სარჩევი

ქსელის ფუნქციონირება, საქსელო მოდელი OSI. ზოგადი ანალიზი.

ყველა პროცედურის მოწესრიგებას, მათ დონეებად და ქვედონეებად დაყოფას, რომლებიც ურთიერთქმედებენ ერთმანეთთან ემსახურება საქსელო მოდელები. დღესდღეობით ყველაზე ფართო გავრცელება ჰპოვა ე.წ ღია სისტემის ინფორმაციის გაცვლის (Open System Interconnection) OSI ეტალონურმა მოდელმა. ტერმინის ქვეშ „ღია სისტემა“ იგულისხმება არა ჩაკეტილი სისტემა, არამედ სისტემა, რომელიც ურთიერთმოქმედებს სხვა სისტემებთან (ჩაკეტილი სისტემებისგან განსხვავებით).

OSI მოდელი წარმოადგინა სტანდარტების საერთაშორისო ორგანიზაციამ ISO (International Standards Organization) 1984 წელს. მას შემდეგ მას იყენებენ ქსელური პროდუქტების მწარმოებლები. როგორც ყველა სხვა უნივერსალური მოდელი OSI მოდელიც საკმაოდ დიდია მოცულობით და არც თუ ისე მოქნილია. ამიტომაც რეალური ქსელური საშუალებები, რომლებიც წარმოდგენილია სხვადასხვა ფირმების მიერ დღეს არ ეყრდნობიან ამ მოდელს. თუმცა OSI მოდელის გაცნობა დაგვეხმარება უკეთ გავერკვეთ თუ რა ხდება ქსელში.

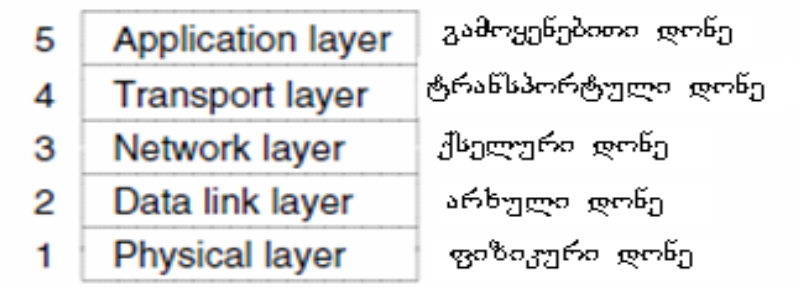
ყველა ქსელური ფუნქცია OSI მოდელში დაყოფილია 7 დონედ (ნახ. 1). ამასთანავე ზედა დონეები უფრო რთულ და გლობალურ ამოცანებს ასრულებენ და იყენებენ ამისათვის ქვედა დონეებს და აგრეთვე მართავენ მათ. ქვედა დონეები ასრულებენ უფრო მარტივ და კონკრეტულ ფუნქციებს. იდეაში ყოველი დონე ურთიერთქმედებს მხოლოდ მის მეზობელ დონეებთან (მის ზემოთ და მის ქვემოთ). ზედა დონე შეესაბამება გამოყენებით ამოცანას მოცემულ მომენტში, ხოლო ქვედა დონე უშუალოდ სიგნალების გადაცემას კავშირის არხში.

OSI მოდელი მიეკუთვნება არამხოლოდ ლოკალურ ქსელებს, არამედ ნებისმიერ სხვა ქსელებსაც. კერძოდ ინტერნეტ ქსელის ფუნქციები შეიძლება ასევე დავყოთ დონეებად OSI მოდელის შესაბამისად. პრინციპული განსხვავება ლოკალურსა და გლობალურ ქსელებს შორის, OSI მოდელის თვალსაზრისით, შეინიშნება მხოლოდ ქვედა დონეებზე. ყველა დონის ფუნქციას, რომლებიც მოცემულია ნახ.1.-ზე ასრულებს ქსელის ყოველი აბონენტი. ამასთანავე ყოველი დონე ერთ აბონენტზე მუშაობს ისე, რომ თითქოს მას აქვს კავშირი მეორე აბონენტის შესაბამის დონესთან. ერთი დონის აბონენტებს შორის არსებობს ვირტუალური (ლოგიკური) კავშირი, მაგ. გამოყენებით ანუ პროგრამულ დონეებს შორის. რეალური ანუ ფიზიკური კავშირი (კაბელი, რადიოარხი) აბონენტებს გააჩნიათ მხოლოდ ყველაზე დაბალ დონეზე (პირველ ანუ ფიზიკურ დონეზე). გადამცემ აბონენტში ინფორმაცია გაივლის ყველა დონეს დაწყებულ ზედა დონიდან და დამთავრებული ქვედათი. ხოლო მიმღებ აბონენტში კი პირიქით ინფორმაცია გაივლის გზას უკუმიმართულებით: ქვედა დონიდან ზედა დონემდე.

OSI მოდელი			
	მონაცემების ერთეული	**დონე**	**ფუნქცია**
ჰოსტის დონეები	მონაცემები	პროგრამული	ქსელის მიწოდება პროგრამისათვის
		პრეზენტაციის	მონაცემების შიფრაცია და წარდგენა
		სესიის	კავშირის კავშირი
	სეგმენტები	ტრანსპორტული	კავშირი ორ უკიდურეს წერტილს შორის და საიმედოობა
მატარებელი დონეები	პაკეტები	ქსელური	გეზის განსაზღვრა და ლოგიკური მისამართები (IP)
	კადრები	მონაცემთა არხი	ფიზიკური მისამართები (MAC და LLC)
	ბიტები	ფიზიკური	მატარებელი ნაზი, სიგნალი და ორობითი გადაცემა

გარდა OSI-მოდელისა არსებობს მოდელი, **IEEE Project 802,** რომელიც მიღებულ იქნა 1980 წელს, იგი შეიძლება განხილულ იქნას როგორც OSI-მოდელის მოდიფიკაცია, განვითარება და დაზუსტება. ამ მოდელის მიერ განსაზღვრული სტანდარტები (ე.წ. 802-სპეციფიკაციები) მიეკუთვნება OSI-მოდელის ქვედა ორ დონეს და იყოფა 23 კატეგორიად.

საბოლოო დასკვნა: მიუხედავად თავისი ნაკლოვანებებისა OSI მოდელი (სეანსური და წარმოდგენითი დონეების გარდა) საკმაოდ სასარგებლოა კომპიუტერულ ქსელებში თეორიული დისკუსიებისათვის. ხოლო OSI მოდელის პროტოკოლებმა კი ვერ ჰპოვეს ფართო გავრცელება. TCP/IP მოდელისათვის კი პირიქით: მოდელი პრაქტიკულად არ არსებობს, მაშინ როდესაც ამ მოდელის პროტოკოლები საკმაოდ პოპულარულია. აქედან გამომდინარე დღესდღეობით გამოიყენება მოდიფიცირებული OSI მოდელი, ხოლო პროტოკოლები კი ძირითადად TCP/IP. ამრიგად, გამოიყენება ქსელის ჰიბრიდული მოდელი, რომელიც მოცემულია ქვემოთ.



სტატიკური IP მისამართი და დინამიური IP მისამართი. DHCP სერვერი.

სტატიკური IP მისამართის მინიჭებისას ქსელში ადმინისტრატორი თვითონ აკონფიგურირებს ქსელის პარამეტრებს თითოეული ჰოსტისთვის, როგორიცაა: ჰოსტის IP მისამართი (IP address), ქსელის ნიღაბი (Subnet mask) და ინტერნეტში გასასვლელი (Default Gateway).
სტატიკურ IP მისამართებს გააჩნიათ გარკვეული უპირატესობები. მაგ. მათი გამოყენება განსაკუთრებით მოსახერხებელია ლოკალურ ქსელში პრინტერებისთვის, სერვერებისათვის და ქსელში მომუშავე სხვა მოწყობილობებისათვის, რომლებსაც უკავშირდებაინ მომხმარებლები. თუ ჰოსტი უკავშირდება სერვერს განსაზღვრული IP მისამართით, მაშინ ამ მისამართის შეცვლა არა არის მიზანშეწონილი. IP მისამართის სტატიკურად განსაზღვრა ზრდის ქსელის მართვის რესურსებს, მაგრამ საკმაოდ შრომატევადია ქსელური პარამეტრების შეყვანა თითოეული ჰოსტისთვის ცალ-ცალკე. ხშირია შეცდომებიც ამ მეთოდის შემთხვევაში.
სტატიკური IP მისამართის გამოყენების შემთხვევაში აუცილებელია ზუსტი ცოდნა იმისა თუ რომელი IP მისამართი რომელ მოწყობილობას მიენიჭა. სტატიკური IP მისამართები მუდმივი მისამართებია, რომელთა ხელახლა გამოყენება არ ხდება.

