პროტოკოლთა ნაკრებია, რომელიც შეიქმნა კორპორაცია ნოველის მიერ. ის TCP/IP-ის მსგავსი ფუნქციის მატარებელია. ნოველის ახალი პროდუქცია მხარს უჭერს TCP/IP-ს, მაგრამ არის შემორჩენილი დიდი რაოდენობით ქსელები, რომლებიც ამჟამადაც IPX/SPX-ს იყენებენ.
- NetBEUI – NetBios Extended User Interface არის პროტოკოლი, რომელიც ძირითადად გამოიყენება Windows NT-ის პატარა ქსელებში, მისი გამოყენება მარშრუტიზატორებს არ შეუძლიათ. შესაბამისად ის არ არის მისაღები დიდი ქსელებისათვის. თუმცა მისი გამოყენება შეიძლება TCP/IP-ის პარალელურად, რაც

მოგვცემს იმის საშუალებას, რომ ლოკალური ქსელის გარეთაც დავამყაროთ კავშირგაბმულობა.

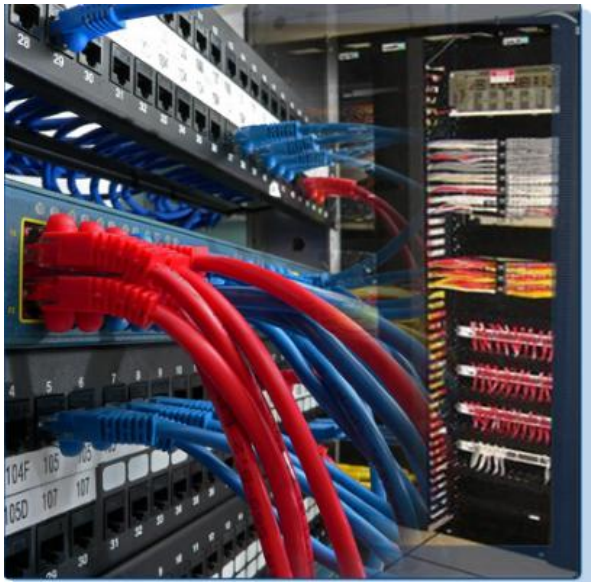
- AppleTalk – არის კომპანია Apple-ის პროტოკოლი, რომელიც გამოიყენება მაკინტოშის კომპიუტერებში. ის იყო შექმნილი LocalTalk-ზე სამუშაოდ, რაც არის ამავე კომპანიის მიერ შექმნილი ლოკალური ქსელის ფიზიკური ტოპოლოგია, თუმცა ის ასევე მხარს უჭერს კარგად გავრცელებულ ტექნოლოგიებს, ისეტებს, როგორიც არის ეზერნეტი და ტოკენ რინგი.
- HTTP – ღია სტანდარტია, შექმნილი IETF-ის მიერ, ის განსაზღვრავს, თუ როგორ გადაიგზავნება ტექსტი, სურათები, ხმა, და ვიდეო გამოსახულებები მსოფლიო აბლაბუდაში(WWW).
- FTP – ფაილების გადაცემის პროტოკოლი
- SSH – კომპიუტერების უსაფრთხო დაკავშირებისათვის გამოიყენება
- Telnet – ბრძანებათა ველის კავშირის დასამყარებლად დაშორებულ კომპიუტერთან
- POP – საფოსტო პროტოკოლი, წერილების გადმოსაწერად სერვერიდან
- IMAP – საფოსტო პროტოკოლი, წერილების გადმოსაწერად სერვერიდან
- SMTP – საფოსტო პროტოკოლი, წერილების გასაგზავნად

პროტოკოლის არჩევისას გაითვალისწინეთ შემდეგი:

- TCP/IP არის საჭირო ინტერნეტთან დასაკავშირებლად შესაბამისად ეს პროტოკოლი არის უკეთესი არჩევანი.
- NetBEUI არის პატარა, სწრაფი პროტოკოლი რომელიც სასარგებლო შეიძლება იყოს ქსელებში სადაც გვაქს დაბალი უსაფრთხოება, ის ადვილი დასაყენებელია და არ საჭიროებს კონფიგურაციას. თუმცა მან შეიძლება გამოიწვიოს ზედმეტი ტრაფიკი დიდ ქსელში, შესაბამისად ეს არ არის კარგი არჩევანი თუ არის მოსალოდნელი ქსელის ზრდა.
- IPX/SPX არის მოძველებული პროტოკოლი, ამჟამად ნოველის პროდუქციას აქვს TCP/IP-ის მხარდაჭერა.
- კომპანია Apple-ი აღარ იყენებს AppleTalk პროტოკოლს და სრულად გადაერთო TCP/IP-ის პროტოკოლზე, რათა სრულად უზრუნველყონ მაკინტოშის ქსელების ინტერნეტთან თავსებადობა.

Protocol	Port	Purpose
HTTP	Port 80	Transports web pages over a TCP/IP network
HTTPS	Port 443	Securely transports web pages over a TCP/IP network
SMTP	Port 25	Sends e-mail over a TCP/IP network
Telnet/SSH	Port 23/22	Provides connections to computers over a TCP/IP network
FTP/TFTP	Port 20 or 21	Transports files over a TCP/IP network
DNS	Port 53	Translates URLs to IP address
DHCP	Port 67	Automates assignment of IP address on a network

ქსელური ტოპოლოგიის არჩევასთან ერთად ჩვენ ვსაზღრავთ, რა ტიპის მოწყობილობების, კაბელების და ქსელური ადაპტერების გამოყენებას ვაპირებთ ქსელში. ამასთან ერთად, ინტერნეტპროვაიდერთან კავშირიც უნდა დამყარდეს. ერთ-ერთი ნაბიჯი ქსელის აგებაში არის განსაზღვრა ქსელური კომპონენტებისა, რომლებიც იმუშავებენ როგორც მომხმარებლის მოწყობილობებთან, ასევე თავსებადნი იქნებიან კაბელურ გაყვანილობასთანაც.



აირჩიეთ კაბელის ტიპი რომელიც არის ყველაზე სასარგებლო და ოპტიმალური ფასის, მომხმარებლებისათვის და მომსახურეობებისათვის რომლებიც დაუკავშირდებიან ქსელს.

კაბელის ტიპები

ქსელის ზომა განსაზღვრავს ქსელური კაბელის ტიპს, ქსელების უდიდესი ნაწილი დღევანდელ დღეს არიან გაყვანილნი, ერთი ან მეთი ტიპის გრეხილი ხვეული წყვილის სპილენძის კაბელით:

- Cat5
- Cat5e
- Cat6
- Cat6A

- Cat5 და Cat5e გარეგნულად გვანან ერთმანეთს, თუმცა Cat5e კაბელის დამზადება უფრო მაღალი სტანდარტით ხდება, რათა შეიძლებოდეს უფრო მაღალი მონაცემთა გადაცემის სიჩქარის მიღება. Cat6 კაბელი კიდევ უფრო მაღალი სტანდარტით იწარმოება, Cat6-ს შეიძლება ჰქონდეს ცენტრში მაყოფი რომელიც ერთმანეთისაგან ყოფს წყვილებს კაბელის შიგნით.

ყველაზე გავრცელებული კაბელი რომელიც გამოიყენება ქსელიში არის Cat5e. ეს კაბელი უზრუნველყოგს 100მბიტ/წამში კავშირს 100მეტრ მანძილამდე. ზოგიერთ კომპანიაში და ახლად აშენებულ სახლებში აყენებენ Cat6 ტიპის კაბელს რათა წინასწარ მზარდი გამტარუნარიანობისათვის იყვნენ მომზადებულნი.

ყველაზე თანამდეროვე ტიპი გრეხილი წყვილის კაბელი არის Cat6A. მისი გადაცემის სიჩქარე აღწევს 10გიგაბიტ/წამს. ასეთ ეზერნეტის ქსელის აღმნიშვნელი აბრევიატურა არის 10GBase-T. ის არის აღწერილი IEEE 802.3an-2006 სტანდარტში.

ახალ ან განახლებულ შენობებს როგორც წესი გააჩნიათ რაიმე ტიპის UTP კაბელის გაყვანილობა რომელიც აკავშირებს თითოეულ ოფისს ცენრალურ წერტილს რომელსაც ეწოდება Main Distribution Facility(MDF). მაქსიმალური დისტანცია რომელზეც UTP კაბელს შეუძლია გადასცეს ინფორმაცია არის 100მ. თუ ინფორმაციის გადაცემა არის საჭირო უფრო შორ მანძილზე უნდა გამოვიყენოთ შუამავალი მოწყობილობები როგორებიც არიან გამმეორებლები და კონცენტრატორები.

ფასი

როდესაც ქმნით ქსელის დიზაინს, უნდა გაითვალისწინოთ ფასიც, კაბელების დამონტაჟება ძვირია, თუმცა პირველი, ერთჯერადი დანახარჯის შემდგომ მისი მოვლა, როგორც წესი, ძვირი არ ჯდება. მოწყობილობების უმეტესობა, რომლებიც შეერთებულია ამ ქსელში, ღირს ბევრად უფრო ნაკლები იმ მოწყობილობებთან შედარებით, რომელთა შეერთებაც ხდება უკაბელო ქსელში.

უსაფრთხოება

კაბელირებული ქსელი, როგორც წესი, უკაბელო ქსელზე უფრო უსაფრთხოა. კაბელი, ძირითადად, კედლებსა და ჭერშია გაყვანილი და, შესაბამისად, არ არიან ადვილად მისაწვდომნი, ხოლო უკაბელო ქსელის „მოსმენა“ უფრო ადვილია, სიგნალები მიდიან ყველასთან, ვისაც აქვს მიმღები, შესაბამისად, მისი უსაფრთხოებისათვის გვესაჭიროება შიფრაცია.

სამომავლო დიზაინი

ბევრი ორგანიზაცია ირჩევს უმაღლესი კატეგორიის კაბელს, რათა მომავლაში, როდესაც გამტარუნარიანობისადმი მოთხოვნები გაიზრდება, არ დასჭირდეს გამოცვლა სრული კაბელური გაყვანილობის. იცოდეთ, თქვენი და თქვენი კლიენტის გადასაწყვეტია, აუცილებელია თუ არა უმაღლესი კატეგორიის კაბელის გამოყენება.

უკაბელო

უკაბელო გადაწყვეტა შეიძლება გამოვიყენოთ იქ, სადაც რთულია ან შეუძლებელი კაბელის გაყვანა. წარმოიდგინეთ ძველი ისტორიული შენობა, იქ აკრძალულია სტრუქტურული ცვლილებები. ამ შემთხვევაში კაბელის გაყვანა შეუძლებელია და უკაბელო კავშირი ერთადერთი გადაწყვეტაა.

ინტერნეტპროვაიდერის არჩევამ შეიძლება დიდი ზეგავლენა მოახდინოს თქვენს ქსელზე.

სამი ძირითადი გასათვალისწინებელი ფაქტორი ინტერნეტ კავშირის არჩევის დროს:

- სიჩქარე
- საიმედოობა
- წვდომადობა

POTS – ჩვეულებრივი ძველი სატელეფონო სისტემა Plain old telephone system POTS კავშირი არის ძალიან ნელი, თუმცა ხელმისაწვდომია ყველგან, სადაც არის ტელეფონი. მოდემი მონაცემების გადასაცემად და მისარებად სატელეფონო ხაზს იყენებს.

ISDN – ინტეგრირებულ მომსახურებათა ციფრული ქსელი Integrated Services Digital Network (ISDN) გვთავაზობს უფრო სწრაფ დაკავშირებას და dial-up-თან შედარებით სიჩქარეც მეტი აქვს. ის აძლევს საშუალებას რამდენიმე მოწყობილობას, გაინაწილოს

ერთი სატელეფონო ხაზი. ის ძალიან საიმედოა, იყენებს POTS ხაზებს და ხელმისაწვდომია იქ, სადაც სატელეფონო კომპანია ახორციელებს ციფრული სიგნალების გადაცემას.

DSL (Digital Subscriber Line) DSL ისევე, როგორც ISDN-ი, გვაძლევს შასუალებას რამდენიმე მოწყობილობამ გაინაწილოს ერთი სატელეფონო ხაზი. თუმცა მისი სიჩქარე, როგორც წესი, უფრო მეტია ISDN-თან შედარებით.

ამ ტექნოლოგიას შეზღუდვებიც აქვს, არ არის ხელმისაწვდომი ყველგან და უკეთ მუშაობს ე.წ. „ატეესთან“ ახლოს. ის ბევრად უფრო სწრაფია ინფორმაციის მიღებაში, ვიდრე გადაცემაში. და კიდევ, ზოგჯერ ხაზი, რომელზეც ის მუშაობს, არ შეესაბამება საჭირო ხარისხს.

Cable – კაბელური ინტერნეტ კავშირი ეს კავშირი არ იყენებს სატელეფონო ხაზს, არამედ კოაქსიალურ კაბელს, რომლებზეც თავდაპირველად მხოლოდ სატელევიზიო არხები მოგზაურობდნენ. ისევე, როგორც DSL, ის გვთავაზობს მაღალ სიჩქარეებს და always-on, ანუ ყოველთვის ჩართულ კავშირს. რაც ნიშნავს იმას, რომ მაშინაც კი, როდესაც კავშირი ინტერნეტთან არ გამოიყენება, ის ხელმისაწვდომია. მრავალი კაბელური კომპანია ასევე სატელეფონო კავშირსაც სთავაზობს მომხმარებლებს.

იმის გამო, რომ საკაბელო ტელევიზია ძალიან ბევრ სახლშია, ის კარგი ალტერნატივაა იმათთვის, ვისაც არა აქვთ საშუალება, მიიღონ DSL მომსახურება. თეორიულად სატელევიზიო კაბელის გამტარუნარიანობა უფრო დიდია DSL-თან შედარებით, თუმცა ის შეიძლება ხელოვნურად იყოს შეზღუდული მომწოდებლის მიერ.

Satellite – სატელიტური კავშირი

მაღალმთიან რეგიონებში სწრაფი ინტერნეტის მისაღებად სატელიტური კავშირი იდეალური გადაწყვეტაა. სატელიტური თეფში გამოიყენება სიგნალების გადასაცემად და მისაღებად სატელიტისაგან, რომელიც გადასცემს სიგნალებს ინტერნეტ პროვაიდერისაკენ.

სატელიტური კავშირის ინსტალაციის ფასი და ყოველთვიური გადსახადი ბერვად უფრო მაღალია DSL-ისა და კაბელური კავშირის მომსახურებებთან შედარებით. ძლიერმა შტორმმა შეიძლება გააუარესოს კავშირი ხარისხი ან საერთოთ გაწყვიტოს. ამიტომ, როგორც წესი, მომწოდებელი ალტერნატიული dial-up კავშირითაც ამარაგებს მომხმარებელს.

უკაბელო – Wireless
მრავალგვარი ტექნოლოგიის უკაბელო ინტერნეტის მომსახურება არის დანერგილი და

ხელმისაწვდომი. კომპანიები, რომლებიც გვთავაზობენ ფიჭურ კავშირს, შეიძლება იმავდროულად გვთავაზობდნენ ინტერნეტსაც. PCMCIA და PCI კარტები გამოიყენება კომპიუტერის ინტერნეტთან დასაკავშირებლად. მაგრამ ეს მომსახურება არ არის ხელმისაწვდომი ყველა ადგილას.

კომპანიამ შეიძლება შემოგვთავაზოს ინტერნეტი მიკროტალღური ტექნოლოგიის გამოყენებით, ამ შემთხვევაში სიგნალი შეიძლება გადაიცემოდეს პირდაპირ ანტენაზე, რომელიც დამონტაჟებული შენობის სახურავზეა დამონტაჟებული.

ინტერნეტ პროვაიდერის არჩევამდე ვითარების და შესაბამისად უნდა გაარკვიოთ, რა ტიპის კავშირი გამოგადგებათ. შეადარეთ კავშირების სიჩქარე, საიმედოობა და ფასი კონტრაქტის გაფორმებამდე.

ყოველ ხელსაწყოს ქსელში ესაჭიროება ქსელური ადაპტერი. არსებობს მრავალი ასეთი ადაპტერი:

- სტაციონალური კომპიუტერის ქსელური ინტერფეისის უმეტესი ადაპტერი ან დედაპლატაშია ინტეგრირებული, ან სლოტში ჯდება.
- პორტატული კომპიუტერის ქსელური ინტერფეისის უმეტესი ადაპტერიც ან დედაპლატაშია ინტეგრირებული, ან ერთდება კომპიუტერში PC Card-ის სახით ან ExpressBus სლოტში.
- USB ქსელური ადაპტერები ერთდება ნებისმიერ ხელმისაწვდომ USB პორტში და მათი გამოყენება შეიძლება როგორც სტაციონარულ, ასევე პორტატულ კომპიუტერებში.