დინამიური IP მისამართი

ლოკალურ ქსელებში დღითიდღე მატულობს მომხმარებელთა რიცხვი. ქსელის ადმინისტრატორი ანიჭებს IP მისამართს ყოველ მომხმარებელს პერსონალურად, ამიტომაც უფრო ადვილია IP მისამართების ავტომატურად მინიჭება. ეს კი შესაძლებელია ე.წ. DHCP (Dynamic Host Configuration Protocol) პროტოკოლის მიერ.
DHCP–ს გააჩნია მექანიზმი, რომელიც ავტომატურად ანიჭებს დამისამრთების (addressing) პარამეტრებს, როგორიცაა: IP მისამართი, ქსელის მასკა, ქსელში გასასვლელი და კონფიგურაციის სხვა ინფორმაცია.
DHCP – ის ენიჭება უპირატესობა ჰოსტებისთვის IP მისამრთების მინიჭებისას დიდმაშტაბიან ქსელებში, რადგანაც ის უმსუბუქებს ქსელის ადმინისტრატორს შრომას და ამასთანავე აღმოაჩენს შეცდომებს.
მეორე ღირებულება DHCP – ისა ის არის, რომ IP მისამართი ჰოსტს ენიჭება არა მუდმივად, არამედ ის დაქირავებულია დროის განსაზღვრული პერიოდისათვის. თუ ჰოსტი გამოირთო, მაშინ IP მისამრთი ბრუნდება რეზერვში შემდგომში გამოსაყენებლად. ეს კი მოსახერხებელია განსაკუთრებით მობილური აბონენტებისათვის.

DHCP სერვერი

თუ თქვენი laptop-ის DHCP– კლიენტი უკავშირდება DHCP– სერვერს უსადენოდ ამ შემთხვევაში laptop-ს ენიჭება IP მისამართი DHCP – სერვერის მიერ.

DHCP – სერვერი შეიძლება იყოს ნებისმიერ მოწყობილობა, რომელიც გამოიყენებს DHCP სერვისულ პროგრამულ უზრუნველყოფას. უფრო მეტ შემთხვევაში DHCP – სერვერად გამოიყენება გამოყოფილი ლოკალური PC სერვერი.
სახლის ქსელების შემთხვევაში DHCP – სერვერს მართავს ISP (Internet Service Provider), ხოლო ჰოსტი IP კონფიგურაციას იღებს პირდაპირ ISP-გან.
სახლის და მცირე ბიზნესის ქსელების უმრავლესობა იყენებს ინტეგრირებულ როუტერს ISP მოდემთან შესაერთებლად. ამ შემთხვევაში ინტეგრირებული როუტერი არის როგორც კლიენტი, ასევე სერვერი. ინტეგრირებული როუტერი ასრულებს კლიენტის როლს და იღებს IP კონფიგურაციას ISP-გან, ხოლო შემდეგ კი იქცევა, როგორც DHCP სერვერი ლოკალური ქსელის შიდა ჰოსტებისათვის.

ერთრანგიანი და სერვერის შემცველი ქსელები. კომპიუტერული ქსელის ტოპოლოგიები და მათი სახესხვაობები.

ლოკალური ქსელები. არის კომპიუტერების გაერთიანება, რომლებიც ერთმანეთისაგან მცირე მანძილით არიან დაშორებულნი, ადრე ეს მანძილი ეს 1-2 კმ-ის რადიუსს შეადგენდა. თუმცა ცალკეულ შემთხვევაში ლოკალურ ქსელს შეიძლება უფრო დიდი, ფართო მასშტაბები ჰქონდეს. ლოკალური ქსელი წარმოადგენს საკომუნიკაციო სისტემას, რომელიც ერთ ორგანიზაციას განეკუთვნება. პირველ ხანებში კომპიუტერების დასაკავშირებლად გამოიყენებოდა არასტან-დარტული პროგრამულ-აპარატული საშუალებები, სხვადასხვაგვარი მოწყობილობები, რომლებიც იყენებდნენ საკუთარ მეთოდებს მონაცემთა გადასაცემად. მათ შეეძლოთ გაეერთიანებინათ მხოლოდ კომპიუტერების კონკრეტული მოდელები, რომლებისთვისაც იყვნენ შექმნილები. ლოკალურ ქსელებში მდგომარეობა კარდინალურად შეიცვალა 80-იან წლებში. შეიქმნა და დამტკიცდა სტანდარტული ქსელური ტექნოლოგიები, როგორიც არის Ethernet, Arcnet, Token Ring, Token Bus, მოგვიანებით – FDDI. მათ შესაქმნელად მნიშვნელოვანი სტიმული გახდა პერსონალური კომპიუტერების არსებობა. ეს მასობრივი პროდუქტი ქსელის შესაქმნელად იდეალური ელემენტი აღმოჩნდა - ერთის მხრივ ისინი საკმაოდ მძლავრები იყვნენ ქსელური პროგრამების უზრუნველსაყოფად და მეორეს მხრივ ნათლად საჭიროებდნენ თავიანთი სიმძლავრის გაერთიანებას რთული ამოცანების გადასაჭრელად და ძვირადღირებული პერიფერიული მოწყობილობების გასანაწილებ-ლად. პერსონალური კომპიუტერები ქსელში არა მხოლოდ კლიენტი კომპიუტერის სახით გამოიყენეს, არამედ როგორც მონაცემების შენახვისა და დამუშავების ცენტრებად ანუ სერვერებად.

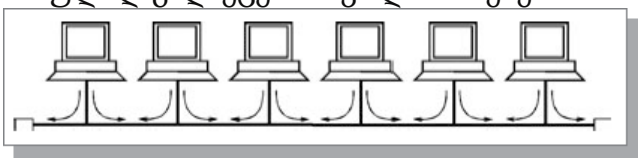
ლოკალური ქსელის ტოპოლოგიის (აგების, კონფიგურაციის, სტრუქტურის) ქვეშ იგულისხმება კომპიუტერების ფიზიკური განლაგება ურთიერთ შორის და მათი შეერთების მეთოდი კავშირის ხაზებით. ცნება ტოპოლოგია მიეკუთვნება, უპირველეს ყოვლისა, ლოკალურ ქსელებს, სადაც კავშირების სტრუქტურის განსაზღვრა სირთულეს არ წარმოადგენს. გლობალურ ქსლებში კი კავშირების სტრუქტურა დაფარულია მომხმარებლებისგან და არ არის მნიშვნელოვანი, რადგანაც ყოველი კავშირის სეანსი იწარმოება საკუთარი გზით.

ტოპოლოგია განსაზღვრავს მოთხოვნილებებს აპარატურისადმი, გამოყენებული კაბელის ტიპისადმი, გაცვლის მართვის მეთოდებისადმი, მუშაობის საიმედოობისა და ქსელის გაფართოების შესაძლებლობებისადმი.

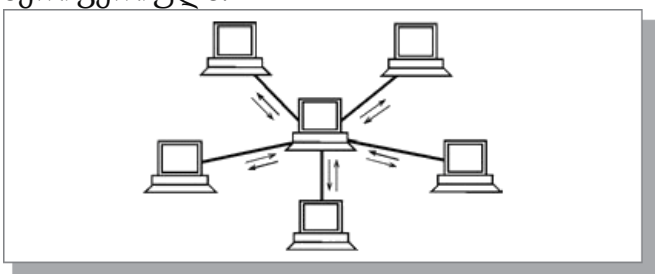
არსებობს ქსელის სამი ძირითადი ტოპოლოგია:

- სალტის
- ვარსკვლავის
- წრის

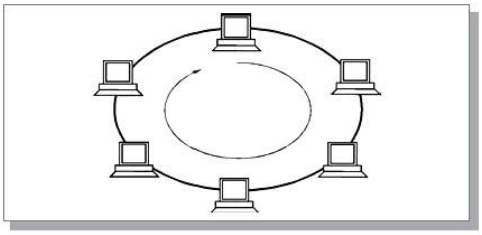
სალტის (BUS) ტოპოლოგიის შემთხვევაში კომპიუტერები პარალელურადაა მიერთებული ერთადერთ კავშირის არხთან. ინფორმაცია თითოეული მათგანიდან ერთდროულად გადაეცემა სხვა დანარჩენებს.



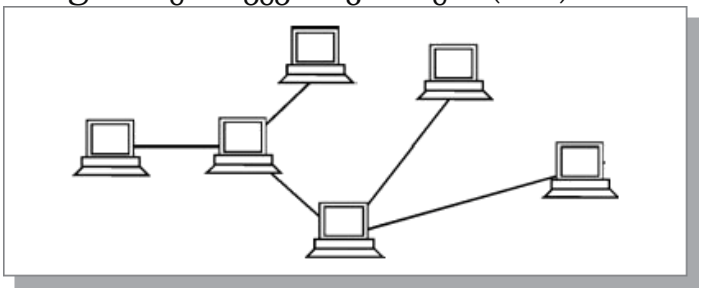
ვარსკვლავის (STAR) ტოპოლოგია – ცენტრალურ კომპიუტერს უერთდება ყველა დანარჩენი პერიფერიული კომპიუტერები, ამასთანავე თითოეული მათგანი იყენებს ცალკეულ კავშირის ხაზს. ინფორმაცია პერიფერიული კომპიუტერიდან გადაეცემა მხოლოდ ცენტრალურს, ხოლო ცენტრალურიდან ერთს ან რამდენიმე პერიფერიულს.



წრის (RING) – კომპიუტერები თანამიმდევრობით ერთდებიან წრეში. მონაცემთა გადაცემა წრეში ხდება მხოლოდ ერთი მიმართულებით. ყოველი კომპიუტერი ინფორმაციას გადასცემს მხოლოდ ერთ კომპიუტერს მის შემდგომს ხოლო ღებულობს ინფორმაციას წინ მდგომისაგან.

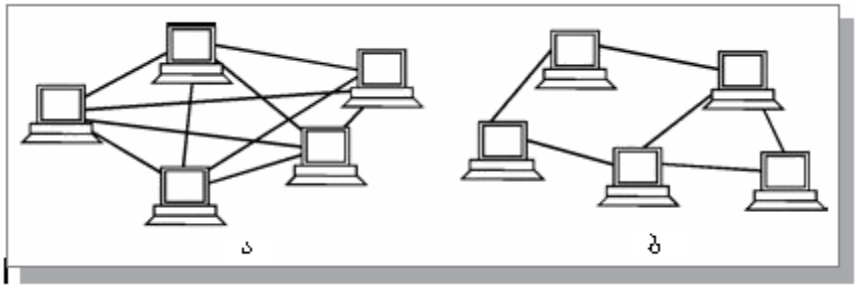


გარდა სამი საბაზო ტოპოლოგიებისა საკმაოდ ხშირად გამოიყენება **ხისებრი ქსელური ტოპოლოგია (tree),** რომელიც შეიძლება განვიხილოთ როგორც რამდენიმე ვარსკვლავის კომბინაცია. აქტიური ხის შემთხვევაში რამდენიმე კავშირის არხის შეერთების ცენტრებში განლაგებულია ცენტრალური კომპიუტერები, ხოლო პასიურის შემთხვევაში კი ჰაბები (Hub).



საკმაოდ ხშირად გამოიყენება კომბინირებული ტოპოლოგიები მათ შორის ყველაზე გავრცელებულია ვარსკვლავურ-სალტისებრი (star-bus) და ვარსკვლავურ-წრიული (star-ring).

უნდა აღინიშნოს ბადური ტოპოლოგია (mesh topology), უნდა აღინიშნოს ბადური ტოპოლოგია



სრული ბადური ტოპოლოგიის შემთხვევაში ყოველი კომპიუტერი პირდაპირ კავშირშია დანარჩენებთან. ამ შემთხვევაში კომპიუტერების რიცხვის გაზრდის შემთხ-ვევაში იზრდება კავშირის ხაზებიც. გარდა ამისა, ნებისმიერი ცვლილება კონფიგურაციაში მოითხოვს ცვლილებების შეტანას ყველა კომპიუტერის ქსელურ აპარატურაში., ამიტომაც სრულმა ბადურმა ტოპოლოგიამ ვერ ჰპოვა ფართო გავრცელება.

ქსელში არასანქცირებული წვდომის რისკები და მათთან ბრძოლის მეთოდები.

სადენიანი თუ უსადენო კომპიუტერული ქსელები უფრო და უფრო მნიშვნელოვანი ხდებიან ყოველდღიურ ცხოვრებაში. კერძო პირები თუ და ორგანიზაციები თუ მათი ყოველდღიური საქმიანობა დამოკიდებულია კომპიუტერებზე და ქსელებზე ფუნქციონალურად, კერძოდ მათ სერვისებზე, როგორიცაა ელექტრონული ფოსტა, საბუღალტრო აღრიცხვა, ფაილების მენეჯმენტი და ა.შ. არასანქცირებული პირის მიერ ქსელში შემოღწევამ კი შეიძლება გამოიწვიოს ქსელის მწყობრიდან გამოყვანა და მუშაობის ჩაგდება, შესაბამისად მნიშვნელოვანი ინფორმაციის დაკარგვა და ფინანსური ზარალი.

არასანქცირებულ პირებს, რომლებსაც შეუძლიათ ქსელთან წვდომა პროგრამული უზრუნველყოფის სუსტი წერტილის პოვნით ან მასში ცვლილებების შეტანით მათ **ჰაკერები** ეწოდებათ.

თუ ჰაკერმა მოახდინა ქსელთან წვდომა შეიძლება შეიქმნას ოთხი სახის საშიშროება:

- ინფორმაციის მოპარვა
- იდენტიფიკაციის მოპარვა
- მონაცემების დაკარგვა/მანიპულაცია
- სერვისის მწყობრიდან გამოსვლა

ქსელში შეღწევის წყაროები

ჰაკერების ქსელში შემოღწევის საშიშროება არსებობს, როგორც შიდა ასევე გარე წყაროებიდან.

გარეშე საფრთხეები

გარეშე საფრთხეები წარმოიქმნება გარეშე პირების მიერ, რომლებსაც არა აქვთ მოცემულ ქსელთან ავტორიზებული წვდომის უფლება. მათ შეიძლება ქსელში შემოაღწიონ ან ინტერნეტის, უსადენო არხების ან კიდევ dial-up წვდომის სერვერების მეშვეობით.

შიდა საფრთხეები

შიდა საფრთხეები წარმოიქმნება, როდესაც აუტორიზებული პირი, რომელსაც აქვს ქსელთან წვდომის უფლება და შესაბამისად მომხმარებლის ექაუნთი ან ფიზიკური წვდომა ქსელის აპარატურასთან დატოვებულია უყურასღებოდ. შიდა ატაკერმა იცის კორპორაციის შიდა პოლიტიკა და ხალხი. აგრეთვე იცის თუ რა ინფორმაციაა ძვირადღირებული მტკივნეული და როგორ შეიძლება მათი მოპოვება.

თუმცა ყველა შიდა ატაკერი არ შეიძლება მოქმედებდეს წინასწარ გამიზნულად. ზოგ შემთხვევებში შიდა საფრთხე შიდა მოდის კომპანიის თანამშრომლისგან, რომელიც იმსახურებს ნდობას. მან შეიძლება ეს გამოიწვიოს ვირუსების აკიდებით და ამით შექმნას დაცვის საფრთხე არა შეგნებულად.

კომპანიების უმეტესობა საკმაო რესურსებს უთმობენ გარე ატაკერების საწინააღმ-დეგოდ, როცა უმეტესობა დაცვის საფრთხეებიდან მოდის შიდა რესურსებიდან. FBI -

ის მიხედვით შიდა წვდომა და კომპიუტერული სისტემების ბოროტად გამოყენების 80% -ია დაფიქსირებული.