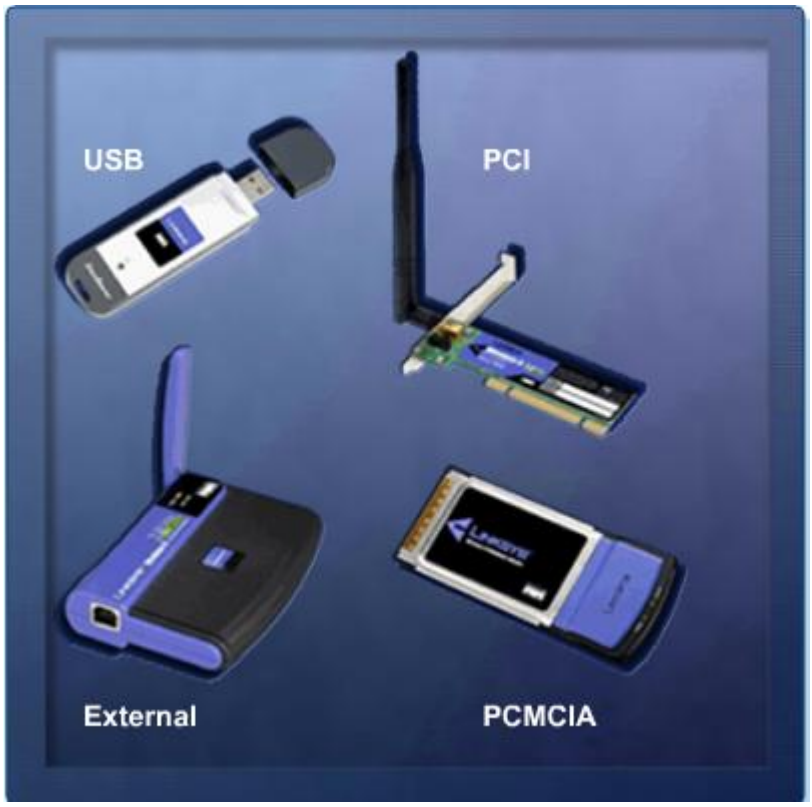
ქსელური ადაპტერის ყიდვამდე გაარკვიეთ მისი ფასი, დიზაინი და შესაძლებლობები. გაარკვიეთ, რა სიჩქარე და შესაძლებლობები აქვთ კონცენტრატორსა და კომუტატორს, რომელიც იქნება მიერთებული კომპიუტერზე.

ეზერნეტის ქსელური ადაპტერები უკუთავსებადნი ძველ თაობებთან შეიძლება იყვნენ:

- თუ გაქვთ ქსელური ადაპტერი 10/100 Mbps სიჩქარით და კონცენტრატორი რომელიც მუშაობს 10 Mbps, მაშინ თქვენი ადაპტერი იმუშავებს 10 Mbps სიჩქარით.

- თუ თქვენ გაქვთ 10/100/1000 Mbps ქსელური ადაპტერი და კომუტატორი, რომელიც მუშაობს 100 Mbps სიჩქარით, მაშინ თქვენი ადაპტერი იმუშავებს 100 Mbps სიჩქარით.

თუმცა, თუ გაქვთ გიგაბიტიანი კომპუტატორი, მაშინ უმჯობესია თუ იყიდით გიგაბიტიან ქსელურ ადაპტერს, რათა მათი სიჩქარეები დაემთხვეს ერთმანეთს. თუ არის პერსპექტივა, რომ ქსელი გარდაიქმნება გიგაბიტ ეზერნეტში, მაშინ შეიძინეთ ადაპტერი, რომელსაც შეუძლია ამ სიჩქარის უზრუნველყოფა. მათი ფასები შეიძლება დიდად განსხვავდებოდეს შესაბამისად შეიძინეთ ზუსტად ის ადაპტერი, რომელიც ესაჭიროება თქვენს კლიენტებს.



უკაბელო ქსელური ადაპტერები მრავალი ფორმატის და მრავალგვარი შესაძლებლობის არსებობს. თქვენ უნდა აირჩიოთ ადაპტერი იმისდა მიხედვით, თუ რომელი სტანდარტის უკაბელო ქსელის დაყენებას აპირებთ:

- 802.11b ადაპტერები შეიძლება იყნენ ასევე გამოყენებულნი 802.11g ქსელებში.
- 802.11b და 802.11g ადაპტერები შეიძლება იყნენ ასევე გამოყენებულნი 802.11n ქსელებში.
- 802.11a შეიძლება იყოს გამოყენებული მხოლოდ 802.11a ქსელებში.

ამოირჩიეთ უკაბელო ადაპტერები, რომლებიც ემთხვევა თქვენი კლიენტის მოთხოვნებს. თქვენ უნდა იცოდეთ, რა ტიპის უკაბელო აპარატურა იქნება გამოყენებული და რა იქნება დაინსტალირებული ქსელზე, რათა უზრუნველყოთ შესაბამისობა და გამოყენებისთვის ვარგისობა.

რამდენიმე ტიპის მოწყობილობა არის ხელმისაწვდომი კომპონენტების ქსელთან დასაკავშირებლად. თქვენ ამოირჩიეთ ის მოწყობილობები, რომლებიც დაემთხვევა თქვენი კლიენტის მოთხოვნებს.

კონცენტრატორები – Hubs
კონცენტრატორი გამოიყენება ქსელში რამდენიმე მოწყობილობას შორის მონაცემების გასანაწილებლად. კონცენტრატორი შეიძლება უკავშირდებოდეს სხვა ტიპის ქსელურ მოწყობილობას, ისეთის, როგორიც არის კომუტატორი ან მარშრუტიზატორი, რომელიც, თავის მხრივ, დააკავშირებს მას ქსელის სხვა ნაწილთან ან სხვა თავად ქსელთან. ქსელის მაქსიმალური სიჩქარე განისაზღვრება კონცენტრატორის სიჩქარით.

კონცენტრატორები დღესდღეობით ნაკლებად გამოიყენებიან. ამის მიზეზი არის კომუტატორების ეფექტურობა და დაბალი ფასი. კონცენტრატორები არ ახდენენ ქსელური ტრაფიკი სეგმენტირებას, შესაბამისად, ისინი ამცირებენ ხელმისაწვდომ გამტარუნარიანობას ყველა მოწყობილობისათვის. აგრეთვე, კონცეტრატორებს არ შეუძლიათ გაფილტრონ მონაცემები, ამის გამო დიდი რაოდენობით არასასურველი ტრაფიკი მოგზაურობს ყველა მოწყობილობას შორის.

მისი ერთი უპირატესობა არის ის, რომ ახდენს სიგნალის გაძლიერებას, როდესაც ის გაივლის კონცენტრატორს. ეს ნიშნავს, რომ კონცეტრატორი შეგვიძლია ასევე გამოვიყენოთ როგორც გამმეორებელი, კონცენტრატორს შეუძლია გაზარდოს ჩვენი ქსელის განფენილობა, რადგანაც სიგნალის გაძლიერება, დაძლევს დისტანციით შექმნილ დაბრკოლებას.

კომუტატორები – Switches თანამედროვე ქსელებში კომუტატორებმა შეცვალეს კნცენტრატორები, როგორც კავშირების ცენტრალური კვანძები. როგორც კონცენტრატორის, კომუტატორის სიჩქარეც განსაზღვრავს ქსელის მაქსიმალურ სიჩქარეს. თუმცა კომუტატორები ფილტრავენ და ასეგმენტებენ ქსელურ ტრაფიკს მონაცემების გაგზავნით მხოლოდ დანიშნულების ადგილზე. ეს უზრუნველყოფს უფრო მეტ გამტარუნარიანობას თითოეული მოწყობილობისათვის ქსელში.

კომუტატორებს აქვთ კომუტაციის ცხრილი. მასში არის ქსელში არსებული ყველა ფიზიკური (MAC) მისამართის სიას. კომუტაციის ცხრილი სწავლობს მისამართებს შემოსულ კადრებში წყაროს მისამართის წაკითხვით და თან იმახსოვრებს, რომელი პორტიდან შემოვიდა ეს კადრი. ამის შემდგომ ქმინს ცხრილს, რომელშიც ასახულია, რომელი მისამართი რომელ გამომავალ პორტს შეესაბამება. როდესაც მოვა კადრი, რომელიც კონკრეტული მისამართისკენ უნდა გადაიგზავნოს, კომუტატორი ხელმძღვანელობს ამ ცხრილით იმის გადასაწყვეტად, თუ რომელი გამომავალი პორტი გამოიყენოს კადრის გადასაგზავნად დანიშნულების ადგილისაკენ. იმის გამო, რომ კადრი იგზავნება მხოლოდ ერთ პორტში, დანარჩენები ზეგავლენას არ განიცდიან, და სრულად ქსელზე გამტარუნარიანობაც ზეგავლენას არ განიცდის.

მარშრუტიზატორები – Routers მარშრუტიზატორები აკავშირებენ ერთამანეთს ქსელებს. კორპორატიულ ქსელში როუტერის ერთი პორტი უერთდება WAN კავშირს, ხოლო დანარჩენები – კორპორაციის ლოკალურ ქსელებს. მარშრუტიზატორი ხდება გასასვლელი ლოკალური ქსელისათვის გარე სამყაროში. საოჯახო ქსელში ის აკავშირებს კომპიუტერებს და ქსელურ მოწყობილობებს. უკაბელო მარშრუტიზატორი მუშაობს ისე, როგორც firewall-ი და ამავდროულად გვაწვდის უკაბელო კავშირს. როდესაც საოჯახო ქსელის მარშრუტიზატორი ასრულებს რამდენიმე ტიპის მომსახურებას, მას შეიძლება ვუწოდოთ მრავალფუნქციური მოწყობილობა.

ინტერნეტ პროვაიდერის აპარატურა

როდესაც ირჩევთ ინტერნეტ პროვაიდეს, უნდა გაიგოთ, რა ტიპის აპარატურა არის ხელმისაწვდომი, რათა აირჩიოთ ყველაზე შესაფერისი მოწყობილობა. მრავალი ინტერნეტ პროვაიდერი შემოგთავაზებთ ფასდაკლებას აპარატურაზე, რომლის შეძენაც ხდება მომსახურების შეძენის დროს.

ზოგიერთი პროვაიდერისგან შეიძლება იქირავოთ აპარატურა. ეს შეიძლება უფრო ხელსაყრელი წინადადება იყოს, რადგანაც პროვაიდერები ზრუნავენ თავიანთ აპარატურაზე და მათი გაფუჭების, ცვლილების ან განახლების შემთხვევაში თქვენ დამატებითი ხარჯისგან ტავისუფალი იქნებით. სახლის მომხმარებლებმა უმჯობესია შეიძინონ აპარატურა პროვაიდერისაგან, რადგანაც გარკვეული დროის შემდგომ პირვანდელი ფასი მოწყობილობის უფრო დაბალი იქნება ქირაობასთან შედარებით.

კაბელების გაყვანა, იქნება ეს სპილენძის თუ ოპტიკურ-ბოჭკოვანი, შეიძლება ხშირად სახიფათოც იყოს. ზოგჯერ კაბელები ჭერში ან კედლებში უნდა იყვნენ გატარებული, სადაც სხვადასხვა დაბრკოლება შეიძლება დაგვხდეთ. თქვენ უნდა გეცვათ ისეთი ტანსაცმელი, რომელიც დაგიცავთ იმ შემთხვევაში, თუ ტოქსიკურ ნივთიერებებს შეეხებით. შესაბამისად, თქვენმა სამოსმა უნდა დაფაროს თქვენი ფეხები და მკლავები. აუცილებლად ატარეთ დამცავი სათვალე. თუ შესაძლებელია, ჰკითხეთ შენობის კომენდანტს ან სხვა პასუხისმგებელ პირს, თუ არის რაიმე დაბრკოლება, რომლის შესახებაც უნდა იცოდეთ, სანამ დაიწყებთ მუშაობას.

კიბის გამოყენების დროს გასათვალისწინებელი საფრთხეები:

- წაიკითხეთ ეტიკეტი კიბეზე და დაიცავით უსაფრთხოების ყველა ზომა
- არასოდეს არ დადგეთ კიბის სულ ზედა საფეხურზე, რადგანაც ადვილად შეიძლება დაკარგოთ წონასწორობა და ჩამოვარდეთ.
- დარწმუნდით, რომ გარშემომყოფებმა იციან, თქვენ რომ კიბეზე ხართ
- შემოფარგლეთ თქვენი სამუშაო სივრცე გამაფრთხილებელი ლენტით ან კონუსებით.

- როდესაც იყენებთ კიბეს, რომელიც ეყრდნობა კედელს, მიჰყევით მასზე მოცემულ უსაფრთხოების ინსტრუქციებს და სთხოვეთ ვინმეს, სიმტკიცისთვის დაიჭიროს კიბე.

ხელსაწყოები, რომლებიც საჭიროა სპილენძის ან ოპტიკურ-ბოჭკოვანი კაბელების ინსტალაციისათვის, შესაძლოა იყოს სახიფათო. ეს წესები ყოველთვის უნდა დაიცვათ, როდესაც მუშაობთ კაბელებთან:

- დარწმუნდით, რომ ხელსაწყოები, რომლებსაც იყენებთ, არის კარგ მდგომარეობაში.
- არ იჩქაროთ და ფრთხილად იმუშავეთ, რომ შემთხვევით ან საკუთარი თავი, ან სხვა არ ჩააგდოთ საფრთხეში.
- ყოველთვის, როდესაც ჭრით ან ატყავებთ კაბელებს, გქონდეთ დამცავი სათვალე, რადგანაც მცირე ზომის ფრაგმენტი შეიძლება თვალში მოგხვდეთ.
- თუ ამის საჭიროება და შესაძლებლობაა, გეკეთოთ ხელთათმანი; ნარჩენები წესების დაცვით გაანადგურეთ.

განსაკუთრებით საღად იაზროვნეთ პრობლემის გადაჭრის დროს. თუ დახმარება დაგჭირდათ, მიმართეთ სხვა პიროვნებას.

როდესაც მუშაობთ ოპტიკურ-ბოჭკოვან კაბელებთან, სპეციფიური ხელსაწყოები და ქიმიკატები უნდა გამოიყენოთ. მათი გამოყენებისას უნდა გამოიჩინოთ სიფრთხილე:

ქიმიკალიები
გამხსნელები და წებო, რომელებიც გამოიყენება ოპტიკურ-ბოჭკოვან კაბელებთან, სახიფათოა. ყოველთვის წაიკითხეთ და დაიცავით მათი ინსტრუქცია.

ხელსაწყოები
ნებისმიერი ხელსაწყოთი მუშაობისას უსაფრთხოება უნდა იყოს პირველი რიგის ამოცანა. ნებისმიერი კომპრომისი უსაფრთხოებაში შეიძლება გახდეს მიზეზი სხეულის სერიოზული დაზიანებისა და სიკვდილისაც კი. ხელსაწყოებს, რომლებიც გამოიყენება შუშის დასაჭრელად, ბასრი პირები აქვთ და დიდი სიფრთხილით უნდა მოხმარა კაბელების მოჭერისათვის მაღალი წნევით, რათა გაუკეთდეთ კონექტორები. ამ ხელსაწყოების გამოყენებამ შეიძლება გამოიწვიოს შუშის პატარა ნამსხვრევების გაფანტვა ჰაერში. უნდა აირიდოთ ისინ თქვენი კანიდან, პირიდან და თვალებიდან.

მავნე შუქი

დაიცავით თქვენი თვალები მავნე შუქისგან, რომელიც შეიძლება იყოს ოპტიკურ-ბოჭკოვანი კაბელების გულებში. ის ადამიანის თვალისთვის შეუმჩნეველი ფერისაა, ამიტომ შეიძლება ისე დააზიანოს თქვენი თვალი, რომ ვერც კი შეიგრძნოთ. როდესაც

იყენებთ გამადიდებელ შუშას კაბელის გამოკვლევისათვის, სინათლე შეიძლება აირეკლოს ამ შუშამ და მოგხვდეთ თვალებში. შესაბამისად, როდესაც იმუშავებთ ამ ტიპის კაბელებთან, დარწმუნდით, რომ ის გამოერთებულია სინათლის წყაროდან. სპეციალურ დეტექტორებს შეუძლიათ გითხრან, არის თუ არა ის ენერგიით დატუმბული.

მინის ზედა ფრთები

როდესაც ჭრით ან უჭერთ ოპტიკურ-ბოჭკოვან კაბელებს, შეიძლება მათმა უმცირესმა ნაწილაკებმა შეაღწიონ თქვენს თვალებსა ან კანში და გამოიწვიონ სერიოზული გაღიზიანება. მათი შემჩნევა სხეულზე ძალიან ძნელია, რადგან გამჭვირვალენი არიან. მუშაობის პროცესში იატაკზე უნდა გქონდეთ დაფენილი მუქი ფერის მატრასი, რათა შეძლოთ დანახვა ამ ნაწილაკებისა. მატრასი ასევე ქიმიკალიების გამძლე უნდა იყოს.

სამუშაო ადგილი ყოველთვის სუფთა და მოხერხებული უნდა იყოს. არასოდეს არ აიღოთ ნარჩენები ხელით. გამოიყენეთ ლენტი პატარა ნაჭრების ასაღებად და გადააგდეთ ისინი წესების დაცვით. კონტეინერის დანიშნულებით შეგიძლიათ გამოიყენოთ პლასტმასის ბოთლი, რომელსაც მჭიდრო სარქველი აქვს.