სოციოტექნიკა და ფიშინგი

ყველაზე ადვილი მეთოდი ჰაკერებისათვის ქსელთან წვდომისათვის არის ადამიანის ქცევის ექსპლუატაცია.

ერთ-ერთი ზოგადი მეთოდებიდან ადამიანური სისუსტეების ექსპლუატირებისათვის არის ე.წ. სოციოტექნიკა (Social Engineering).

სოციოტექნიკა (Social Engineering)

სოციოტექნიკა არის ცნება, რომელიც გულისხმობს რაღაცის ან ვიღაცის შესაძლებლობას, ზემოქმედება მოახდინოს ადამიანთა ჯგუფის ქცევაზე. კომპიუტერის და ქსელის დაცვის კონტექსტში სოციოტექნიკა გულისხმობს მეთოდების ერთობლიობას, რომელსაც იყენებს შიდა მომხმარებლების მოსატყუებლად სპეციალური მოქმედებების შესრულებით ან კონფიდენციალური ინფორმაციის გახსნით.

მსგავსი მეთოდების მეშვეობით ჰაკერს აქვს უპირატესობა ვიდრე ქსელში ჩართულ სწორუფლებიან მომხმარებლებს, რომ მოიპოვოს წვდომა შიდა რესურსებთან და საიდუმლო ინფორმაცია, როგორიცაა ბანკებია ექაუნთები და პაროლები.

სცოიოტექნიკის თავდასხმებისას სარგებლობენ დაცვის მეთოდების სუსტი მხარეებით. ხაკერები შეიძლება იყოს, როგორც შიგნით ორგანიზაციაში, ასევე გარეთაც, მაგრამ ყოველი მათგანი არასოდეს პირისპირ არ ხვდება თავის მსხვერპლს.

სოციოტექნიკის ყველა გავრცელებული მეთოდებია: მოტივირება (pretexting), ფიშინგი (phishing), ვიშინგი (vishing).

(მოტივირება) pretexting

Pretexting არის სოციოტექნიკის ფორმა, სადაც გამოგონილი სცენარი (pretext) გამოიყენება მსხვერპლის მიმართ, რომ გასცეს ინფორმაცია ან შეასრულოს შესაბამისი მოქმედება. სამიზნე კი ტელეფონით კონტაქტია. მოტყუება, რომ ეფექტური იყოს ჰაკერმა უნდა განახორციელოს მსხვერპლთან კანონიერი კავშირი. რასაც სჭირდება ჰაკერისგან შესაბამისი ცოდნის ქონა. მაგ. თუ ჰაკერმა იცის მისი დაზღვევის ნომერი, მაშინ შეუძლია მოატყუოს მსხვერპლი, რომელიც დარწმუნებულია ჰაკერის ლეგალობაში.

ფიშინგი (phishing)

ფიშინგი არის სოციოტექნიკის ფორმა, რომლის დროსაც ჰაკერი უკავშირდება ინდივიდუალურად მსხვერპლს ელ-ფოსტის მეშვეობით ორგანიზაციის გარეთ. ფიშერი ეკითხება ინფორმაციის ვერიფიკაციისათვის ინფორმაციას, როგორიცაა მომხმარებლის სახელი და პაროლი.

IP-დამისამართება, კლასები, Unicast, Broadcast და Multicast მისამართები.

IP-მისამართი წარმოადგენს მისამართების ძირითად ტიპს, რომლის საფუძველზეც ქსელური დონე აგზავნის პაკეტებს ქსელებს შორის. ეს მისამართები შედგება 4 ბაიტისგან, მაგ. 109.26.17.100. IP-მისამართი განისაზღვრება ადმინისტრატორის მიერ კომპიუტერისა და მარშრუტიზატორების კონფიგურაციისას. IP-მისამართი შედგება ორი ნაწილისგან: ქსელის ნომრისა და კვანძის ნომრისაგან. ქსელის ნომერი შეირჩევა ადმინისტრატორის მიერ ნებისმიერი ან Internet-ის (Internet Network Information Center, InterNIC) სპეციალური ქვეგანყოფილების რეკომენდაციების მიხედვით, თუ ქსელმა უნდა იმუშაოს, როგორც Internet-ის შემადგენელმა ნაწილმა. Internet-ის სერვისების მიმწოდებლები ჩვეულებრივ მისამრთების დიაპაზონს იღებენ InterNIC-გან და შემდგომ ანაწილებენ თავიანთ აბონენტებს შორის. მარშრუტიზატორი განსაზღვრების თანახმად შედის რამდენიმე ქსელში და ამიტომაც მის ყოველ პორტს გააჩნია საკუთარი IP-მისამართი. საბოლოო კვანძი შეიძლება შედიოდეს რამდენიმე IP-ქსელში. ამ შემთხვევაში კომპიუტერს უნდა გააჩნდეს რამდენიმე IP-მისამართი ქსელური კავშირების რიცხვის მიხედვით. მაშასადამე, IP-მისამართით ხასიათდება არა ერთი ცალკეული კომპიუტერი ან მარშრუტიზატორი, არამედ ერთი ქსელური შეერთება.

IP-მისამართების კლასები. IP-მისამართის სიგრძე შეადგენს 4 ბაიტს და ჩვეულებრივ ჩაიწერება ოთხი რიცხვის სახით, სადაც ყოველი ბაიტი გამოისახება ათობითი რიცხვით, რომლებიც დაყოფილნი არიან წერტილებით. მაგ., 128.10.2.30 – ტრადიციული ათობითი ფორმა მისამართის წარმოსადგენად, 10000000 00001010 00000010 00011110 - ორობითი ფორმა ამავე მისამართისა.

მისამართი შედგება ორი ლოგიკური ნაწილისგან - ქსელის ნომრისა და ქსელში კვანძის ნომრისგან. მისამართის თუ რომელი ნაწილი მიეკუთვნება ქსელის ნომერს და რომელი კვანძისას, განისაზღვრება მისამართის პირველი ბიტების მნიშვნელობებით. ამ ბიტების მნიშვნელობები კი განსაზღვრავენ თუ რომელ კლასს მიეკუთვნება ესა თუ ის IP-მისამართი.

Unicast მისამართი ერთი-ყველასთან IP ქსელისაა. პაკეტი Unicast მისამართით დანიშნულია სპეციალური ჰოსტისთვის. მაგალითად შეიძლება მოვიყვანოთ ჰოსტი 192.168.1.5 IP მისამართით (გადამცემი), რომელმაც გააგზავნა მოთხოვნა WEB გვერდზე სერვერისგან IP მისამართისგან 192.168.1.200 (მიმღები).

Broadcast მისამართის შემთხვევაში პაკეტი შეიცავს მიმღების IP მისამართს, რომელიც შეიცავს მხოლოდ ერთიანებს ჰოსტის ნაწილში. ეს ნიშნავს, რომ ყველა ჰოსტს ლოკალურ ქსელში შეუძლია მიიღოს და ნახოს პეკეტები. ქსელური პროტოკოლების უმრავლესობა, როგორიცაა: ARP და DHCP იყენებენ Broadcast–ს.

Multicast მისამართის მეშვეობით გადამცემი პაკეტს გადასცემს მოწყობილობათა ჯგუფს.

მოწყობილობებს, რომელიც მიეკუთვნება Mmulticast ჯგუფს მიენიჭება Multicast ჯგუფის IP მისამართი. Multicast მისამრთის დიაპაზონი შეადგენს 224.0.0.0-დან 239.255.255.255-მდე. ე.ი. Multicast მისამრთები გამოსახავენ მისამართების ჯგუფს (ზოგჯერ უწოდებენ ჰოსტის ჯგუფებს), რომლებიც გამოიყენება პაკეტის მიმღები. გადამცემს კი ყოველთვის Multicast მისამრთი გააჩნია.

ინფორმაციის გადაცემის ფიზიკური არე, სადენიანი და უსადენო გარემო, სტანდარტები.

კომპიუტერული ქსელების შესაქმნელად საჭიროა მისი კომპონენტების შეერთება. ქსელის ძირითად კომპონენტებს შეადგენენ პირველ რიგში თვითონ კომპიუტერები, როგორც კომპიუტერ-კლიენტები, ასევე კომპიუტერ-სერვერები, შემდეგ სხვადასხვა დანიშნულების მოწყობილობები. ქსელის შესაქმნელად ასევე საჭიროა სათანადო გარემოს არსებობა.

საქსელო კომპონენტები გარკვეული კანონებით, გარკვეულ გარემოში უერთდებიან ერთმანეთს და ქმნიან სხვადასხვა დანიშნულების კომპიუტერების ფუნქციონირების ერთიან სისტემას. ინფორმაციის გადამცემი გარემო ეწოდება კავშირის ხაზს (ან კავშირის არხს), რომ-ლის მეშვეობითაც კომპიუტერები აწარმოებენ ინფორმაციის გაცვლას ერთმანეთს შორის. კომპიუტერული ქსელების (განსაკუთრებით ლოკალური ქსელების) უმეტეს შემთხვევაში გამოიყენება სადენიანი კავშირის ხაზები, თუმცა არსებობს უსადენო ქსელებიც, რომლებიც უფრო ფართოდ გამოიყენებიან განსაკუთრებით პორტატულ კომპიუტერებში. ლოკლაურ ქსელებში ინფორმაცია უფრო მეტად მიმდევრობითი კოდის საშუა-ლებით გადაეცემა, ანუ ბიტობით. ასეთი გადაცემა ნელია და თან რთული ვიდრე პარალელური კოდის შემთხვევაში. ამისა დიდ მანძილებზე გადაცემა კაბელის ნებისმიერი ტიპის შემთხვევაში მოითხოვს გადამცემ და მიმღებ მხარეებზე სპეციალურ აპარატურას. მიმდევრობითი გადაცემის დროს ამისათვის აუცილებელია მხოლოდ ერთი გადამცემი და ერთი მიმღები. მხოლოდ პარალელურის შემთხვევაში მოთხოვნილი გადამცემისა და მიმღების რიცხვი იზრდება პარალელური კოდის თანრიგიანობის შესაბამისად. ამის გამო უფრო ხშირად გამოიყენება მიმდევრობითი გადაცემა. ზოგიერთ მაღალსიჩქარიან ლოკალურ ქსელებში გამოიყენება პარალელური გადაცემა 2-4 კაბელში. რაც საშუალებას იძლევა გამოყენებულ იქნას უფრო იაფი კაბელები უფრო დაბალი გამტარუნარუანობით. მაგრამ კაბელის დასაშვები სიგრძე

არ აღემატება 100 მეტრს. ამ შემთხვევის მაგალითს წარმოადგენს Fast Ethernet ქსელის 100BASE-T4 სეგმენტი.

კაბალების სამი ძირითადი ჯგუფს განასხვავებენ:

- ელექტრული (სპილენძის) კაბელები **მავთულების ხვეული წყვილის ბაზაზე,** რომლებიც იყოფა ეკრანირებული (shielded twisted pair, STP) და არაეკრანირებული (unshielded twisted pair, UTP);
  - ხვეული წყვილი (UTP/STP, არაეკრანირებული/ეკრანირებული ხვეული წყვილი) დგესდგეობით ყველაზე გავრცელებული გარემოა სიგნალის გადასაცემად ლოკალურ ქსელებში. UTP/STP კაბელები გამოიყენება Ethernet, Token Ring და ARCnet ქსელებში. მე-5 კატეგორიის კაბელში, როგორც წესი, არის 8 წვერი, გადახვეული წყვილ-წყვილად. Ethernet ქსელში გამოყენება სადენების (გრეხლი წყვილების) შეერთების ორი სახე: Patchcord და Crossover(ორი კომპიუტერის ერთმანეთთან დასაკავშირებლად).
- **ლექტრული (სპილენძის) კოაქსიალური კაბელები (coaxial cable);**
  - ლოკალური სადენებში თავდაპირველად კოაქსიალური კაბელი გამოიყენებოდა. ის, როგორც მონაცემთა გადაცემის გარემო უპირატესად Ethernet და ARCnet ქსელებში გამოიყენება. განასხვავებენ “წვრილ” და “მსხვილ” კოაქსიალურ კაბელებს.
- **ოპტიკურბოჭკოვანი კაბელები (fiber optic).**
  - ოპტიკური ბოჭკო, მისი სახელწოდებიდან გამომდინარე, სიგნალებს გადასცემს სინათლის გამოსხივების იმპულსების მეშვეობით. სინათლის წყაროდ გამოიყენება ნახევ-რადგამტარი ლაზერები და აგრეთვე სინათლის დიოდები. ოპტიკური ბოჭკო იყოფა ერთმოდიან და მრავალმოდიან კატეგორიებად.

თითოეულ კაბელს გააჩნია, როგორც უპირატესობები ასევე ნაკლოვანებები. ასე რომ მათი არჩევისას გასათვალისწინებელია ამოსახსნელი ამოცანის, ასევე კონკრეტული ქსელის და გამოყენებული ტოპოლოგიის თავისებურებები.

კაბელების შემდეგი ძირითადი პარამეტრები, რომლებიც პრინციპიალურად მნიშვნელოვანია ლოკალური ქსელებისათვის, წარმოადგენს:

- კაბელის გამტარუნარიანობა
- კაბელის დაბრკოლებისადმი მდგრადობა და ინფორმაციის გადაცემის დაცვა;
- კაბელში სიგნალის გავრცელება და სიგნალის დაყოვნება;
- ტალღურუ წინააღმდეგობის სიდიდე.

თანამედროვე ქსელების ორგანიზირება სულ უფრო ხშირად ხორციელდება უგამტარო გარემოს ბაზაზე. გამოთქმა „უგამტარო გარემო“ გარკვეულ დაზუსტებას მოით-ხოვს. იგი არ გულისხმობს ქსელში გამტარების საერთოდ არ ქონებას: ქსელი უგამტარო კომპონენტები ურთიერთქმედებენ ქსელის იმ ნაწილთან, რომელიც იყენებს გამტარებს. ტიპიური უგამტარო ქსელი გამოიყურება და ფუნქციონირებს, ისევე როგორც კაბელური, განსხვავება მხოლოდ გადაცემის გარემოშია. უგამტარო საქსელო ადაპტერი დაყენებულია თითოეულ კომპიუტერში და მომხმარებელი ისე სარგებლობს ამ კომპიუ-ტერით, თითქოს იგი სხვა კომპიუტერთან კაბელით არის შეერთებული. სპეციალური ტრანსივერი, რომელსაც ზოგჯერ შეღწევის წერტილსაც უწოდებენ, უზრუნველყოფს სიგნალების გაცვლას კომპიუტერებს შორის, რომელთა ნაწილი უგამტარო გარემოში მუშაობს და ნაწილი კი ჩვეულებრივ საკაბელო გარემოში. ამგვარად ისინი ამყარებენ რადიოკონტაქტს ქსელის კაბელიან ნაწილსა და გადასატან მოწყობილობებს შორის.

უგამტარო გარემო შეიძლება იყოს:

- ინფრაწითელი გამოსხივება Idra;
- ლაზერის სხივი;
- რადიოგადაცემა ვიწრო ზოლში;
- Bluetooth
- რადიოგადაცემა გაფანტული სპექტრით (WiFi).

IP-მისამართის დანიშნულება. კლასები და შესაბამისი ქვექსელის მასკები.