გაფრთხილება: გაიარეთ შესაბამისი ტრეინინგი, სანამ შეეცდებით გაჭრათ, გაატყაოთ ან მოუჭიროთ ოპტიკურ-ბოჭკოვან კაბელს. გამოცდილმა ტექნიკოსმა უნდა გიხელმძღვანელოთ მანამ, სანამ არ მიიღებთ საკმარის გამოცდილებას.

გაფრთხილება: როდესაც მუშაობთ კაბელებთან, ყოველთვის გამოიყენეთ დამცავი სათვალე და არასოდეს შეეხოთ არანაირი ტიპის კაბელის წვერებს შიშველი ხელით.

სპილენძის კაბელებთან დაკავშირებული საფრთხეები
სპილენძის კაბელებიც შეიძლება იყვნენ სახიფათონი. როდესაც გაჭრით სპილენძის კაბელს, მისმა პატარა ნაწილეკბმა შეიძლა დააზიანოს თქვენი კანი. ეს ნაწილაკები ასევე ჰაერშიც იფანტებიან და გახსოვდეთ, რომ ყოველთვის უნდა გეკეთოთ დამცავი სათვალე როდესაც ჭრით ნებისმიერი ტიპის კაბელს.

ხელსაწყოები, რომლებსაც გამოიყენებთ სპილენძის კაბელთან მუშაობის დროს, შესაძლოა იყვნენ სახიფათონი თუ მათ არასწორად მოიხმართ. აუცილებლად წაიკითხეთ ინსტრუქცია, რომელიც მათ მოყვება. ივარჯიშეთ კაბელის ნაგლეჯზე და სთხოვეთ გამოცდილ ინსტალატორს დახმარება, თუ ატყობთ, რომ გესაჭიროებათ.

გახსოვდეთ, რომ სპილენძის კაბელი დენის გამტარია. მოწყობილობის დაზიანებამ, სტატიკურმა დენმა ან ელვამ შეიძლება გამოიწვიონ დამუხტვა გამოერთებული

კაბელისაც კი. თუ არ ხართ დარწმუნებულნი, რომ უსაფრთხოა, შეამოწმეთ მარტივი ვოლტმეტრით.

ქსელის ინსტალაცია და ტესტირება, ინტერნეტთან კავშირის დამყარება და ქსელური რესურსების კონფიგურაცია

კლიენტის ქსელის გაუმჯობესება, უკაბელო ქსელის ადაპტერის ინსტალაცია და კონფიგურაცია, უკაბელო ქსელის მარშრუტიზატორის ინსტალაცია და კონფიგურაცია

ქსელის ინსტალაცია და აწყობა შეიძლება იყოს რთული ამოცანა. ზოგიერთი პატარა ქსელის ისნტალაციაც კი შეიძლება გახდეს რთული და ხანგრძლივიც. თუმცა სწორი დაგეგმვა დაგეხმარებათ პროცესის გამარტივებასა და სისწრაფეში.

ინსტალაციის დროს შესაძლებელია ცოტა ხნით არსებული, ძველი ქსელის გათიშვა. მაგ., გათიშვა შეიძლება გამოიწვიოს ქსელური კაბელის შეცვლამ. პროექტი არ ითვლება დასრულებულად, სანამ არ მოხდება ყველა მოწყობილობის ინსტალაცია, კონფიგურაცია და ტესტირება.

მას შემდგომ, რაც განსაზღვრავთ ადგილმდებარეობას ყველა ქსელური მოწყობილობისათვის, შეგიძლიათ შეუდგეთ კაბელის გაყვანას. ზოგიერთ ახალ ან განახლებულ შენობაში კაბელების გაყვანა წინასწარ ხდება, რათა თავი აარიდონ ამოყვანილი კედლების ნგრევას.

ქსელის ინსტალაციის ნაბიჯები

გახსოვდეთ, კაბელის გაყვანის დაწყებამდე წინასწარი სამუშაო უნდა შეასრულოთ, უნდა მოემზადოთ უშუალოდ ამ პროცესისთვის – შეიმუშაოთ კაბელის გაყვანის გეგმა და ყველა საჭირო იარაღი და მასალა მოაგროვოთ.

1.კედლებსა და ჭერში კაბელების გაყვანისათვის უნდა შეუსრულოთ ეგრეთ წოდებული ოპერაცია cable pull, რაც ნიშნავს, რომ ერთი პიროვნება ქაჩავს კაბელს, ხოლო მეორე აწვდის მას კედელიI. კაბელის ორივე წვერზე რაიმე ტიპის იდნეტიფიკატორები აუცილებლად მიამაგრეთ. ეს მარკირება

მოახდინეთ ან უკვე არსებული წესდების მიხედვით, ან TIA/EIA 606-A სტანდარტის მიხედვით.

2. მას შემდგომ, რაც მოახდენთ კაბელის ორივე მხარის ტერმინირებას, უნდა გამოცადოთ, რომ დარწმუნდეთ მის გამართულ მუშაობაში.

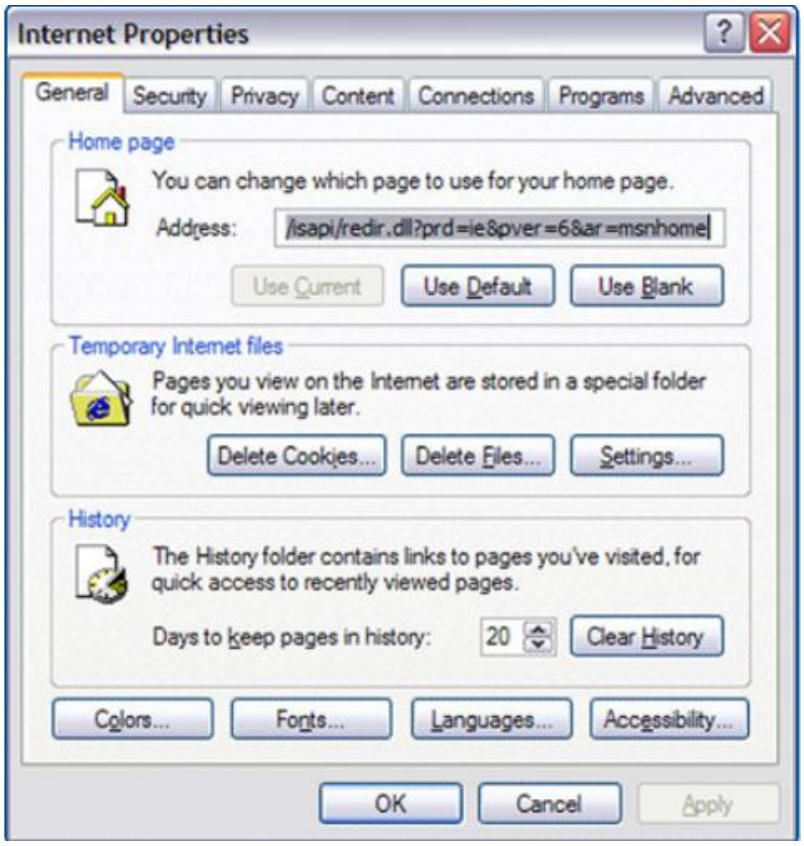
3.დარწმუნდით, რომ ქსელური ინტერფეისები სწორად არიან დაინსტალირებული სტაციონალურ და პორტატულ კომპიუტერებსა და ქსელურ პრინტერებზე. მას შემდგომ, რაც ქსელური ინტერფეისები იქნებიან დაინსტალირებულნი, დააკონფიგურეთ კლიენტებზე პროგრამული უზრუნველყოფა და მიანიჭეთ IP მისამართები ყველა მოწყობილობას.

4. დააინსტალირეთ კომუტატორები და მარშრუტიზატორები უსაფრთხო ცენტრალურ ადგილას. ლოკალური ქსელის ყველა კავშირი უნდა ტერმინირდებოდეს ამ ადგილზე. საოჯახო ქსელში თქვენ შეიძლება მოგიწიოთ ამ მოწყობილობების სხვადასხვა ადგილას განლაგება ან გქონდეთ მხოლოდ ერთი მოწყობილობა.

5. დააინსტალირეთ ეზერნეტის პატჩ-კაბელი კედელზე განლაგებული აუტლეტიდან თითოეულ ქსელურ მოწყობილობამდე. შეამოწმეთ, გაქვთ თუ არა ანთებული სინათლე ყველა ქსელურ ინტერფეისზე. საოჯახო ქსელში დარწმუნდით, რომ თითოეული ქსელური მოწყობილობის პორტი, რომელიც უკავშირდება მოწყობილობას, არის ანთებული.

6. როდესაც ყველა მოწყობილობა არის დაკავშირებული და ყველა კავშირის შესაბამისი ნათურა ანათებს, დადგა დრო ქსელური კავშირების ტესტირებისა. გამოიყენეთ ბრძანება ipconfig /all CMD-ში, რათა დაინახოთ IP მისამართების კონფიგურაცია ყველა კომპიუტერზე. გამოიყენეთ ბრძანება ping, რათა შეამოწმოთ კავშირი. თქვენ უნდა შეგეძლოთ ქსელში არსებული სხვა კომპიუტერების, gateway-ის და ლოკალურ ქსელს გარეთ მყოფი კომპიუტერების დაპინგვა. მას შემდგომ, რაც დადასტურდება კავშირის არსებობა, უნდა დააკონფიგურიროთ და გამოცადოთ ისეთი ქსელური პროგრამები, როგორიც არის ელექტრონული ფოსტის კლიენტი და ინტერნეტის ბრაუზერი.

მას შემდგომ, რაც ქსელის აწყობა და ტესტირება წარმატებით დამთავრდა, უნდა დააკონფიგურიროთ ვებ ბრაუზერი, ისეთი, როგორიც, მაგალითად, არის Microsoft Internet Explorer-ი. თქვენ შეგიძლიათ განახოციელოთ ეს კონფიგურაცია ინტერნეტის თვისებების (Internet Properties) ფანჯრიდან. იხ. სურათი.



დროებითი ინტერნეტის ფაილები Temporary Internet Files

როდესაც ისეთი ოპერაციული სისტემაა დაყენებული, როგორიც არის ვინდოუს XP, მას მოყვება ზემოთ ხსენებული პროგრამაც. ამ პროგრამის გამოყენების დროს, როდესაც მომხმარებელი შედის ვებგვერდზე, დიდი რაოდენობით ფაილების გადმოწერა ხდება კომპიუტერის საქაღალდეში სახელწოდებით Temporary Internet Files. ამ ფაილების უმეტესობა არის სურათები, მაგ., სარეკლამო ბანერები და ვებგვერდის სხვა კომპონენტები.

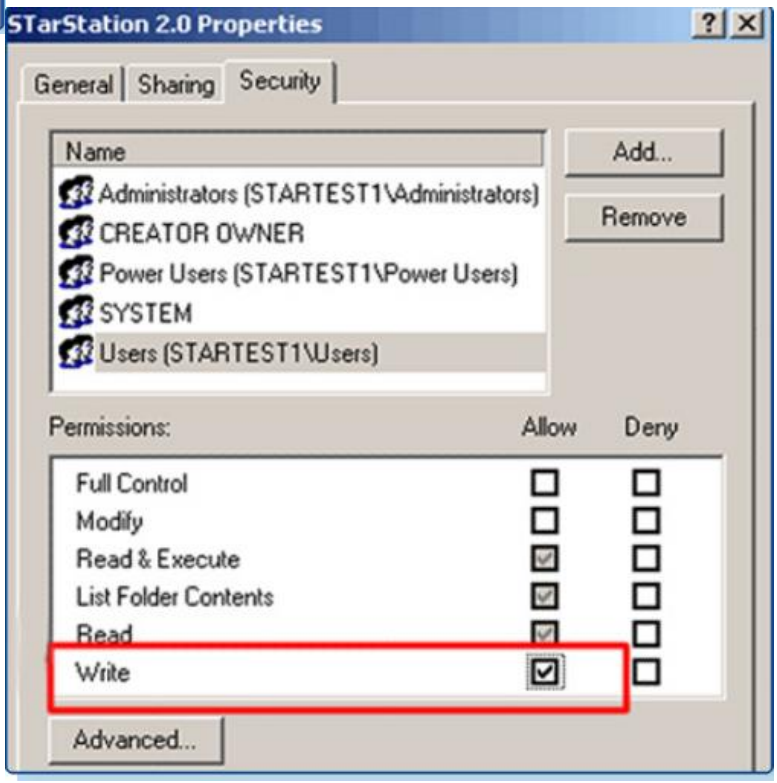
დროებითი ინტერნეტის ფაილები ინახება თქვენს კომპიუტერში, იმისთვის, რომ თუ მეორედ შეხვალთ ამ ვებგვერდზე, ის უფრო სწრაფად ჩაიტვირთოს. იმის და მიხედვით, თუ რა სიხშირით ათვალიერებთ ვებგვერდებს, შესაძლებელია, რომ ეს საქაღალდე სწრაფად აივსოს. იმისდა მიუხედავად რომ ეს არ არის ძალიან მნიშვნელოვანი, სჯობს, რომ თქვენ დროდადრო გაწმინდოთ ხოლმე ეს საქაღალდე, განსაკუთრებით მაშინ, როდესაც განახორციელებთ რაიმე საბანკო ტრანზაქციას თქვენი კომპიუტერიდან.

ძირითადი ბრაუზერი

თქვენ შეგიძლიათ აირჩიოთ ბრაუზერი, რომელიც უნდა გამოიყენოს ვინდოუსმა როგორც ძირითადი. დააჭირეთ **Start > Run**, შეიყვანეთ ვებგვერდის მისამართი და დააჭირეთ **OK**-ს ვებ გვერდი გაიხსნება ძირითადი ბრაუზერის მეშვეობით. თუ გსურთ, რომ IE იყოს თქვენი ბრაუზერი, დაიწყეთ მისი ჩართვით, შემდგომ აირჩიეთ ხელსაწყოების (Tools) პუნქტი მენიუდან > ინტერნეტის პარამეტრები (Internet Options) პროგრამების ტაბზე შეგიძლიათ შეამოწმოთ, არის თუ არა IE თქვენი ძირითადი ბრაუზერი., და შეგიძლიათ აირჩიოთ ის, თუ ასე გსურთ.

ფაილების გაცვლა File Sharing მომხმარებლებს შეუძლიათ გაუნაწილონ ერთმანეთს რესურსები ქსელის მეშვეობით. თქვენ შეგიძლიათ გაანაწილოთ ერთი ფაილი, კონკრეტული საქაღალდე ან მთლიანი დისკი. იხ. სურათი.

იმისთვის, რომ ერთი ფაილის განაწილება განახორციელოთ, პირველ რიგში გადააკოპირეთ ის საქაღალდეში. დააჭირეთ მაუსის მარჯვენა ღილაკს საქაღალდეზე და აირჩიეთ Sharing and Security. თქვენ შეგიძლიათ განსაზღვროთ, ვის და რა უფლება ჰქონდეს ამ საქაღალდეზე. იხ. სურათი.



Permissions ანუ უფლებები განსაზღვრავენ რა ტიპის უფლებები ჰქონდეს მომხმარებელს საქაღალდეზე:

- Read – წაკითხვის უფლება, როდესაც მოხმრებელს შეუძლია შევიდეს საქაღალდეში, გახსნას და დაათვალიეროს ქვესაქაღალდეები და ფაილები.
- Change – როდესაც მომხმარებელს აქვს ყველა ზემოხსენებული უფლება და კიდევ უფლება, შექმნას ქვესაქაღალდეები და ფაილები, შეცვალოს ინფორმაცია ფაილებში და წაშალოს ქვესაქაღალდეები და ფაილები.
- Full Control – სრული კონტროლი გულისხმობს ყველა ზემოხსენებულ უფლებას და კიდევ უფლებას, შეცვალოს უფლებები საქაღალდეზე, თუ არსებული საქაღალდე არის NTFS ფაილურე სისტემის დანაყოფზე.

Windows XP Professional-ის შეზღუდვა არის მაქსიმუმ. 10 ერთდროული ფაილების გაზიარებითი კავშირი.

Printer Sharing – პრინტერის გაზიარება იმისთვის, რომ პრინტერის გაზიარება მოახდინოთ, აირჩიეთ Start > Control Panel > Printers and Faxes. დააჭირეთ მარჯვენა ღილაკს პრინტერზე და ამოირჩიეთ Sharing-ი. დააჭირეთ **Share this Printer-ს და შემდგომ დააჭირეთ OK-ს**. ამის შემდგომ პრინტერთან კავშირს დაამყარებენ სხვა კომპიუტერებიც.

იმისთვის, რომ დაუკავშირდეთ სხვა კომპიუტერთან მიერთებულ პრინტერს, აირჩიეთ Start > Control Panel > Printers and Faxes. დააჭირეთ Add Printer-ს, გამოიყენეთ დამხმარე უტილიტა, რათა მოძებნოთ და დააინსტალიროთ პრინტერი.

თქვენ უნდა შეგეძლოთ გაძლიერება, ინსტალაცია და კონფიგურაცია კომპონენტებისა, როდესაც კლიენტი მოგთხოვთ მეტ სიჩქარეს და ფუნქციებს ქსელში. ისეთი მოწყობილობები, როგორიც არის უკაბელო წვდომის წერტილი, უკაბელო ქსელის ადაპტერები, უფრო ჩქარი ქსელური ადაპტერები, უფრო ჩქარი ქსელური მოწყობილობები და კაბელები, შეიძლება ინტეგრირებულ იქნენ ქსელში, რათა კლიენტს მისცეთ კომუნიკაციის საშუალება უკაბელო ტექნოლოგიით ან უფრო სწრაფად.