IP-მისამართი (აი-პი (IP) მისამართი, შემოკლ. ინგლ. Internet Protocol Address- ინტერნეტ ოქმის მისამართი) - ლოკალურ ქსელში ან ინტერნეტში ჩართული მოწყობილობის (როგორც წესი კომპიუტერის) უნიკალური იდენტიფიკატორია (მისამართია). IP-მისამართი წარმოადგენს 32-ბიტურ (IPv4 ვერსიით) ან 128-ბიტურ (IPv6 ვერსიით) ორნიშნა რიცხვს, რომელიც ჩაიწერება ოთხი ათობითი რიცხვის სახით (0-დან 255-მდე), დაყოფილს წერტილებით. მაგ., 192.168.0.1. (ან 128.10.2.30 – ათობითი ფორმაა, ხოლო ამავე მისამართის ორობითი ფორმაა – 10000000 00001010 00000010 00011110)
IP-მისამართი შედგება ორი ნაწილისგან: ქსელის ნომრისა და კვანძის ნომრისაგან. ქსელის ნომერი შეირჩევა ადმინისტრატორის მიერ ნებისმიერი ან Internet-ის (Internet Network Information Center, InterNIC) სპეციალური ქვეგანყოფილების რეკომენდაციების მიხედვით, თუ ქსელმა უნდა იმუშაოს, როგორც Internet-ის შემადგენელმა ნაწილმა. Internet-ის სერვისების მიმწოდებლები ჩვეულებრივ მისამრთების დიაპაზონს იღებენ InterNIC-გან და შემდგომ ანაწილებენ თავიანთ აბონენტებს შორის. მარშრუტიზატორი განსაზღვრების თანახმად შედის რამდენიმე ქსელში და ამიტომაც მის ყოველ პორტს გააჩნია საკუთარი IP-მისამართი. საბოლოო კვანძი შეიძლება შედიოდეს რამდენიმე IP-ქსელში. ამ შემთხვევაში კომპიუტერს უნდა გააჩნდეს რამდენიმე IP-მისამართი ქსელური კავშირების რიცხვის მიხედვით. მაშასადამე, IP-მისამართით ხასიათდება არა ერთი ცალკეული კომპიუტერი ან მარშრუტიზატორი, არამედ ერთი ქსელური შეერთება.
მისამართი შედგება ორი ლოგიკური ნაწილისგან - ქსელის ნომრისა და ქსელში კვანძის ნომრისგან. მისამართის თუ რომელი ნაწილი მიეკუთვნება ქსელის ნომერს და რომელი კვანძისას, განისაზღვრება მისამართის პირველი ბიტების მნიშვნელობებით. ამ ბიტების მნიშვნელობები კი განსაზღვრავენ თუ რომელ კლასს მიეკუთვნება ესა თუ ის IP-მისამართი.
გარდა IP მისამართისა კომპიუტერი ინტერნეტის ქსელში რომ ჩაირთოს საჭიროა მიენიჭოს სხვა TCP/IP პარამეტრები, ესენია: Subnet mask - ქვექსელის ნიღაბი, Default gateway - გასასვლელი, DNS სერვერი (DNS server).
ორ-დონიანი კლასობრივი დამისამართება მოიცავს ქსელისა და ჰოსტის იდენტიფიკატორებს. კლასობრივი დასაბნეტების (Subnetting, ქვექსელებად დაყოფის) შემთხვევაში, ქსელის იდენტიფიკატორი რჩება ცალკე, ხოლო ჰოსტისა კი იყოფა ქვექსელისა და ჰოსტის იდენტიფიკატორებად. ჰოსტის იდენტიფიკატორის ამ მეთოდით დაყოფისას ქვექსელების ნიღაბი და ჰოსტების რაოდენობა ყოველ ქვექსელში ყოველთვის ფიქსირებული რაოდენობისაა.
IP მისამართების უფრო ეფექტურად გამოსაყენებლად შეიქმნა უკლასო დომენებსშორისი მარშრუტიზაცია (Classless Inter-Domain Routing, CIDR).
CIDR-ის შემთხვევაში კლასები აღარ არსებობს.

სისტემური ადმინისტრატორი წყვეტს რამდენ ნაწილად და რა პორციით უნდა მოხდეს ქსელის დაყოფა ქვექსელად. მან უნდა იცოდეს რამდენი ქვექსელი არის საჭირო, ხოლო თითოეულ ქვექსელში რამდენი ჰოსტი. ნებისმიერი კლასის ქსელი იყოფა ქვექსელად. ქვექსელის მისამართი მოიცავს ქსელის პორციას პლიუს ქვექსელის და ჰოსტის ველი. ქვექსელის და ჰოსტის ველები იქმნება მთლიანი ქსელის ორიგინალური ჰოსტის პორციიდან. ქვექსელად დაყოფის შესაძლებლობა ქსელის ადმინისტრატორს აძლევს საშუალებას უფრო ადვილად გადაწყვიტოს დამისამართების პრობლემა.
ქვექსელის შესაქმნელად, ქსელის ადმინისტრატორი იღებს ბიტებს ჰოსტის ველიდან და გადასცემს ქვექსელის ველს. როდესაც იქმნება ქვექსელი და არ არის ნასესხები არცერთი ბიტი, მაშინ ფართომაუწყებლობითი მისამართი არის 255.
მაქსიმალურიბიტების რაოდენობა რომელიც შეიძლება იქნას ნასესხები ჰოსტის ნაწილიდან შეიძლება იყოს ნებისმიერი, ოღონდ ბოლო ბაიტში უნდა დარჩეს 2 ბიტი ჰოსტისთვის.
ქვექსელის ნიღაბი არის ის საშუალება რომელიც გამოიყენება ქვექსელის შესაქმნელად. ქვექსელის ნიღაბი აძლევს მარშუტიზატორს ინფორმაციას თუ რამდენი ბიტია ქსელის მისამართი და რამდენი ბიტია ჰოსტის მისამართი. ქვექსელის ნიღაბი არის 4 ბაიტიანი რიცხვი და იქმნება ბინარული ერთიანებით, რომელიც ლოგიკური გამრავლებით ედება IP მისამართს.

კომპიუტერული ქსელის დაპროექტება. ჩამოაყალიბეთ ძირითადი პრინციპები.

დაპროექტების ფუნდამენტური მიზნები

- მაშტაბურობა
- მუშაობის უნარიანობა
- დაცვა
- მართვა

ქსელის იერარქიული დაპროექტების ღირებულებები

იმისათვის, რომ დაკმაყოფილდეს დაპროექტების ოთხივე ფუნდამენტური მოთხოვნა, ქსელის არქიტექტურა უნდა იყოს მოქნილი და შესაძლებელი იყოს მისი გაფართოება.

ქსელების იერარქიული არქიტეტქურა გულისხმობს მოწყობილობების გაერთიანებას სხვადასხვა ქსელებში. ქსელების ორგანიზაცია გულისხმობს მის დონეებად დაყოფას. ქსელის იერარქიული დაპრორქტების მოდელი შედგება სამი ძირითადი დონისაგან:

- **ძირითადი დონე (Core Layer)** – აკავშირებს გამანაწილებელი დონის მოწყობილობებს
- **გამანაწილებელი დონე (Distribution Layer) –** აკავშირებს მცირე ლოკალურ ქსელებს
- **წვდომის დონე (Access Layer) –** უზრუნველყოფს კავშირს ჰოსტებთან და საბოლოო მოწყობილობებთან

ქსელის იერარქიული დაპროექტების უპირატესობები

CISCO-ს კორპორატიული არქიტექტურები იყენებს სამ დონიან იერარქიულ დიზაინს, რომელიც იყოფა მოდულებად. მოდულები წარმოადგენენ არეებს განსხვავებული ლოგიკური და ფიზიკური კავშირებით. მოდულებად დაყოფა ქსელის დიზაინს ხდის უფრო მოქნილს. რომელიც აადვილებს დანერგვასა და გაუმართაობების აღმოჩენას. მოდულურ ქსელის სამი ძირითადი არეებია:

- **კორპორატიული კამპუსი** – ეს არე შეიცავს ქსელის ელემენტებს დამოუკიდებელი მუშაობისათვის ცალკეული კამპუსის ან განყოფილების ფარგლებში.
- **სერვერების ჯგუფი** – კორპორატიული კამპუსის კომპონენტია. საინფორმაციო ცენტრის სერვერების ჯგუფი იცავს სერვერების რესურსებს და უზრუნველყოფს მათ დუბლირებული, საიმედო მაღალ-სიჩქარიანი კავშირით.
- **კორპორატიული საზღვარი** – ეს არე ფილტრავს გარედან შემოსულ ტრაფიკს და ამისამართებს კორპორატიულ ქსელში. ის შეიცავს ყველა ელემენტს ეფექტური და საიმედო კავშირისათვის კორპორატიულ კამპუსსა და დაშორებულ ადგილმდებარეობებს შორის, დაშორებულ მომხმარებლებს შორის და ინტერნეტთან.

მსხვილმაშტაბიანი ქსელის დაპროექტება მოიცავს სამ ძირითად ეტაპს:

1 ეტაპი: ქსელური მოთხოვნების განსაზღვრა.