თუ თქვენი კლიენტი დამატებით კომპიუტერებს ან უკაბელო ტექნოლოგიას, თქვენ უნდა შეგეძლოთ აპარატურის რეკომენდირება მისი მოთხოვნებიდან გამომდინარე. აპარატურა, რომელსაც თქვენ გაუწევთ რეკომენდაციას, უნდა შეესაბამებოდეს არსებულ მოწყობილობებსა და კაბელებს ან უნდა მოხდეს სრული ინფრასტრქტურის განახლება.

იმისთვის, რომ დაუკავშირდეთ უკაბელო ქსელს, თქვენს კომპიუტერს უნდა ჰქონდეს უკაბელო ქსელის ადაპტერი. უკაბელო ქსელის ინტერფეისი გამოიყენება კომუნიკაციისათვის სხვა უკაბელო მოწყობილობებთან, იქნება ეს კომპიუტერი, პრინტერი თუ უკაბელო წვდომის წერტილი.

უკაბელო ადაპტერის შეძენამდე უნდა დარწმნუდეთ, რომ ის შესაბამისია უკვე არსებული უკაბელო ქსელური მოწყობილობებისა, რომლებიც დაინსტალირებულნი არიან ქსელში, და ასევე დარწმუნდით, რომ მას სათანადო დიზაინი აქვს და შეესაბამება კომპიუტერს, რომლისთვისაც ყიდულობთ. უკაბელო USB ადაპტერი შეიძლება გამოყენებულ იქნეს ნებისმიერ კომპიუტერზე, რომელსაც აქვს თავისუფალი USB პორტი.

იმისთვის, რომ დააინსტალიროთ უკაბელო ქსელური ადაპტერი, სტაციონარულ კომპიუტერზე, პირველ რიგში, უნდა მოხსნათ კეისის კედელი,

დაამონტაჟოთ ის თავისუფალ PCI ან PCI express სლოტში. ზოგიერთი უკაბელო ქსელის ადაპტერს აქვს ანტენა, რომელიც მიერთებულია ადაპტერის უკანა ნაწილზე. ზოგიერთი მათგანი დაკავშირებულია კაბელის მეშვეობით, რომ გვქონდეს საშუალება, გადავიტანოთ ანტენა სიგნალის მიღების უკეთეს წერტილში.

მას შემდგომ, რაც უკაბელო ქსელის ადაპტერი იქნება დაინსტალირებული, არის რამდენიმე საკონფიგურაციო ნაბიჯი, მათ შორის, მოწყობილობის დრაივერების კონფიგურაცია და ქსელური ინფორმაციის დამატება. როდესაც ეს დასრულდება, კომპიუტერს უნდა შეეძლოს უკაბელო ქსელის აღმოჩენა და მასთან დაკავშირება.

უკაბელო ქსელის ადაპტერები შეიძლება იყენებდნენ „დამხმარე უტილიტას“ (wizard) უკაბელო ქსელთან დასაკავშირებლად. ასეთ შემთხვევაში თქვენ ჩადებდით კომპიუტერში კომპაქტ დისკს, რომელიც მოყვა ადაპტერს და მასში ჩაწერილ მითითებებს შეასრულებდით ქსელთან დასაკავშირებლად.

უკაბელო ქსელის ინსტალაციის დროს, უნდა გადაწყვიტოთ, სად დააყენოთ უკაბელო კავშირის წერტილები და შემდგომ დააკონფიგურიროთ ისინი. შემდეგი ნაბიჯები აღწერენ ინსტალაციის პროცესს:

1. გამოიყენეთ შენობის გეგმა კავშირის წერტილებისათვის, რომ მიიღოთ მაქსიმალური დაფარვის ზონა. საუკეთესო ადგილი კავშირის წერტილისათვის არის ზონის ცენტრში, ისე რომ უკაბელო კავშირის მოწყობილობებს ქონდეთ პირდაპირი თვალთახედვის გზა უკაბელო კავშირის წერტილამდე.
2. დააკავშირეთ კავშირის წერტილი არსებულ ქსელთან. უკაბელო მარშრუტიზატორის Linksys WRT300N მოდელს უკანა მხარეს აქვს 5 პორტი, შეაერთეთ DSL-ი ან კაბელური მოდემი პორტში, რომელსაც აწერია Internet კომუტაციის ლოგიკა არის ისეთი, რომ ყველა პაკეტი იგზავნება ამ პორტში, თუ არის კომუნიკაცია ინტერნეტიდან ან მისკენ. შეაერთეთ ერთი კომპიუტერი რომელიმე პორტში დანარჩენი ოთხიდან. რომ შეძლოთ საკონფიგურაციო ვებ გვერდზე მოხვედრა.
3. ჩართეთ მოდემი და შეაერთეთ დენი მარშრუტიზატორში. როდესაც მოდემი სრულად დაამყარებს კავშირს ინტერნეტ პროვაიდერთან, მარშრუტიზატორი ავტომატურად გამოკითხავს მოდემს საჭირო ინფორმაციას ინტერნეტთან დასაკავშირებლად. ეს ინფორმაცია არის IP მისამართი, ქვექსელის ნიღაბი და DNS სერვერების მისამართები.
4. როდესაც მარშრუტიზატორი დაამყარებს კავშირს მოდემთან, თქვენ უნდა დააკონფიგურიროთ მარშრუტიზატორი, რომ მან მოახდინოს დაკავშირება ქსელში არსებულ მოწყობილობებთან. ჩართეთ კომპიუტერი, რომელიც არის შეერთებული მარშრუტიზატორში. გახსენით ვებ ბრაუზერი, მისამართის ველში ჩაწერეთ 192.168.1.1, ეს არის ამ მოდელის მარშრუტიზატორის საკონფიგურაციო მისამართი.

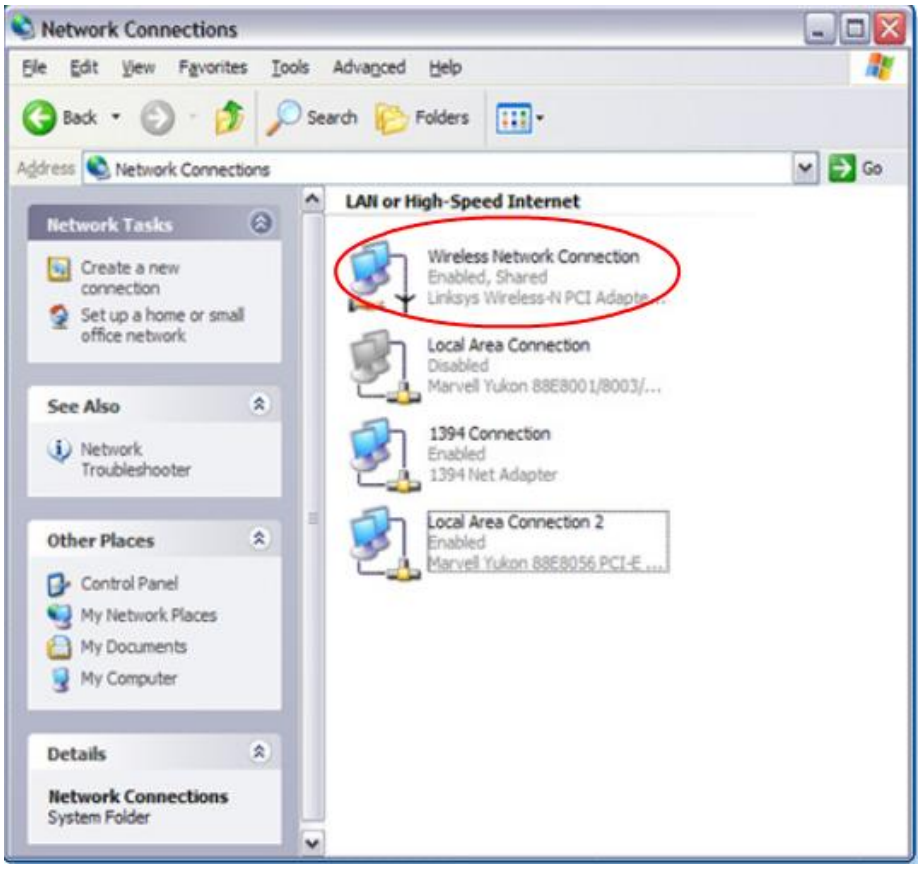
5. უსაფრთხოების ეკრანი გამოვა და მოგთხოვთ აუტენტიფიცირებას. მომხმარებლის ველი დატოვეთ ცარიელი და შეიყვანეთ სიტყვა admin, როგორც პაროლი.
6. გააგრძელეთ დაყენება, თქვენ ნახავთ ტაბებს, რომლებსაც აქვთ ქვეტაბები, და დაიმახსოვრეთ, რომ უნდა დააჭიროთ Save Settings ყოველ ეკრანზე ცვლილებების განხორციელების შემდგომ.

როდესაც იყენებთ 300N მარშრუტიზატორის საკონფიგურაციო ეკრანს, თქვენ შეგიძლიათ დააჭიროთ help ტაბს დამხმარე ინფორმაციის გამოსატანად. თუ ეს ინფორმაცია არ არის საკმარისი, მოიძიეთ ინსტრუქცია.

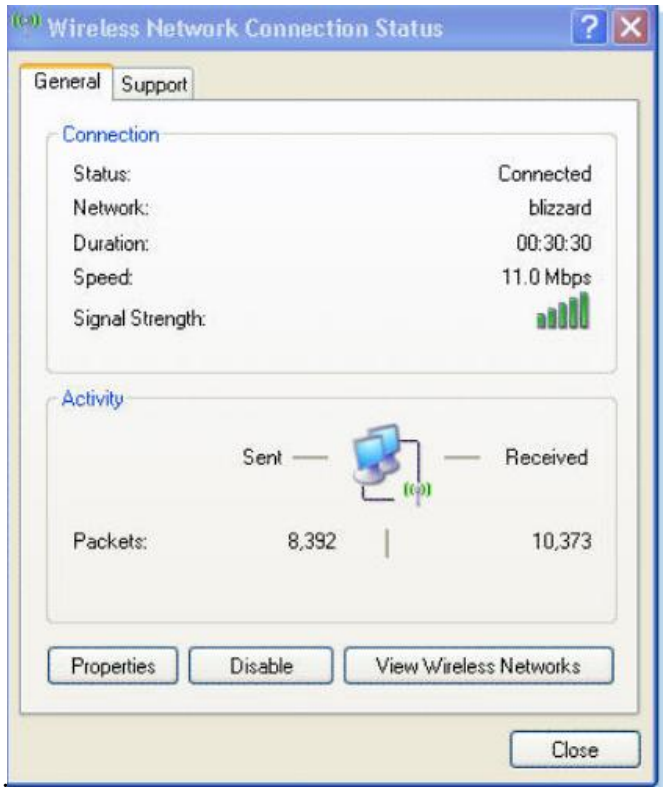
შეიძლება იყოს რთული გაიგოთ, მუშაობს თუ არა თქვენი უკაბელო კავშირი, მაშინაც კი როდესაც ვინდოუსი ამბობს, რომ თქვენ ხართ დაკავშირებული, ეს შეიძლება ნიშნავდეს მხოლოდ იმას, რომ თქვენ ხართ დაკავშირებული უკაბელო კავშირის წერტილთან, მაგრამ არა ინტერნეტთან. ყველაზე მარტივი გზა ამ კითხვაზე პასუხის მისაღებად არის ვებ ბრაუზერის გახსნა და ნახვა, შედიხართ თუ არა რომელიმე ვებ გვერდზე.

ქსელური კავშირები

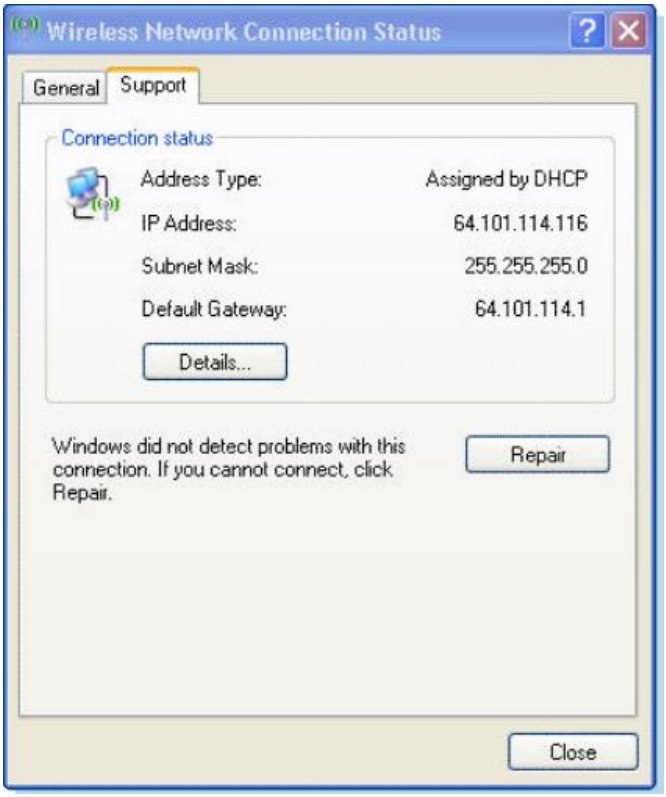
იმისთვის, რომ დაადასტუროთ უკაბელო ქსელის კავშირი ვინდოუს XP-ს გრაფიკული სამომხმარებლო ინტერფეისის გამოყენებით, შედით Start > Control Panel > Network Connections, ორჯერ დააჭირეთ უკაბელო ქსელის კავშირზე, რათა დაინახოთ მისი მდგომარეობა.



გამოვა ფანჯარა, რომელზეც იქნება ასახული გაგზავნილი და მიღებული პაკეტების რაოდენობა. პაკეტები ეს არის კომუნიკაცია ქსელურ მოწყობილობასა და კომპიუტერს შორის. ფანჯარა გვაჩვენებს, არის თუ არა კავშირი დამყარებული, და თუ არის, რამდენი ხანია, რაც არის.



იმისთვის, რომ დაინახოთ Address Type ისე, როგორც არის მოცემული ქვედა სურათზე, დააჭირეთ ტაბს **Support.** ამ ეკრანზე იხილავთ ინფორმაციას ან სტატიკური მისამართის ან დინამიურად აღებული მისამართის შესახებ, ასევე არის ნაჩვენები ქვექსელის ნიღბის და gateway-ის მისამართები, მაგრამ თუ გსურთ ნახოთ ფიზიკური მისამართი, უნდა დააჭიროთ ღილაკს Details, თუ კავშირი არასრულყოფილია, დააჭირეთ Repair ღილაკს, რათა ვინდოუსმა ცადოს თავიდან დამყარება ამ კავშირის.



ბრძანება Ipconfig ეს ბრძანება გამოიყენება IP მისამართის შესამოწმებლად ბრძანებათა ველიდან. ამ ბრძანებას აქვს შემდეგი პარამეტრები:

- /all – ყველა ქსელური ადაპტერის შესახებ სრული საკონფიგურაციო ინფორმაციის ნახვა
- /release – ქსელურ ადაპტერზე IP მისამართების მოხსნა
- /renew – განაახლებს ქსელური ადაპტერის IP მისამართს
- /flushdns – ასუფთავებს იმ მეხსიერებას, რომელშიც მოთავსებულია DNS ჩანაწერები
- /registerdns – DHCP სერვერს თავიდან სთხოვს DNS ჩანაწერს
- /displaydns – გამოაქვს ეკრანზე შენახული DNS ჩანაწერები.

ბრძანება Ping ეს ბრძანებაც ბრძანებათა ველში გამოსაყენებელია და ის არკვევს კავშირის არსებობა-არარსებობის მოწყობილობებს შორის.

შედით start>run>cmd დააჭირეთ OK-ს და შემდგომ დაბეჭდეთ Ping localhost. ასე შეამოწმებთ, მუშაობს თუ არა თქვენი ქსელური ადაპტერი. დაპინგეთ თქვენი gateway, რათა შეამოწმოთ, გაქვთ თუ არა ინტერნეტთან კავშირი. ხოლო gateway-ის მისამართის მოძიება შეგიძლიათ ბრძანებით **ipconfig**. პინგ ბრძანებაზე პასუხი გვიჩვენებს ან მობრუნებულ პაკეტებს, ან გვაუწყებს, რომ მოლოდინის რეჟიმში

ამოიწურა ის დრო, რომელიც არის საჭირო პაკეტისთვის დასაბრუნებლად, მაგრამ ის არ დაბრუნებულა.

ბრძანება Tracert

ამ ბრძანების მეშვეობით შეგვიძლია დავათვალიეროთ ის გზა, რომელსაც გაივლის მონაცემი ჩვენი კომპიუტერიდან დანიშნულების ადგილამდე. თუ სადმე გზაზე არის დაზიანება, პაკეტი ვერ მიაღწევს დანიშნულების ადგილს, თუმცა ჩვენ გავიგებთ, სად არის დაზიანება.

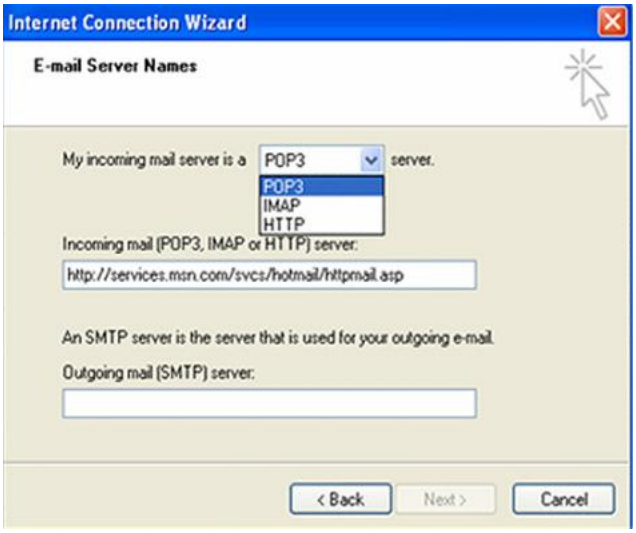
მარტივი ფოსტის სერვერის ინსტალაცია, კონფიგურაცია და მართვა

ქსელის Troubleshooting-ი (პრობლემის აღმოფხვრა)

ელექტრონული ფოსტის სისტემა იყენებს e-mail client პროგრამულ უზრუნველყოფას მომხმარებლის მოწყობილობაზე და e-mail server პროგრამულ უზრუნველყოფას ერთ ან მეტ იმეილ სერვერზე. მოხმმარებლები კითხულობენ ელექტრონულ ფოსტას სერვერებიდან ორიდან რომელიმე ერთი პროტოკოლის მეშვეობით:

- Post Office Protocol (POP)
- Internet Message Access Protocol (IMAP)

მომხმარებლები აგზავნიან ელექტრონულ ფოსტას იმეილს სერვერზე, ხოლო ის სხვა სერვერებზე გადაამისამართებს Simple Mail transfer Protocol(SMTP)-ს გამოყენებით.



თქვენ უნდა გაიგოთ, თუ როგორ უნდა დააკონფიგუროთ მომხმარებლის კომპიუტერი ისე, რომ მიიღოს სწორი ფორმატის შემომავალი ფოსტა და ამასთანავე უნდ გაიგოთ საფოსტო სერვერის აწყობის პროცესი. „საფოსტო კლიენტების“ პროგრამული უზრუნველყოფის კონფიგურირება შეიძლება დამხმარე უტილიტის (wizard) გამოყენებით, როგორც ეს ჩანს სურათზე

:

SMTP

SMTP აგზავნის ფოსტას მომხმარებლიდან სერვერისაკენ ან ერთი სერვერიდან მეორეზე. მისი მახასიათებელებია:

- მარტივი, ტექსტით მომუშავე პროტოკოლი
- იყენებს TCP-ს, პორტის ნომრით 25
- უნდა იქნეს დანერგილი, რომ გაგზავნოს ფოსტა
- ფოსტა იგზავნება იმის შემდეგ, რაც მიმღები იდენტიფიცირება და გადამოწმება.

POP

Post Office Protocol (POP) – გამოიყენება მომხმარებლის პროგრამული უზრუნველყოფის მიერ ფოსტის გადმოსაწერად სერვერიდან, მისი ყველაზე თანამედროვე ვერსია არის POP3, ეს პროტოკოლი იყენებს 110 პორტს.

IMAP

Internet Message Access Protocol (IMAP) – ის მსგავსია POP3 პროტოკოლისა, მაგრამ აქვს დამატებითი ფუნქციები. ისევე როგორც POP3, IMAP გაძლევთ საშუალებას, გადმოიწეროთ ფოსტა სერვერიდან პროგრამული უზრუნელყოფის გამოყენებით. განსხვავება არის ის, რომ IMAP უფლებას გვაძლევს ორგანიზება გავუკეთოთ ფოსტას საფოსტო სერვერზე. IMAP-ი არის უფრო სწრაფია POP3-თან შედარებით და საჭიროებს მეტ ადგილს დისკზე და მეტ დატვირთვას ახდენს პროცესორზე. IMAP-ის ყველზე თანამედროვე ვერსია არის IMAP4. IMAP4 ხშირად გამოიყენება დიდ ქსელებში, მაგ., უნივერსიტეტების ქსელებში. როგორც წესი, ის იყენებს 143 პორტს.

საფოსტო სერვერ E-mail Server საფოსტო სერვერი არის კომპიუტერი, რომელსაც შეუძლია გააგზავნოს და მიიღოს ფოსტა მომხმარებლების სახელით. ხშირად იყენებენ შემდეგ საფოსტო სერვერებს:

- Microsoft Exchange
- Sendmail
- Eudora Internet Mail Server (EIMS)

როგორც სურათიდან ჩანს, ხშირად გვხდება უტილიტები და ხელსაწყოები, რომლებიც გვეხმარებიან საფოსტო სერვერის დაყენებაში. სანამ დააყენებდეთ საფოსტო სერვერს (მაგ., Microsoft Exchange), თქვენ, პირველ რიგში, უნდა დარწმუნდეთ, რომ ქსელი პასუხობს ყველა მოთხოვნას და არის სწორად კონფიგურირებული. Active directory, global catalog და DNS სერვერები, ყველა უნდა იყოს ადვილად დასაკავშირებელი და მუშა მდგომარეობაში, სანამ შევძლებთ Exchange-ის დაყენებას და ამუშავებას. active directory სერვერ არის კომპიუტერი, რომელზეც არის განთავსებული მონაცემთა ბაზა, რომლის მეშვეობითაც ხდება ქსელში არსებული კომპიუტერების ცენტრალიზებული მართვა. global catalog სერვერი არის ცენტრალური სათავსო, რომელშიც ვინახავთ ინფორმაციას ყველა დომეინის შესახებ, რომლებიც არის ჩვენს ქსელში.

Exchange-ი უნდა დაინსტალირდეს დომეინში, რომელშიც ყველა კომპიუტერზე აყენია Windows 2000 მაინც. ის არის ცნობილი როგორც native mode. Windows NT-ს დომეინ კონტროლერს არ შეუძლია მუშაობა ასეთ გარემოში.

Active Directory-ის მონაცემთა ბაზა არის ორგანიზებული თანმიმდევრობით, რომელსაც ეწოდება schema. ერთი სერვერი, რომელზეც გვაქს გაშვებული Windows 2003 განისაზღვრება როგორც Schema Master. ეს არის ერთადერთი სერვერი, რომელსაც შეუძლია განახორციელოს ცვლილება Active Directory-ის მომხმარებლების მონაცემთა ბაზის ორგანიზაციაში. როდესაც ქსელურ ადმინისტრატორს ესაჭიროება Active

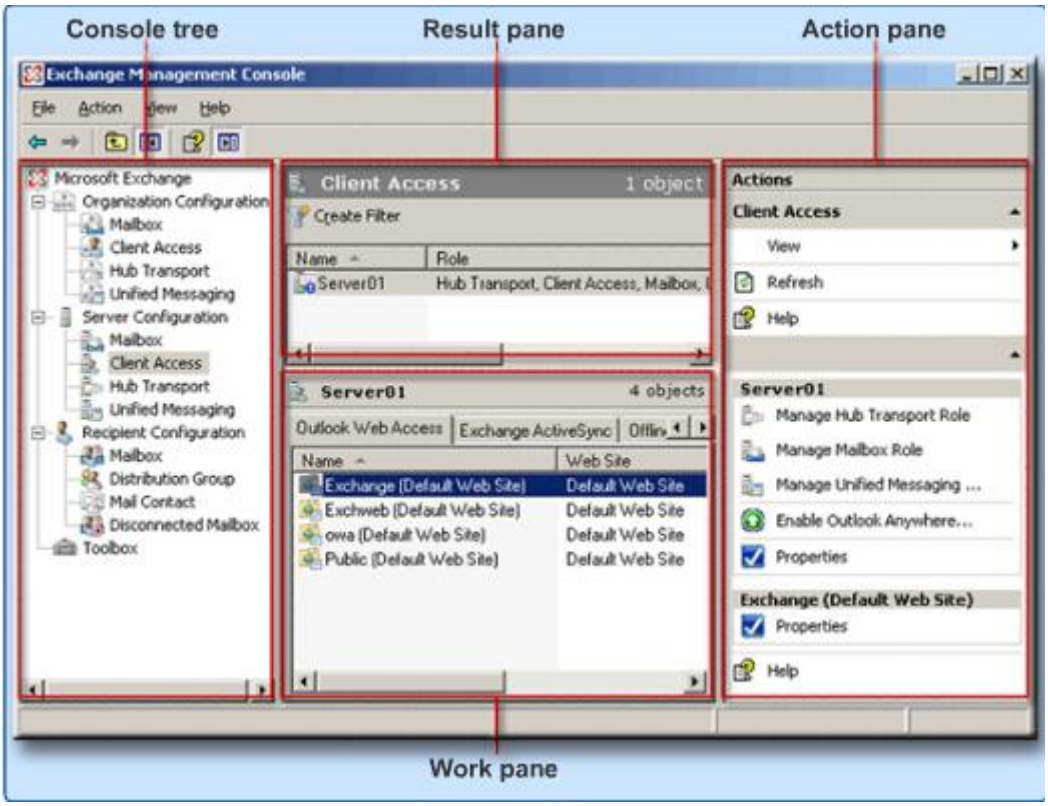
Directory-ის სტრუქტურის ცვლილება, ეს ხორციელდება Schema Master-ზე. ხოლო დანარჩენ სერვერებზე ავტომატურად კოპირდება.

საფოსტო სერვერის ისნტალაცია თქვენ უნდა შეამოწმოთ გარემო, სანამ დააინსტალირებთ Exchange-ს. იმისთვის, რომ თავიდან აირიდოთ ქსელის მწყობრიდან გამოსვლა, გამოყავით ცალკე სერვერები და მათზე დააინსტალირეთ Exchange-ი და ყველა საჭირო მომსახურება. მას შემდგომ რაც დარწმუნდებით, რომ ყველაფერი კარგად მუშაობს, შეგიძლიათ დააკავშიროთ სერვერები დანარჩენ ქსელთან.

სანამ დააინსტალირებთ Exchange-ს, მზად გქონდეთ შესაბამისი მოწყობილობები და ინფორმაცია:

- სრულყოფილად მომუშავე და საიმედო DNS სერვერი
- Active Directory-ის დომეინი
- მინიმუმ ერთი Global Catalog
- Windows 2000 ან უფრო ახალი ვერსია
- Exchange სერვერის პროგრამული უზრუნველყოფა
- Windows სერვერის უზრუნველყოფის ხელსაწყოები
- Schema master სერვერი
- მაღალი სიჩქარის შეერთება ინტერნეტთან

თქვენ იქნებით მზად დააინსტალიროთ საფოსტო სერვერი, როდესაც ყველა ზემოთ ჩამოთვლილ პირობას დააკმაყოფილებს თქვენი ქსელი. თქვენ მოგიწევთ დაამატოთ Internet Information Services (IIS), Add/Remove Windows Components უტილიტის გამოყენებით, სანამ დაიწყებდეთ ინსტალაციას. IIS-ი არის სერვერი, რომელსაც აქვს პროგრამები, რომლებიც გამოიყენება ვებგვერდების შესაქმნელად და ადმინისტრირებისათვის. მას შემდგომ, რაც IIS-ი იქნება დაინსტალირებული, Exchange-ი შეიძლება დაინსტალირდეს. ჩადეთ საინსტალაციო დისკი და დაიწყეთ ინსტალაცია.



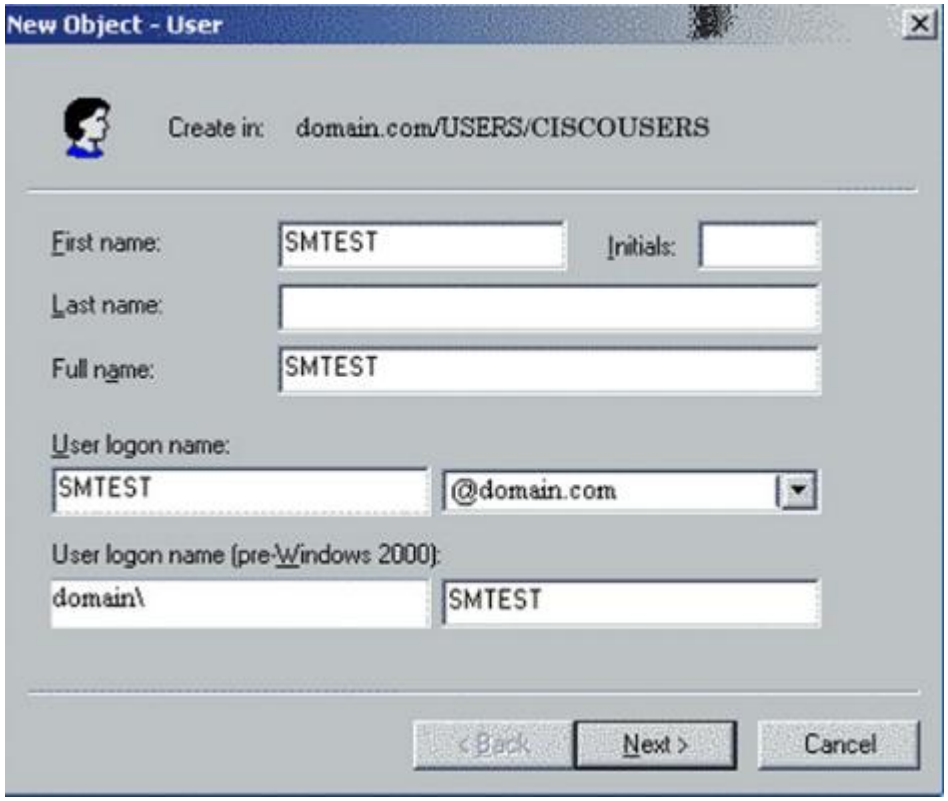
საინსტალაციო უტილიტა შეგასრულებინებთ რამდენიმე ქმედებას დასარწმუნებლად, რომ Exchange-ი მზად არის ისნტალაციისათვის. უტილიტა შეამოწმებს, არის თუ არა IIS-ი დაინსტალირებული, მუშაობენ თუ არა დომეინური სერვერები და დაინსტალირებულია თუ არა Windows-ის მხარდაჭერის ხელსაწყოები. თუ იქნება რაიმე პრობლემა, საინსტალაციო პროგრამა ამას შეგატყობინებთ. ამ შემთხვევაში გადატვირთეთ ის.

მას შემდგომ, რაც Exchange-ი დაინსტალირდება, Microsoft Management Console პლაგინი Exchange-სათვის, იხ. სურათი, მოგცემთ საშუალებას, შეცვალოთ უამრავი პარამეტრი ერთი ხელსაყრელი ადგილმდებარეობიდან. გადაამოწმეთ და დააინსტალირეთ ყველა განახლება, რომ სერვერმა სწორად იმუშაოს. Exchange System Manager, რაც აკონტროლებს Exchange-ის დანერგვას, შეიძლება იქნეს გამოყენებული სერვერის პარამეტრების მართვისათვის.

გამოიყენეთ Active Directory Users and Computer (ADUC) კონსოლი, რომ დააკონფიგურიროთ მომხმარებლის საფოსტო ყუთი. ის ასევე ცნობილია, როგორც mailbox-enabled.

გახსენით ADUC, რომ შექმნათ ახალი მომხმარებელი. მომხმარებლის სახელი და პაროლი შეიყვანეთ დომეინის უსაფრთხოების წესედების თანახმად. როგორც

სურათიდან ჩანს, მომხმარებლის საფოსტო ყუთი იქმნება მაშინ exchange სერვერის მიერ, როდესაც მომხმარებელი მიიღებს პირველ წერილს.



Exchange-ის დაყენებას სჭირდება დაგეგმვა და იმის უზრუნველყოფა, რომ სერვერები, მომსახურებები და ტექნოლოგიები, რომლებიც მას ესაჭიროება, სწორად მუშაობენ ქსელში. ზოგიერთ შემთხვევაში ინსტალაციის დროს თუ იქნა პრობლემა, შეიძლება დაგჭირდეთ ოპერაციული სისტემის გადაყენება და Exchange-ის ინსტალაციის დაწყება თავიდან.

პრევენციული დაცვა ქსელისთვის ისეთივე მნიშვნელოვანია, როგორც კომპიუტერებისათვის, რომლებიც არიან ქსელში. თქვენ უნდა შეამოწმოთ კაბელების, ქსელური მოწყობლობები, სერვერები და კომპიუტერები რომ დარწმუნდეთ, რომ ისინი არიან სუფთად და კარგ სამუშაო მდგომარეობაში.

თქვენ უნდა ჩამოაყალიბოთ გეგმა, რომლის მიხედვითაც შეამოწმებთ და გაწმენდთ ხოლმე მათ რეგულარულად. ეს დაგეხმარებათ, არ მოხდეს ქსელის მწყობრიდან გამოსვლა. ასევე გეგმის ნაწილი უნდა იყოს კაბელების შემოწმება. დარწმუნდით, რომ კაბელები სწორედ არის მარკირებული და მარკერები არ ცილდებიან. შეცვალეთ დაძველებული ან წაუკითხავი მარკერები.