- ქსელის დამპროექტებელი ითვალისწინებს მომხმარებლების მოთხოვნებს. მოთ-ხოვნები შეიძლება დაიყოს ორ კატეგორიად:
  • ბიზნეს მოთხოვნები – მიმართულია თუ როგორ გახადოს ქსელმა ბიზნესი უფრო წარმატებული
  • ტექნიკური მოთხოვნები – ფოკუსირებულია იმაზე თუ რა სახის ტექნოლოგია ინერგება ქსელში.
-

2 ეტაპი: არსებული ქსელის დახასიათება.

- ხორციელდება არსებული ქსელის სერვისების ანალიზი. აუცილებლად უნდა მოხდეს შედარება არსებული ქსელის ფუნქციონიერებასა და ახალი განსაზღვრული ქსელის პროექტს შორის. დამპროექტებლები განსაზღვრავენ თუ რომელი არსებული აპარატურა, ინფრასტრუქტურა და პროტოკოლები შეიძლება ხელახლა გამოყენებულ იქნას, და რა ახალი აპარატურა და პროტოკოლებია საჭირო იმისათვის, რომ დასრულდეს პროექტი.

3 ეტაპი: ქსელის ტოპოლოგიისა და ამოცანების განსაზღვრა.

- ქსელის დაპროექტების მთავარი სტრატეგიაა ზემოდან - ქვემოთ პრინციპი (top dawn), რომლის მიხედვითაც განისაზღვრება ქსელური პროცედურები და სერვისის მოთხოვნები, ხოლო შემდგომ დაპროექტებისას ქსელმა უზრუნველყოს ყველა ეს მოთხოვნა.

პროექტის დასრულების შემდეგ მიმდინარეობს შექმნილი ქსელის პროტოტიპის ტესტირება. რის შედეგადაც მოწმდება დაპროექტებული ქსელის ფუნქციონირება მის საბოლოო დანერგვამდე.

ადრესაცია IP-ქსელებში. TCP/IP სტეკის მისამართების ტიპები.

TCP/IP სტეკში გამოიყენება მისამართების სამი ტიპი: ლოკალური (ე.წ. აპარატურული) მისამართები, IP- მისამართები და სიმბოლური დომენური სახელები.

TCP/IP ტერმინოლოგიაში ლოკალური მისამართი - იგულისხმება მისამართის ტიპი, რომელიც გამოიყენება საბაზო ტექნოლოგიების საშუალებების მიერ ინფორმაციის გადასაცემად ქვექსელში, რომელიც წარმოადგენს შედგენილი ქვექსელის ელემენტს. სხვადასხვა ქვექსელებში გამოიყენება სხვადასხვა ქსელური ტექნოლოგიები, პროტოკოლების სხვადსხვა სტეკი, ამიტომაც TCP/IP სტეკის შექმნისას შემოღებულ იქნა ლოკალური მისამართების სხვადასხვა ტიპები.

ფიზიკური მისამართი. თუ ქვექსელი ლოკალური ქსელია მაშინ ლოკალურ (ფიზიკურ) მისამართს წარმოადგენს MAC-მისამართი. MAC-მისამართი განისაზღვრება ქსელური ადაპტერისა და მარშრუტიზატორების ქსელური ინტერფეისების საშუალებით. MAC-მისამართები განისაზღვრება მოწყობილობის მწარმოებლის მიერ და არის უნიკალური, რადგანაც მათი მართვა ხდება ცენტრალიზებულად. ლოკალური ქსელის ყველა არსებული ტექნოლოგიებისათვის MAC-მისამართს გააჩნია 6 ბაიტიანი (48 ბიტიანი) ფორმატი, მაგ.

11-A0-17-3D-BC-01. რადგან IP პროტოკოლს შეუძლია იმუშაოს უფრო მაღალი დონის პროტოკოლებთან, როგორიცაა IPX და X.25. ამ შემთხვევაში ლოკალური მისამართი IP პროტოკოლისათვის იქნება შესაბამისად IPX და X.25 მისამართები. უნდა გავითვალისწინოთ, რომ კომპიუტერს ლოკალური ქსელში შეიძლება ჰქონდეს რამდენიმე ლოკალური მისამართი ერთი ქსელური ადაპტერის შემთხვევაშიც. ზოგიერთ ქსელური მოწყობილობას არ გააჩნია ლოკალური მისამართი. მაგ., ასეთ მოწყობილობებია მარშრუტიზატორების გლობალური პორტები, რომლებიც დანიშნულია შესაერთებლად „წერტილი-წერტილი“.

IP-მისამართი წარმოადგენს მისამართების ძირითად ტიპს, რომლის საფუძველზეც ქსელური დონე აგზავნის პაკეტებს ქსელებს შორის. ეს მისამართები შედგება 4 ბაიტისგან, მაგ. 109.26.17.100. IP-მისამართი განისაზღვრება ადმინისტრატორის მიერ კომპიუტერისა და მარშრუტიზატორების კონფიგურაციისას. IP-მისამართი შედგება ორი ნაწილისგან: ქსელის ნომრისა და კვანძის ნომრისაგან. ქსელის ნომერი შეირჩევა ადმინისტრატორის მიერ ნებისმიერი ან Internet-ის (Internet Network Information Center, InterNIC) სპეციალური ქვეგანყოფილების რეკომენდაციების მიხედვით, თუ ქსელმა უნდა იმუშაოს, როგორც Internet-ის შემადგენელმა ნაწილმა. Internet-ის სერვისების მიმწოდებლები ჩვეულებრივ მისამრთების დიაპაზონს იღებენ InterNIC-გან და შემდგომ ანაწილებენ თავიანთ აბონენტებს შორის. მარშრუტიზატორი განსაზღვრების თანახმად შედის რამდენიმე ქსელში და ამიტომაც მის ყოველ პორტს გააჩნია საკუთარი IP-მისამართი. საბოლოო კვანძი შეიძლება შედიოდეს რამდენიმე IP-ქსელში. ამ შემთხვევაში კომპიუტერს უნდა გააჩნდეს რამდენიმე IP-მისამართი ქსელური კავშირების რიცხვის მიხედვით. მაშასადამე, IP-მისამართით ხასიათდება არა ერთი ცალკეული კომპიუტერი ან მარშრუტიზატორი, არამედ ერთი ქსელური შეერთება.

კომპიუტერული ქსელების მახასიათებლები, თანამედროვე ქსელების მიმართ წაყენებული მოთხოვნები.

ლოკალური ქსელების მუშაობის ეფექტურობის ასამაღლებლად საჭიროა გადავწყვიტოთ შემდეგი ამოცანები:

1. ჩამოვაყალიბოთ ქსელის ეფექტური მუშაობის კრიტერიუმები. ხშირ შემთხვევაში ასეთ კრიტერიუმებად გვევლინება წარმადობა და საიმედოობა. რომელთაც თავიანთ რიგში საჭიროა შეურჩიოთ კონკრეტული ხარისხობრივი მაჩვენებლები. მაგ: როგორიცაა რეაქციის დრო და მზადყოფნის კოეფიციენტი.
2. განვსაზღვროთ ვარირებადი (ცვლადები) პარამეტრების რაოდენობა. (სიმრავლე). რომლებიც პირდაპირ ან ირიბ გავლენას ახდენენ ეფექტურობის კრიტერიუმებზე. ყველა ასეთი პარამეტრი შეიძლება დაჯგუფებული იქნას სხვადასხვა სახით. მაგ: კონკრეტული პროტოკოლის (Ethernet–პროტოკოლის კადრის მაქსიმალური ზომა ან TCP–პროტოკოლში დაუდასტურებელი პაკეტების კადრის ზომა) ან მოწყობილობის პარამეტრები. (სამისამართო ცხრილის ზომა ან ბოგირის (bridge) ფილტრაციის სიჩქარე, მარშრუტიზატორის შიდა სალტის გამტარიანობა). პარამეტრებად შეიძლება ჩაითვალოს, როგორც თვითონ მოწ-ყობილობა, ასევე მთლიანად პროტოკოლი, მაგ: რომ გავაუმჯობესოთ შენელებული და გლობალური არხებით გადავსებული ქსელი საკმარისია გადავიდეთ პროტოკოლების IPX/SPX სტიკიდან TCP/IP-ზე. ასევე შეგვიძლია მივაღწიოთ საკმაო გაუმჯობესებას, თუ შევცვლით უცნობი მწარმოებლის მიერ შეთავაზებულ ადაპტერს ცნობილი ფირმის პროდუქციით;
3. განვსაზღვროთ მგრძნობიარობის ზღვარი ეფექტურობის კრიტერიუმის მნიშვნელობებისათვის.