როგორც ტექნიკოსმა, თქვენ შეიძლება შეამჩნიოთ, რომ მოწყობილობა გამოსცემს უჩვეულო ხმას ან გაფუჭებულია. შეატყობინეთ ეს ქსელის ადმინისტრატორს, რომ მან არ დაუშვას ქსელის მწყობრიდან გამოსვლა.

პრინტერებთან და კომპიუტერებთან არსებული კაბელები ზედმიწევნით უნდა შემოწმდეს. როდესაც კაბელები მაგიდის ქვეშაა, მათ შეიძლება ფეხიც მოხვდეს და იმოძრაონ კიდეც, ეს გამოიწვევს მათ დაგრეხას და შედეგად – გამტარუნარიანობის შემცირებას ან კავშირის დაკარგვას. თქვენ ასევე უნდა იყოთ აქტიური ქსელის მომხმარებლების განათლებაში, აჩვენეთ მათ, როგორ უნდა კაბელის სწორად გამოერთება და შეერთება და როგორ გადაიტანონ ის, თუ დასჭირდათ.

იმისთვის, რომ განახორციელოთ ქსელის troubleshooting, პირველ რიგში, იპოვეთ პრობლემის წყარო. შეამოწმეთ, მომხმარებლების ჯგუფს აქვს პრობლემა თუ მხოლოდ ერთ მომხმრებელს. თუ პრობლემა არის მხოლოდ ერთ მომხმარებელთან, მაშინ დაიწყეთ troubleshooting-ის პროცესი მისი კომპიუტერიდან.

ქსელური პრობლემები შეიძლება წარმოიქმნას პრობლემების კომბინაციიდან აპარატურულ უზრუნველყოფაში, პროგრამულ უზრუნველყოფასა და კავშირში. კომპიუტერის ტექნიკოსს უნდა შეეძლოს გააანალიზოს პრობლემა და დაადგინოს მისი მიზეზი და აღმოფხვრას ის. ამ პროცესს ეწოდება troubleshooting-ი.

პირველი ნაბიჯი ამ პროცესში არის ინფორმაციის შეგროვება მომხმარებლისაგან. იხ. შეკითხვები, რომელთა დასმაც შეიძლება მომხმარებლისათვის:

- როდის დაიწყო პრობლემა?
- რაგვარად გამოვლინდება პრობლემა?
- არის რაიმე, რისი დამატებაც შეგიძლიათ პრობლემის შესახებ?
- სხვა მომხმარებლებს თუ აქვთ ეს პრობლემა?
- რა ტიპის აპარატურას აქვს პრობლემა?
- რა შედეგები მოაქვს პრობლემას?
- აღწერეთ თქვენი სამუშაო გარემო.
- როდის მოახდინეთ უკანასკნელად კომპიუტერის სარეზერვო ასლის შენახვა?
- რა ტიპის რეზერვირება მოხდა?
- რომელი ჯგუფის წევრი ხართ?

მას შემდგომ, რაც დაელაპარაკებით მომხმარებელს, უნდა დააზუსტოთ პრობლემა:

- რა არის თვენი IP ინფორმაცია?
- ემთხვევა ქსელური აპარატურის პარამეტრები?
- არის რაიმე აქტივობა უკაბელო მარშრუტიზატორზე?
- არის რაიმე აქტივობა მოდემზე?
- არის თქვენი უკაბელო წვდომის წერტილი კონფიგურირებული სწორად?
- გათიშული ხომ არ არის ქსელთან კავშირი?

მას შემდგომ, რაც დააზუსტებთ პრობლემას, სცადე რამდენიმე სწრაფი გადაწყვეტა:

- გადატვირთეთ მოწყობილობა.
- განაახლეთ IP მისამართი.
- წაშალეთ DNS ჩანაწერები.
- აღადგინეთ დრაივერის ძველი ვერსია (Roll Back a driver).
- დაუბრუნდით უკანასკნელ შენახულ Restore Point-ს.

თუ სწრაფმა გადაწყვეტილებებმა არ გამოასწორა პრობლემა, დრო არის მოაგროვოთ ინფორმაცია კომპიუტერიდან, ამისთვის გამოიყენეთ:

- Device Manager
- Event Viewer
- ipconfig
- დაპინგეთ თქვენივე კომპიუტერი
- დაპინგეთ gateway

- დაპინგეთ ცნობილი ვებგვერდი
- გადაამოწმეთ უკაბელო მარშრუტიზატორის კონფიგურაცია
- გადაამოწმეთ „საფოსტო კლიენტის“ კონფიგურაცია

ამ მომენტისათვის თქვენ გექნებათ საკმარისი ინფორმაცია, რომ შეაფასოთ პრობლემა, გამოიკვლიოთ ის და განახორციელოთ გადაწყვეტილების დანერგვა.

- პრობლემების აღმოფხვრის გამოცდილება
- სხვა ტექნიკოსები
- ინტერნეტში ძიება
- ახალი ამბების ჯგუფები
- მწარმოებლის FAQ დოკუმენტი
- კომპიუტერის ინსტრუქცია
- მოწყობილობის ინსტრუქცია
- ონლაინ ფორუმები
- ტექნიკური ვებგვერდები

ეს ყველაფერი დაგეხმარებათ გადაწყვეტილების პოვნაში.

მას შემდგომ, რაც პრობლემა აღმოიფხვრება, შეასრულეთ შემდეგი:

- მომხმარებელთან განიხილეთ გადაწყვეტილება, რომელიც განახორციელეთ.
- სთხოვეთ მომხმარებელს დაადასტუროს, რომ პრობლემა აღმოიფხვრა.
- მიაწოდეთ კლიენტს ყველა საჭირო დოკუმენტი.
- აღწერეთ, რა ნაბიჯები გადადგით პრობლემის აღმოსაფხვრელად შეკვეთის ფორმაშიც და ტექნიკოსის ჯურნალშიც.
- ჩამოწერეთ ყველა კომპონენტი, რომლების გამოყენებაც მოხდა პრობლემის აღმოფხვრის დროს.
- აღნიშნეთ რა დრო დაგჭირდათ პრობლემის აღმოსაფხვრელად.

ქსელური პრობლემები შეიძლება იყვნენ დაკავშირებულნი აპარატურასთან, პროგრამულ უზრუნველყოფასთან, ქსელთან ან სამივეს კომბინაციასთან, თქვენ მოგიწევთ ზოგიერთი ტიპის პრობლემის უფრო ხშირად აღმოფხვრა სხვებთან შედარებით. იხილეთ ხშირი პრობლემების და მათი გადაწყვეტების სია:

- მოხმმარებლები გატყობინებენ, რომ ქსელური პრინტერის საიმედოობა საეჭვო გახდა, ქსელის კაბელი გაჭიმული მაგიდის ქვეშ და ის გაცვდა ან დაზიანდა. გადაწყვეტა – თავიდან გაიყვანეთ ახალი კაბელი პრინტერამდე.
- მომხმარებლის კომპიუტერი რამდენიმე საათის მანძილზე იყო ჩართული თუმცა Connection Status-ში, მხოლო რამდენიმე პაკეტი არის გაგზავნილი და მიღებული.

უკაბელო ქსელის კავშირი ვერ შედგა. გადაწყვეტა – გადატვირთეთ ქსელური ადაპტერი და განაახლეთ IP მისამართი Repair ღილაკის მეშვეობით.

- მოხმარებელი ახდენს უამრავ ცვლილებას WRTN300 უკაბელო მარშრუტიზატორში, მაგრამ რატომღაც ცვლილებები არ მოქმედებენ. მოხმარებელს ავიწყდება Save Settings ღილაკის დაჭერა ყოველ ტაბზე ცვლილებების განხორციელების შემდგომ.
- მომხმარებელი იღებს გაფრთხილებას იმის შესახებ, რომ მყარ დისკზე არის ძალიან ცოტა ადგილი. დაადგინეთ, ეს პრობლემა ხომ არ არის გამოწვეული დროებითი ფაილების საქაღალდით, რომელშიც ბრაუზერი ინახავს ინფორმაციას. თუ ასეა, გამოიყენეთ დისკი გამწმენდი უტილიტა ან თუნდაც ხელით წაშალეთ ეს ფაილები.
- ქსელის სიჩქარემ იკლო ახალი მომხმარებლების დამატების გამო. ყველა მომხმარებელი შეერთებულია 24-პორტიან კონცენტრატორში. გადაწყვეტა – გამოცვალეთ კონცეტრატორი კომუტატორითურთ.

უსაფრთხოების საჭირო დონის დადგენა, უსაფრთხოების წესების შემუშავება

აღწერეთ, როდის და რისთვის უნდა გამოვიყენოთ „უსაფრთხოების აპარატურა“ და უსაფრთხოების პროგრამული უზრუნველყოფა

ორგანიზაცია უნდა ცდილობდეს მიაღწიოს საუკეთესო უსაფრთხოებას რაც შეიძლება მისაღებ ფასად. ქსელურმა ტექნიკოსებმა და ორგანიზაციის მმართველობამ ერთად უნდა იმუშაონ უსაფრთხოების წესედების შექმნაზე, რომ დაიცვას მონაცემები და აპარატურა ყველა შესაძლო საფრთხისგან. უსაფრთხოების წესდება შეიცავს დაწვრილებით ინფორმაციას იმის შესახებ, თუ რა დონის უსაფრთხოება არის საჭირო და როგორ უნდა მოხდეს მისი მიღწევა.

თქვენ შეიძლება მიიღოთ მონაწილეობა უსაფრთხოების წესდების შექმნაში კლინეტისათვის ან ორგანიზაციისათვის. როდესაც ქმნით უსაფრთხოების წესდებას, დასვით შემდეგი შეკითხვები, რომ მიიღოთ წარმოდგენა უსაფრთხოების ფაქტორების შესახებ:

სად არის კომპიუტერი განთავსებული, ბინაში თუ კომპანიაში?

- კომპიუტერებისათვის ბინებში დიდია საფრთხე უკაბელო ტექნოლოგიის გამოყენებით არასანქცირებული შეღწევისა, ხოლო კომპანიებში პრობლემა დგას ქსელში არასანქცირებული შეღწევისა, იმის გამო, რომ ზოგი მომხმარებელი ბოროტად იყენებს ქსელში შეღწევის თავის პრივილეგიას.

- არის თუ არა მუდმივი ინტერნეტთან კავშირი?
- რაც უფრო დიდხანს არის კომპიუტერი ჩართული ინტერნეტში, მით უფრო დიდია საფრთხე მასზე თავდასხმებისა. კომპიუტერს, რომელსაც აქვს კავშირი ინტერნეტთან, უნდა ჰქონდეს ანტივირუსი და firewall-ი
- კომპიუტერი პორტატული ხომ არ არის? მათი ფიზიკური უსაფრთხოება მნიშვნელოვანია. არსებობენ საშუალებები მათი უსაფრთხოებისთვის, მაგ., cable lock იხ. სურათი.

უსაფრთხოების წესდება არის უსაფრთხოების წესების, ქმედებების და შესამოწმებელი ობიექტების ერთობლიობა. ის შეიცავს შემდეგს:

- აღწერს კომპიუტერის გამოყენების მიუღებელ საქმიანობას.
- საზღვრავს, ვისა აქვს ორგანიზაციაში უფლება გამოიყენოს კომპიუტერი
- საზღვრავს, რომელი მოწყობილობები და როგორ შეიძლება დაყენდეს ქსელში, მაგ., მოდემებს და უკაბელო კავშირის წერტილებს შეუძლიათ თავდასხმის საფრთხე შეუქმნან ქსელს.
- საზღვრავს მონაცემების კონფიდენციალობის შენარჩუნებისთვის საჭირო მოთხოვნებს.
- საზღვარავს პროცესს, რომლის მიხედვითაც უნდა მიიღონ თანამშრომლებმა უფლება მოწყობილობებსა ან მონაცემებზე. ამ პროცესში შეიძლება იყოს საჭიროება, თანამშრომელმა მოაწეროს ხელი შეთანხმება, ორგანიზაციის წესების შესახებ და მასშივე უნდა იყოს აღწერილი, რა მოხდება წესებისადმი დაუმორჩილებლობის შემთხვევაში.

უსაფრთხოების წესდებაში ასევე უნდა იყოს გაწერილი დეტალური ინფორმაცია იმის შესახებ, თუ რა ქმედებები უნდა განხორციელდეს, თუ მოხდა მოულოდნელი შემთხვევა:

- ქმედებები, რომლებიც უნდა შესრულდეს უსაფრთხოების წესების დარღვევის შემთხვევაში.
- ვისთან მოხდეს დაკავშირება მოულოდნელი შემთხვევების დროს
- ინფორმაცია, რომლის გაზიარებაც დასაშვებია კლიენტებთან, პრესასთან და ა.შ.
- მეორადი ადგილმდებარეობების გამოყენება ევაკუაციის შემთხვევაში.

- ქმედებები, რომლებიც უნდა განხოციელდეს მას შემდეგ, რაც მოულოდნელი შემთხვევა დასრულდება, ეს შეიცავს პრიორიტეტს მომსახურებებისაც, რომლებიც უნდა აღდგეს.

შენიშვნა: უსაფრთხოების წესდება უნდა იქნას დაცული ყველა თანამშრომლის მიერ, რომ ჰქონდეს ეფექტი.

უსაფრთხოების წესდება უნდა საზღვრავდეს აპარატურულ უზრუნველყოფას და მოწყობილობებს, რომელთა გამოყენებაც შეიძლება ქურდობის, ვანდალიზმის და მონაცემთა დაკარგვის არდასაშვებად.

დაიცავით ტერიტორია:

- ღობეებით
- უსაფრთხოების აპარატურული უზრუნველყოფით

დაიცავით ქსელური ინფრასტრუქტურა: კაბელები, სატელეკომუნიკაციო მოწყობილობები და ქსელური მოწყობილობები:

- უსაფრთხო კავშირგაბმულობის ოთახი
- არასანქცირებული კავშირის უკაბელო წერტილების აღმომჩენი
- აპარატურული firewall-ები
- ქსელის მართვის სისტემა, რომელიც აღმოაჩენს ცვლილებებს კაბელურ გაყვანილობასა და პატჩ პანელში.

დაცავით ინდივიდუალური კომპიუტერები, ამ ჩამონათვალის გამოყენებით:

- Cable lock-ები
- პორტატული კომპიუტერის docking station lock-ები
- საკეტებიანი ქეისები
- უსაფრთხო კაბინები დესკტოპების ქეისების ჩასადგმელად.

დაიცავით მონაცემები აპარატურის მეშვეობით, რომელიც არ იძლევა არასანქცირებული კავშირის საშუალებას ან შემნახველი მოწყობილობის ქურდობას:

- საკეტიანი მყარი დისკის მზიდი
- უსაფრთხო საცავი და სარეზერვო ასლების გადასატანი საშუალება
- USB მეხსიერების უსაფრთხო dongle-ები (ანუ კორპუსები)

სწორი უსაფრთხოების ნარევი

ფაქტორები, რომლებიც განსაზღვრავენ ყველაზე ეფექტურ უსაფრთხოების საშუალებებს, რომლითაც უნდა დავიცვათ ჩვენი აპარატურა და მონაცემები, შემდეგია:

- როგორ მოხდება აპარატურის გამოყენება
- სად არის განთავსებული კომპიუტერული აპარატურა
- მომხმარებელს რა სახის კავშირი სჭირდება მონაცემებთან

მაგ., კომპიუტერი გადატვირთულ საჯარო ადგილას, როგორიც არის ბიბლიოთეკა, საჭიროებს დამატებითი დაცვის საშუალებებს.

საჯარო ადგილას სადაც საჭიროა ნოუთბუქის გამოყენება, უსაფრთხოების dongle შეგვიძლია გამოვიყენოთ. ის უზრუნველყოფს უსაფრთხოებას იმით, რომ დაბლოკავს სისტემას, თუ ნოუთბუქი და მომხმარებელი ერთმანეთს განცალკევდებიან.

უსაფრთხოების პროგრამები იცავენ ოპერაციულ სისტემას და პროგრამული უზრუნველყოფის მონაცემებს.

ჩამონათვალში შეგიძლიათ იხილოთ პროდუქტები და პროგრები, რომელთა გამოყენებაც შეიძლება ქსელური მოწყობილობების დასაცავად:

- პროგრამული Firewall – ფილტრავს შემომავალ ინფორმაციას და ჩაშენებულია Windows XP-ში
- Intrusion Detection Systems (IDS) – არასანქცირებული კავშირის აღმომჩენი სისტემა თვალს ადევნებს და გვატყობინებს ცვლილებებს, რომლებიც განხოციელდა პროგრამულ კოდში ან უჩვეულო ქსელურ აქტივობას.
- პროგრამების და ოპერაციული სისტემების Patche-ები – ახლად აღმოჩენილ უსაფრთხოების სისუსტეებს აღმოფხვრის პროგრამებში ან ოპერაციულ სისტემებში.

არსებობს რამდენიმე ტიპის პროგრამული უზრუნველყოფა, რომლებიც იცავს კომპიუტერებს არასანქცირებული მავნე კომპიუტერული კოდისაგან:

- ვირუსებისაგან დაცვა
- Spyware პროგრამებისაგან დაცვა
- Adware პროგრამებისაგან დაცვა
- Grayware პროგრამებისაგან დაცვა

როგორც წესი, პატარა ოფისებსა და ბინებში კომპიუტერები პირდაპირ არიან შეერთებულები ინტერნეტთან და არ გადიან დაცულ ლოკალურ ქსელში, რომელიც მათ ორგანიზებას მოახდენდა. ეს მათ უფრო მეტ საფრთხეს უქმნის, და როგორც მინიმუმ, მათ უნდა ჰქონდეთ ანტივირუსული და ანტი-malware პროგრამული უზრუნველყოფა უახლესი განახლებებით. პროგრამული firewall-იც შეიძლება იყოს გადაწყვეტის ნაწილი,

რა თქმა უნდა, ოპერაციულ სისტემას და სხვა პროგრამებსაც უნდა ჰქონდეთ დაყენებული უახლესი Patche-ები.

უსაფრთხოების წესდება უნდა საზღრავდეს, რა რაოდენობით უსაფრთხოების პროგრამები იყოს გამოყენებული. თოთეული ნაბიჯი, რომელიც ზრდის უსაფრთხოებას, ზრდის ფასსაც, წესდების შემუშავების პროცესში ორგანიზაციის მმართველებმა უნდა დაითვალონ, რა დაუჯდებათ მონაცემების დანაკარგი და მისი დაცვა და გადაწყვიტონ, რა თანხის დახარჯვა არის მიზანშეწონილი.

უსაფრთხოების კომპონენტების არჩევა კლიენტის საჭიროების safuZvelze, უსაფრთხოების ხერხები. kavSiris კონტროლის მექანიზმები, Firewall-ის ტიპები

უსაფრთხოების წესდება ეხმარება კლიენტებს კომპონენტების არჩევაში, რომლებიც ესაჭიროებათ აპარატურის და მონაცემების უსაფრთხოებისათვის. თუ არ არის უსაფრთხოების წესდება, უნდა განიხილოთ საფრთხეები კლიენტთან ერთად.

გამოიყენეთ თქვენი გამოცდილება და გამოიკვლიეთ უსაფრთხოების საშუალებები ბაზარზე. როდესაც ირჩევთ მათ, გახსოვდეთ, კლიენტისათვის ყველაზე მნიშვნელოვანია მისი საჭიროებების დაკმაყოფილება.

პაროლები Passwords
უსაფრხო დაშიფრული აუტენტიფიცირების ინფორმაციის გამოყენება უნდა იყოს მინიმალური მოთხოვნა ყველა ქსელში ჩართული კომპიუტერისათვის ნებისმიერ ორგანიზაციაში. ზოგიერთი ტიპის მავნე პროგრამული უზრუნველყოფა ადევნებს თვალყურს იმ მონაცემებს, რომლებიც მოგზაურობენ ქსელში და თუ პაროლი არ იქნება დაშიფრული, ის პირდაპირ გაიგებს პაროლს. ხოლო დაშიფრული პაროლის შემთხვევაში, მისი გაშიფვრა დასჭირდება.

ჩანაწერები და აუდიტი მოვლენების ჩაწერა/დამახსოვრება და აუდიტი უნდა იყოს ჩართული, რომ შევძლოთ ქსელში აქტივობის მონიტორინგი. ქსელის ადმინსტრატორი აუდიტს ატარებს ფაილისა, რომელშიც ინახება ეს ინფორმაცია, რომ გამოიკვლიოს არასანქცირებული კავშირი ქსელში.

უკაბელო ქსელების კონფიგურაციები უკაბელო კავშირები განსაკუთრებულად ადვილად მისაწვდომია თავდამსხმელებისთვის. შესაბამისად, კონფიგურაციაში მონაცემების შიფრაცია უნდა გვქონდეს ჩართული.

შიფრაცია Encryption დაშიფვრის ტექნოლოგიები გმაოიყენება ქსელზე მოგზაური მონაცემების კოდირებისათვის. თითოეული ტექნოლოგია გამოიყენება განსხვავებული მიზნისათვის:

- Hash-ის კოდირება – ანუ hashing უზრუნველყოფს მესიჯების მთლიანობას/დაუზიანებლობას მათი გადაცემის დროს. ეს პროცესი იყენებს მათემატიკურ ფუნქციას, რომ მონაცემებიდან გამომდინარე მიიღოს უნიკალური იდენტიფიკატორი. და მონაცემში ერთი სიმბოლოს შეცვლის შემთხვევაშიც კი იდენტიფიკატორი შეიცვლება. თუმცა ფუნქცია ცალმხრივია და ამის გამო რთულია მონაცემის დაჭერა და შეცვლა. ყველაზე ცნობილი ალგორითმების სახელებია SHA და MD5.
- სიმეტრიული შიფრაცია – ამ მეთოდის დროს ორივე მხარეს უნდა ჰქონდეს გასაღები დაშიფვრისას და გაშიფვრისათვის, რომ მოხდეს წარმატებული კომუნიკაცია. გადამცემი და მიმღები უნდა იყენებდეს იდენტურ გასაღებებს.
- ასიმეტრიული შიფრაცია – ამ დროს გვაქს ორი ტიპის გასაღები, საჯარო და დახურული. იმისთვის, რომ დავშიფროთ და გადავაგზავნოთ მონაცემები, საკმარისია საჯარო გასაღების ცოდნა, მაგრამ დახურული გასაღების გარეშე ამ მონაცემების გაშიფვრა შეუძლებელია. ამ სისტემის დადებითი მხარე არის ის, რომ მხოლოდ ერთი გასაღების საიდუმლოდ შენახვა არის საჭირო, ხოლო საჯარო გასაღებები შეიძლება ელექტრონული ფოსტითაც კი დაიგზავნოს.
- Virtual private network (VPN) – ქსელის ეს ტიპი იყენებს შიფრაციას მონაცემების დასაცავად ისე, თითქოს ისინი მოგზაურობენ კორპორატიულ ლოკალურ ქსელში, ხოლო ამ დროს შეიძლება ისინი იყენებდნენ ინტერნეტს. უსაფრთხო კავშირს, რომელიც ყალიბდება ორ წერტილს შორის, უწოდებენ „უსაფრთხო ტუნელს“.

კომპიუტერული აპარატურა და მონაცემები შეიძლება დავიცვათ უსაფრთხოების მეთოდებით, რომლებიც ნაწილობრივ ემთხვევიან ერთმანეთს, ამის მაგალითი არის ორი სხვადასხვა მეთოდის გამოყენება ერთი აქტივის დასაცავად. ეს არის ცნობილი როგორც ორ-ფაქტორიანი დაცვა. როდესაც ვფიქრობთ უსაფრხოებაზე, უნდა გავითვალისწინოთ დანერგვის ფასი და დასაცავი რესურსების ღირებულება.

ფიზიკური უსაფრთხოება Physical Security

გამოიყენეთ უსაფრთხოების აპარატურა, რომ აღკვეთოთ, უსაფრთხოების დარღვევები, მონაცემების ან მოწყობილობების დანაკარგი. ფიზიკური უსაფრთხოების კონტროლში შედის შემდეგი:

- საკეტი – ყველაზე გავრცელებული მოწყობილობა, რომელიც გამოიყენება ფიზიკური სივრცის უსაფრთხოებისათვის. თუ გასაღები დაიკარგა, ყველა იდენტური საკეტი უნდა გამოიცვალოს
- საიზოლაციო მილი – რომელიც იცავს ჩვენი გამტარის ინფრასტრუქტურას დაზიანებისაგან და არასანქცირებული კავშირისაგან
- კარტა გასაღები – ხელსაწყო, რომელიც შეგვიძლია გამოვიყენოთ ფიზიკური სივრცის უსაფრთხოებისათვის, თუ ის დაიკარგება, მხოლოდ ერთი ცალის

დაბლოკვა იქნება საჭირო. ეს სისტემა უფრო ძვირია ჩვეულებრივი გასაღების საკეტთან შედარებით

- ვიდეო აპარატურა – იწერს სურათებს და ხმას მონიტორინგის განსახორციელებლად
- დარაჯი – აკონტროლებს შენობაში შესვლა-გამოსცლას და შენობის შიგნით ქმედებებს

ქსელური აპარატურა უნდა იდგეს უსაფრთხო ოთახებში. ყველა კაბელი უნდა იყოს მოთავსებული საიზოლაციო მილში ან იყოს განთავსებული კედლის შიგნით, რათა აღიკვეთოს არასანქცირებული კავშირის მცდელობები. ქსელური აუტელეტები, რომლებიც არ გამოიყენებიან, უნდა იყვნენ გათიშული. თუ ქსელური მოწყობილობები დაზიანდნენ ან მოპარულ იქნენ, ქსელის ზოგიერთ მომხმარებელს შეიძლება ეთქვას უარი მომსახურებაზე.

უსაფრთხოების წესდება უნდა კარნახობდეს, უსაფრთხოების რა დონე არის საჭირო ორგანიზაციაში. ბიომეტრიული მოწყობილობები, მოწყობილობები, რომლებიც ზომავენ ფიზიკურ მაჩვენებლებს მომხმარებლისა, და მისი მეშვეობით ახდენენ აუტენტიფიცირებას, არის იდეალური ისეთი ადგილებისთვის, სადაც გვესაჭიროება მაღალი დონის უსაფრთხოება. თუმცა უმეტეს პატარა ორგანიზაციაში ასეთი ტიპის გადაწყვეტა იქნებოდა ძალიან ძვირი.

მონაცემთა უსაფრთხოება იმისთვის, რომ დაიცვათ მონაცემები, შეგიძლიათ გამოიყენოთ მონაცემთა დაცვის მოწყობილობები, რომლებიც ახდენენ თანამშრომელთა აუტენტიფიცირებას. ორ ფაქტორიანი იდენტიფიკაცია არის უსაფრთხოების გაზრდის მეთოდი. მომხმარებელმა უნდა გამოიყენოს ორივე – პაროლიც და მონაცემთა უსაფრთხოების მოწყობილობაც:

- Smart card – მოწყობილობა, რომელსაც შეუძლია უსაფრთხოდ შეინახოს მონაცემები. შიგა მეხსიერება იჩიპზეა ნტეგრირებული (ICC), რომელიც უკავშირდება წამკითხველს ან პირდაპირ, ან უკაბელო კავშირის მეშვეობით. ეს მოწყობილობები ძალიან ბევრი დანიშნულებით გამოიყენებიან დღეს მსოფლიოში: როგორც უსაფრთხო მაიდენტიფიცირებელი ნიშნები, ონლაინ აუტენტიფიცირების მეთოდები და უსაფრთხო საკრედიტო ბარათის გადახდებისათვის.
- Security key fob – ეს პატარა მოწყობილობა გარეგნულად წააგავს ორნამენტს გასაღებების რგოლზე. მას აქვს პატარა რადიოსისტემა, რომელიც კომუნიკაციას ამყარებს კომპიუტერთან ახლო მანძილიდან. კომპიუტერმა ჯერ მისგან უნდა მიიღოს სიგნალი, რომ აღიქვას მომხმარებლის სახელი და პაროლი.
- ბიომეტრიული მოწყობილობები – აღიქვამს მომხმარებლის ფიზიკურ მახასიათებლებს, მაგ., თითის ანაბეჭდს, მომხმარებელი იღებს კავშირის უფლებას, თუ ეს მახასიათებლები, აგრეთვე სახელი და პაროლი დაემთხვა.

აპარატურული და პროგრამული firewall-ები იცავენ მონაცემებს და აპარატურას ქსელში არასანქცირებული კავშირისაგან. firewall უნდა იყოს დანამატი უკვე არსებული უსაფრთხოების პროგრამული უზრუნველყოფისა.

უსაფრთხოების და პროგრამული უზრუნველყოფის firewall-ს აქვს ქსელში მონაცემების ფილტრაციის რამდენიმე რეჟიმი:

- პაკეტების ფილტრაცია – წესების ერთობლიობა, რომელიც ნებას რთავს ტრაფიკს ისეთი კრიტერიუმიდან გამომდინარე, როგორიც არის IP მისამართი, პროტოკოლები, ან გამოყენებადი პორტის ნომერი.

- Proxy firewall – firewall, რომელიც იძიებს მთელ ტრაფიკს და ნებას რთავს ან კრძალავს პაკეტებს, კონფიგურირებული წესების შესაბამისად. ის მოქმედებს ქსელში როგორც gateway და იცავს ჩვენი ქსელის შიგნით მყოფ კომპიუტერებს.
- Stateful packet inspection – ეს firewall იმახსოვრებს ქსელში არსებული კავშირების მდგომარეობას და თუ პაკეტი არ არის ცნობილი კავშირის ნაწილი, ის კრძალავს მას.

აპარატურული Firewall-ები ეს არის ფილტრაციის ფიზიკური კომპონენტი, რომელიც იკვლევს მონაცემთა პაკეტებს ქსელიდან, სანამ ისინი მიაღწევენ კომპიუტერებს ან სხვა მოწყობილობებს ქსელში. აპარატურული firewall-ები ხშირად ყენდება მარშრუტიზატორეზე. ის არ იყენებს კომპიუტერების გამოთვილით სიმძლავრეს და, შესაბამისად, არ ტვირთავს კომპიუტერებს არანაირად.

პროგრამული Firewall-ები ეს არის კომპიუტერული პროგრამა, რომელიც იკვლევს და ფილტრავს მონაცემთა პაკეტებს. Windows Firewall არის მაგალითი ასეთი პროგრამის, ის მოყვება ვინდოუსის ოპერაციულ სისტემას. პროგრამული Firewall-ები იყენებენ კომპიუტერის რესურსებს, რაც იწვევს კომპიუტერის წარმადობის შემცირებას. შენიშვნა: უსაფრთხო ქსელში, თუ კომპიუტერის წარმადობა არ არის პრობლემა, უნდა ჩართოთ ოპერაციული სისტემის შიგნით არსებული Firewall-ი დამატებითი უსაფრთხოებისათვის. ზოგიერთმა პროგრამამ შეიძლება ვერ იმუშაოს ნორმალურად, თუ Firewall-ი არ არის მისთვის დაკონფიგურირებული.

უსაფრთხოების პარამეტრების არჩევა, firewall-ის ტიპების კონფიგურაცია და მავნე პროგრამული უზრუნველყოფისგან დაცვა

პრევენციული ქმედებები, ოპერაციული სისტემის განახლებები, განხსვავებული პრივილეგიების მქონე მომხმარებლები, მონაცემთა რეზერვირების პროცედურები

ორი ხშირი უსაფრთხოები შეცდომა არის არასწორი მინიჭებული უფლებები საქაღალდეებზე და ფაილებზე, და არასწორად დაკონფიგურირებული უკაბელო ქსელის უსაფრთხოება.

უფლებების დონეები საქაღალდეებისათვის და ფაილებისათვის

ეს უფლებები კონფიგურირდება, რომ შეიზღუდოს ინდივიდუალური ან ჯგუფური კავშირის უფლებები კონკრეტულ მონაცემზე. ორივე, FAT-იც და NTFS-იც, იძლევა საშუალებას მივანიჭოთ მომხმარებლებს, რომლებსაც აქვთ ქსელთან კავშირი, უფლება კონკრეტულ საქაღალდეზე. ხოლო ფაილებისადმი უფლებების კონფიგურირება ხდება მხოლოდ NTFS-ში.

- Read – დათვალიერება ფაილების და საქაღალდეში ქვესაქაღალდეების, საქაღალდის მფლობელის და მისი ატრიბუტების ნახვა.
- Write – ზემოთ ჩამოთვლილი უფლებები და ახალი ფაილებისა და საქაღალდეების შექმნის უფლება, საქაღალდეების ატრიბუტების შეცვლა.
- List Folder Contents – ფაილებისა და ქვესაქაღალდეების სახელების სიის დათვალიერების უფლება.
- Read and Execute – საქაღალდეებსა და ფაილებს შორის გადასვლა იმ შემთხვევაშიც კი, თუ მომხმარებელს არ აქვს იმ საქაღალდეებზე წვდომა და ასრულებენ მხოლოდ Read და List Folder Contents უფლებებს.
- Modify – საქაღალდის წაშლა, მოდიფიცირება.

უკაბელო ქსელის უსაფრთხოების კონფიგურაცია

- Wired Equivalent Privacy (WEP) – შიფრავს მონაცემებს, რომლებიც მოგზაურობენ კავშირის წერტილსა და კომპიუტერს შორის, ის იყენებს 64- ან 128-ბიტიან გასაღებს. იხილეთ სურათი.

- Wi-Fi Protected Access (WPA) –უკეთეს შიფრაციას და აუტენტიფიკაციას გვთავაზობს WEP-თან შედარებით.
- MAC address filtering – ფიზიკური მისამართების მიხედვით კავშირის შეზღუდვა. ეს მეთოდი მარტო (დამოუკიდებლად) არ უნდა გამოიყენებოდეს, ის მხოლოდ დანამატია.

- Service Set Identifier (SSID) Broadcasting – უკაბელო ქსელის SSID-I არის იდენტიფიკატორი, რომელსაც ფართოდმაუწყებლობს ჩვენი წვდომის წერტილი, მისი მაუწყებლობის გათიშვა იწვევს ჩვენი ქსელის „გაუჩინარებას“ (დამალვას), თუმცა ეს არ არის სანდო ხერხი უკაბელო ქსელის უსაფრთხოებისა.
- უკაბელო ქსელის ანტენა – ანტენის ტიპი განსაზღრავს ჩვენი ქსელის მუშაობის ხარისხს და ამავდროულად ის შეიძლება თავად იყოს საფრთხის შემცველიც. ეს ანტენნა ისე უნდა დააყენოთ, რომ მისი სიგნალი არ გადიოდეს თქვენი ქსელის ფიზიკურ საზღვარს მიღმა.

firewall-ი კომპიუტერთან ან ქსელურ სეგმენტთან ან დაკავშირების ნებას იძლევა, ან კრძალავს მას. როგორც წესი, ის პორტების გახსნით და დაკეტვითმუშაობს, მხოლოდ საჭირო პორტების გახსნით firewall-ზე, თქვენ აყენებთ მკაცრ პოლიტიკას. განსხვავებული ვარიანტი იქნებოდა, თუ დაკეტავდით მხოლოდ რამდენიმე პორტს და დანარჩენს დატოვებდით ღიად. ეს მეთოდი ნაკლებად უსაფრთხოა. ერთ დროს პროგრამული და აპარატურული უზერუნველყოფა გამოდიოდა ისე. რომ მათი ყველა პარამეტრი იყო მეორე ხერხით დაყენებული. ხოლო იმის გამო. რომ უამრავი მომხმრებელი არ ახდენდა თავისი მოწყობილობის კონფიგურირებას, ისინი აღმოჩნდნენ ნაკლებად დაცულნი. უმეტესობა მოწყობილობა ამჟამად რაც შეიძლება მეტი აკრძალვის პარამეტრით გამოდის, თუმცა მათი კონფიგურაცია მაინც მარტივია.

პროგრამული Firewall-ი

როგორც წესი, ასეთი Firewall-ი არსებობს პროგრამების სახით, რომლებიც გაშვებულნი არიან დასაცავ კომპიუტერზე. Windows XP-ში არის ჩაშენებული პროგრამული Firewall (იხილეთ სურათი).

მისი კონფიგურაცია ორი ხერხით შეიძლება:

- ავტომატურად – პროგრამა ეკითხება ხოლმე მომხმრებელს, რა ქნას ამა თუ იმ შემთხვევაში და მომხმარებელს კი აქვს პასუხის არჩევანი: Keep Blocking (გააგრძელე ბლოკირება), Unblock (დართე ნება) ან Ask Me Later (მოგვიანებით მკითხე).

- Manage Security Settings – მომხმარებელი ხელით ამატებს იმ პორტებს, რომლებიც პროგრამებს ესაჭიროება სამუშაოდ.

პროგრამის დასამატებლად: Start > Control Panel > Security Center > Windows Firewall > Exceptions > Add Program

პროგრამის ამოშლისათვის: Start > Control Panel > Security Center > Windows Firewall

Malware არის სახიფათო პროგრამული უზრუნველყოფა, რომელიც ყენდება კომპიუტერზე მომხმარებლის ნებართვის ან ცოდნის გარეშე. მისი ზოგიერთი სახეობა აგროვებს ინფორმაციას და შემდგომ უგზავნის თავდამსხმელს.

თქვენ უდნა გქონდეს ვირუსების და spyware-ის დასასკანირებელი პროგრამები იმისთვის, რომ აღმოაჩინოთ და წაშალოთ ეს მავნე პროგრამები. ზოგიერთ თანამედროვე ბრაუზერს კი მოყვება ხელსაწყოები მათ დასაბლოკად. მავნე პროგრამების წასაშლელად შეიძლება დაგჭირდეთ რამდენიმე სხვადასხვა პროგრამა:

- **ვირუსებისაგან დაცვა** – ანტივირსები, როგორც წესი, ავტომატურად არიან ჩართულნი, ისე მუშაობენ, ჩვენ ხელს არ გვიშლიან, და მონიტორინგს ატარებენნ ხოლო როდესაც ვირუსი იქნება ნაპოვნი, პროგრამა აფრთხილებს მომხმრებელს და ცდილობს ვირუსის კარანტინში მოქცევას ან წაშლას.
- **Spyware-ისგან დაცვა** – Anti-spyware პროგრამები ეძებენ keylogger-ებს და სხვა მავნე პროგრამებს
- **Adware-ისგან დაცვა** – Anti-adware პროგრამები ეძებენ პროგრამებს, რომლებიც გვაჩვენებენ არასასურველ რეკლამებს
- **Phishing-ისგან დაცვა** – Anti-phishing პროგრამები ბლოკავენ ცნობილი phishing ვებ გვერდე IP მისამართებს და აფრთხილებენ მომხმარებელს, რომ ვებგვერდი, რომელზეც ის შევიდა, არის საეჭვო

- რამდენიმე ქმედება შეგვიძლია განვახორციელოთ იმისთვის, რომ დავრწმუნდეთ უსაფრთხოების ეფექტურობაში.

ოპერაციული სისტემა არის ყველაზე ხშირი თავდასხმის ობიექტი, რადგანაც მისი კონტროლით თავდამსხმელი მთელ კომპიუტერს და იყენებს მას თავისი ავი განზრახვებისათვის. ერთ-ერთი გავრცელებული მიზანი არის კომპიუტერის გამოყენება დიდი რაოდენობით სპამ მეილების გასაგზავნად. კომპიუტერებს ასეთ მდგომარეობაში უწოდებენ zombie-ის.

Windows XP ავტომატურად იწერს და აყენებს განახლებებს. თუმცა ეს ავტომატური რეჟიმი შეიძლება არ იყოს საუკეთესო მეთოდი ამ განახლებების განხორციელებისათვის, რადგანაც ეს შეიძლება ეწინააღმდეგებოდეს უსაფრთხოების წესდებას. და ამის გარდა ქსელის ადმინისტრატორს შეიძლება უნდოდეს შემოწმება განახლებების, სანამ ყველა კომპიუტერზე დაყენდებიან. ამისათვის Windows XP-ში არის რამდენიმე პარამეტრი:

- ავტომატური – გადმოწერა და დაყენება ხდება ავტომატურად, მომხმარებლისგან დამოუკიდებლად.
- მხოლოდ გადმოწერა – ავტომატურად ხდება გადმოწერა განახლებების, თუმცა მათი დაყენებისათვის მომხმარებლის ქმედება არის საჭირო.
- შემატყობინე – გამოდის შეტყობინება, რომ ახალი განახლებები გამოვიდა და გვაძლევს საუშუალებას გადმოვიწეროთ და დავაყენოთ.
- ავტომატური განახლების სრული გათიშვა – ამ დროს შემოწმებაც კი არ ხდება, გამოვიდა თუ არა ახალი განახლება.

თუ მომხმარებელი არის dial-up –ით დაკავშირებული ინტერნეტთან, მაშინ უნდა იყოს დაყენებული ან შეტყობინების რეჟიმზე, ან სრულად გათიშულ რეჟიმზე. რადგან ასეთ მომხრებელს ექნება სურვილი, აირჩიოს დრო, როდის მოხდეს განახლება, რომ არ შეფერხდეს ის და არ წაართვას რესურსები მუშაობის პროცესში.

თანამშრომლებს ორგანიზაციაში სხვადასხვა ტიპის კავშირის უფლებები უნდა ჰქონდეთ, მაგ., მენეჯერი და ბუღალტერი – შეიძლება მხოლოდ ამ ორს ჰქონდეს უფლება იხილოს ხელფასების შესახებ ინფორმაცია.

შეიძლება თანამშრომლების დაჯგუფება და უფლებების მინიჭება ჯგუფისათვის. ეს აადვილებს უფლებების მართვის ადმინისტრირებას. ქსელის კარგი მართვა შეამცირებს იმის საფრთხეს, რომ მავნე პროგრამული უზეუნველყოფა შეძლებს შემოაღწიოს ჩვენს ქსელში.

თანამშრომლის კავშირის უფლებების გაუქმება

როდესაც თანამშრომელი ტოვებს ორგანიზაციას, მისი შეღწევის უფლება პროგრამულ და აპარატურულ უზრუნველყოფაზე უნდა გაუქმდეს დაუყონებლივ. თუ ახალ თანამშრომელს დასჭირდება შეღწევა მოცემულ ინფორმაციაზე, შეიძლება მოხდეს აღდგენა და შეცვლა მომხმრებლის სახელის და პაროლის.

სტუმარი მომხმარებლები

დროებით თანამშრომლებს ან სტუმრებს შეიძლება დასჭირდეთ ჩართვა ქსელში. მაგ., ბევრ სტუმარს შეიძლება დასჭირდეს ელექტრონული ფოსტა, ინტერნეტი ან პრინტერი. ყველა ეს რესურსი შეიძლება იყოს ნებადართული სპეციალურად შექმნილი მომხმარებლისათვის, რომელსაც ეწოდება Guest-ი. როდესაც სტუმრები არ არიან, ამ მომხმარებლის გაუქმე შეიძლება, ხოლო შემდგომ ისევ გააქტიურება. ზოგიერთ სტუმარს შეიძლება დასჭირდეს ფართო კავშირი ქსელთან, მაგ., კონსულტანტს ან აუდიტორს. ესეთი ტიპის კავშირის უფლების მინიჭება უნდა მოხდეს მხოლოდ იმ დროის მანძილზე, რა დროც არის საჭირო სამუშაოს შესრულებისთვის.

მონაცემთა სარეზერვო ასლი ინახება გადასატან მოწყობილობაზე, რომლის შენახვაც შეიძლება უსაფრთხო ადგილას.

თუ აპარატურას რაიმე მოუვა ან დაიკარგე მონაცემები, მათი აღდგენა შეგვეძლება სარეზევო ასლიდან და სამუშაო გაგრძელდება.

სარეზერვო ასლების შექმნა უნდა ხდებოდეს რეგულარულად. ყველაზე ახალი ასლი, როგორც წესი, ინახება დაშორებულ ადგილს. თუ რაიმე მოუვა სათაო ოფისს, რომ დარჩეს სარეზერვო ასლი. როგორც წესი, ამ მოწყობილობაზე მრავალჯერ ახდენენ ინფორმაციის დაკოპირებას, რომ მოახდინო თანხის ეკონომია.

სარეზერვო ასლის შესასრულებლად შეგიძლიათ გამოიყენოთ ბრძანება NTBACKUP. თუმცა ამ ბრძანებას ვერ გამოიყენებთ ინფორმაციის აღსადგენად.

რამდენიმე ტიპი არსებობს ასლის სარეზერვო გადაღებისა:

- სრული – სრულად ხდება რეზერვირება მთელი მონაცემების.
- ზრდადი – რეზერვირება ხდება მხოლოდ შეცვლილი ან დამატებული მონაცემების.
- დიფერენციული – იმავეს, როგორც ზრდადი რეზერვირება, თუმცა არ ახდენს მონაცემების მარკირებას როგორც დარეზერვირებულის.

უსაფრთხოების Troubleshooting-ი

Troubleshooting-ის პროცესი გამოიყენება პრობლემების იდენტიფირებისათვის და მათ აღმოსაფხვრელად. ქვემოთ მოხმობილი ნაბიჯები დაგეხმარებათ ამაში:

პირველი ნაბიჯი არის ინფორმაციის მოძიება. დაიწყეთ მომხმარებლის გამოკითხვით:

- არის რომელიმე ქსელური რესურსი, რომელთანაც გაქვთ კავშირი უკაბელო ქსელის მეშვეობით?
- როდის დაწყო პრობლემა?
- რა პრობლემებს გადააწყდით?
- რა უსაფრთხოების პროგრამული უზრუნველყოფა არის დაყენებული თქვენს კომპიუტერზე?
- ინტენეტს როგორ უკავშირდებით?
- რა ტიპის Firewall-ს იყენებთ?
- აღწერეთ თქვენი სამუშაო გარემო.
- უკანასკნელად როდის მოახდინეთ თქვენი მონაცემების სარეზერვო ასლის შექმნა?
- რა ტიპის სარეზერვო ოპერაცია იყო ჩატარებული?
- რომელი ჯგუფის წევრი ხართ?

მას შემდგომ, რაც გაესაუბრებით კლიენტს, უნდა დააზუსტოთ (ნოუთბუქისთვის):

- არის თუ არა უკაბელო კავშირის წერტილი ჩართული?
- ვინმე სხვას, თუ აქვს ასეთი პრობლემა?
- შეძელით თუ არა ინტერნეტთან დაკავშირება მას შემდგომ, რაც განახლდა უკაბელო ქსელის მარშრუტიზატორი?
- ეს პრობლემა მარტო თქვენს მაგიდასთან ხდება, თუ ოფისის სხვა ადგილებშიც?
- დაკავშირებიხართ თუ არა უკაბელო ქსელს წარმატებით ნებისმიერ სხვა ადგილზე?
- ავტომატური განახლება გათიშულია?
- Firewall-ი სწორად არის კონფიგურირებული?

მას შემდგომ, რაც პრობლემას ამოიცნობთ, სცადეთ მარტივი გადაწყვეტები:

- შეამოწმეთ უკაბელო სიგნალი
- შეეცადეთ უსაფრთხოების გათიშული პარამეტრებით ქსელთან დაკავშირებას, რომ დაინახოთ, არის თუ არა პრობლემა მათი ბრალი.
- გამოდით და თავიდან შედით ვინდოუსში.
- გადატვირთეთ მოწყობილობა
- გადაამოწმეთ უფლებები რესურსებზე.
- გაუშვით ანტივირუსული პროგრამა.

თუ სწრაფმა გადაწყვეტებმა ვერ გამოიღეს შედეგი, მაშინ დაიწყეთ კომპიუტერიდან ინფორმაციის მოძიება:

- შეამოწმეთ Firewall-ის ჩანაწერები.
- შეამოწმეთ Task Manager-ი
- შეამოწმეთ, არის თუ არა განახლებული ანტივირუსული პროგრამის ბაზა
- შეამოწმეთ უფლებები
- შეამოწმეთ მომხმარებლის (account-ის) ტიპი.
- დაელაპარაკეთ სისტემურ ადმინისტრატორს
- შეამოწმეთ, ჩართული არის თუ არა CAPs lock და Num lock

პრობლემის აღმოფხვრაში დაგეხმარებათ:

- პრობლემების აღმოფხვრის გამოცდილება
- სხვა ტექნიკოსები
- ინტერნეტში ძიება

- ახალი ამბების ჯგუფები
- მწარმოებლის FAQ დოკუმენტი
- კომპიუტერის ინსტრუქცია
- მოწყობილობის ინსტრუქცია
- ონლაინ ფორუმები
- ტექნიკური ვებ გვერდები

მას შემდგომ, რაც პრობლემა აღმოიფხვრება, შეასრულეთ შემდეგი:

- განიხილეთ გადაწყვეტილება, რომლის განხორციელებაც მოხდა, მომხმარებელთან.
- სთხოვეთ მომხმარებელს, დაადასტუროს, რომ პრობლემა აღმოიფხვრა.
- გადაეცით კლიენტს ყველა საჭირო დოკუმენტი.
- აღწერეთ, რა ნაბიჯები გადადგით პრობლემის აღმოსაფხვრელად შეკვეთის ფორმაშიც და ტექნიკოსის ჟურნალშიც.
- ჩამოწერეთ ყველა კომპონენტი, რომელთა გამოყენებაც მოხდა პრობლემის აღმოფხვრის დროს.
- აღნიშნეთ, რა დრო დაგჭირდათ პრობლემის აღმოსაფხვრელად.

ხშირი პრობლემების ამოცნობა და აღმოფხვრა

უსაფრთხოების პრობლემები შეიძლება იყვიs დაკავშირებული აპარატურასთან, პროგრამულ უზრუნველყოფათან, ქსელთან ან მათ კომბინაციასთა.

- კლიენტი გატყობინებთ, რომ სარეზერვო კოპიის შექმნის პროცესი, რომელიც წინა დღეს დაიწყო, ჯერ კიდევ არ დასრულებულა – ურჩიეთ სხვა ტიპის სარეზერვო კოპირება განახორციელოს, რომ დაზოგოს დრო.
- კონსულტანტს Gუესტ მომხმარებლით, ვერ ახერხებს ქსელურ რესურსთან კავშირს – მისი მუშაობის მანძილზე მიეცით მას წვდომის უფლება ხოლო შემდგომ გააუქმეთ მისი უფლება.
- თანამშრომელი გატყობინებთ რომ ის არ მოგწერთ მომხმარებლის სახელს და პაროლს – აუხსენით მას რომ არ მოგითხოვიათ, და სხვებს შეატყობინეთ ასეთი თავდასხმის შესახებ.
- მომხმარებელი პოულობს ფაილს სერვერზე მაგრამ ვერ იწერს მას – შეუცვალეთ ამ ფაილს უფლებები წაკითხვიდან – წაკითხვა-გაშვებაზე.

- მომხმარებელი ვერ უკავშირდება უკაბელო ქსელს მას შემდეგაც კი, რაც სწორი გასაღები შეიყვანა – გადაამოწმეთ, წერია თუ არა მომხმარებლის ფიზიკური მისამართი უკაბელო ქსელის წვდომის წერტილის ფიზიკური მისამართების ფილტრში.

სარჩევი