ქსელის მუშაობა შეიძლება შევაფასოთ ლოგიკურად ”მუშაობს” – ”არ მუშაობს”, მაშინ ოპტიმიზაცია მიდის ქსელში დაზიანებების დიაგნოსტიკისაკენ, ისე, რომ ქსელმა ნებისმიერი შრომისუნარიანი მდგომარეობა მიიღოს.

შეფასების მეორე ფორმას წარმოადგენს ქსელის ზუსტი დაწყობა, სადაც მუშა ქსელის მახასიათებელი პარამეტრები იცვლება ქსელის წარმადობის ასამაღლებლად სულ მცირე რამდენიმე პროცენტით მაინც. როგორც წესი ქსელის ოპტიმიზაციის ქვეშ იგულისხმება ერთგვარი გარდამავალი ვარიანტი, რომლის არჩევის დროს საჭიროა მოიძებნოს ქსელის პარამეტრების ისეთი მნიშვნელობა, რომლებიც ეფექტურობის მაჩვენებლებს საგრძნობლად გააუმჯობესებს. მაგ: სერვერზე მოთხოვნა (მონაცემების გარეშე) გაგრძელდეს არა 10 წამი, არამედ 3 წამი და დაშორებულ კომპიუტერზე ფაილის გადაგზავნა გაგრძელდეს არა 2 წთ. არამედ 30 წამი. ასეთი სახით შეიძლება შევარჩიოთ ოპტიმიზაციის ამოცანის 3 სხვადასხვა ფორმა:

1. მოვიყვანოთ ქსელი შრომისუნარიან მდგომარეობაში. ის მოიცავს ქსელში დაზიანებული ელემენტების ძებნას. სადენები, მისამართები, ადაპტერები, კომპიუ-ტერები, აქვე მოწმდება მოწყობილობისა და პროგრამული საშუალებების თავსებადობა. ძირითადი პარამეტრებისათვის კორექტული მნიშვნელობების

შერჩევა, რომლებიც უზრუნველყოფენ შეტყობინების ქსელის ყველა კვანძში გატარებას, კადრების ტიპებისა და პროტოკოლების დაწყობას და ა.შ.

2. **უხეში დაწყობა** – ისეთი პარამეტრების დაწყობა, რომლებიც მკვეთრად ახდენენ გავლენას ქსელის მახასიათებლებზე. თუ ქსელი შრომისუნარიანია, მაგრამ მონაცემთა გაცვლა ხდება ძალიან ნელა, ანუ დაყოვნება ათეული წამი ან წუთი, ან კიდევ კავშირი ერთმანეთის შორის ხშირად წყდება გაუგებარი მიზეზით, ასეთ ქსელს შეიძლება შრომისუნარიანი დავარქვათ პირობითად. იგი საჭიროებს უხეშ დაწყობას. ამ ეტაპზე აუცილებელია ქსელში მოძრავი პაკეტების დაყოვნებების მიზეზის მოძებნა.

ძირითადად სერიოზულ შეყოვნებად ან ქსელის ცვალებად მუშაობის მიზეზად ითვლება ქსელის შემადგენელი ერთ-ერთი ელემენტის მწყობრიდან გამოსვლა ან პარამეტრების არაკორექტული დაყენება. თუ ქსელი დიდია, მის აღმოსაფხვრელად საკმაოდ დიდი დრო არის საჭირო, რადგან შესაძლო ვარიანტების რაოდენობა საკმაოდ დიდია. ნორმალური ქსელის (შრომისუნარიანი) მუშაობის დროს სერვერის რეაქცია მომხმარებლის მოთხოვნაზე არ უნდა აღემატებოდეს 5 წამს.

3. **ქსელის პარამეტრების ზუსტი დაწყობა (ოპტიმიზაცია).** თუ ქსელი მუშაობს დამაკმაყოფილებლად, მაშინ მისი წარმადობის და საიმედოობის ამაღლება მხოლოდ რომელიმე პარამეტრის შეცვლით ვერ მოხერხდება. ამ შემთხვევაში ქსელის მუშაობის ხარისხის ამაღლებისათვის საჭიროა მივაგნოთ ისეთი მახასიათებელი, რომელიც განაპირობებს სხვადასხვა პარამეტრების წარმატებულ შეთანხმებას.

ქსელის დაწვრილებითი დაწყობის დროს პარამეტრებს შორის ოპტიმალური შეთანხმების მიღწევა შეუძლებელია (სუფთა მათემატიკური გაგებით) და არც არის საჭირო დაიხარჯოს კოლოსალური ძალები მკაცრი ოპტიმიზაციის მისაღწევად, საკმარისია მოიძებნოს ოპტიმალურთან მიახლოებული შეთანხმება და ქსელის ოპტიმიზაციის ამოცანა შეიძლება გადაჭრილად ჩაითვალოს.

ასეთ გადაწყვეტილებებს რაციონალურ ვარიანტებს უწოდებენ და პრაქტიკაში ქსელის ადმინისტრატორებისათვის სწორედ ამ გადაწყვეტილების მიგნებაა ძირითადი პირობა.

საქსელო არქიტექტურები, Token Ring და FDDI. მარკერის მეთოდი. ზოგადი ანალიზი.

საქსელო არქიტექტურა Token Ring შემუშავებულია ფირმა IBM -ის მიერ. ქსელის ეს ვერსია ითვალისწინებს პერსონალური კომპიუტერების, საშუალო ელექტრონულ-გამომთვლელი მანქანებისა და მეინფრეიმერების (გიგანტური მანქანების) გაერთიანებას ერთიან ქსელში.

Token Ring-ის არქიტექტურა წარმოადგენს ANS/IEEE-ის სტანდარტს. სხვა ქსელებისაგან Token Ring განასახვავებს საკაბელო სისტემის გამოყენების თავისებურება და ქსელში შეღწევის მეთოდი მარკერის გამოყენებით.

მარკერი (Token) - ეს ბიტების წინასწარ განსაზღვრული თანმიმდევრობაა, სპეციალური დანიშნულების, გარკვეული სახის მონაცემების ნაკადია.

ქსელ Token Ring - გააჩნია შემდეგი ძირითადი მახასიათებლები:

ტოპოლოგია - ვარსკვლავი-რგოლი;

გადაცემის სახე - არამოდურილებული;

შეღწევის მეთოდი - მარკერის გადაცემით;

სპეციფიკა - IEEE802.5;

მონაცემების გადაცემის სიჩქარე - 4 და 16მგბტ/წმ;

საკაბელო გარემო - ეკრანირებული და არაეკრანირებული ხვეული წყვილი.

გავარჩიოთ Token Ring - ის ტოპოლოგიის თავისებურება. ამ არქიტექტურაში გარეგნულად საქმე გვაქვს ტოპოლოგია „ვარსკვლავთან“, ლოგიკურად კი იგი „რგოლია“. მომხმარებლები მიერთებულნი არიან სპეციალურ კონცენტრატორთან (MSAU ან MAU – Multistation Access Unit), როგორც ტოპოლოგია ვარსკვლავში, მაგრამ კონცენტრატორი ფიზიკურად რგოლის რეალიზებას ახდენს.

მარკერული წვდომის ქსელებში (Token Ring-ის გარდა მიეკუთვნება FDDI, ArcNet) გარემოზე წვდომის უფლება სადგურიდან სადგურს გადაეცემა ციკლურად ლოგიკური წრეში.

Token Ring ქსელებში ყოველი სადგური დაკავშირებულია მხოლოდ ორ მეზობელ სადგურთან და მხოლოდ მათთან შეუძლია გაცვალოს მონაცემები. სადგურის გარემოსთან წვდომის უზრუნველსაყოფად წრეში ცირკულირებს სპეციალური ფორმატისა და დანიშნულების კადრი - მარკერი.მარკერის მიღების შემდეგ სადგური ანალიზს უკეთებს მას და თუ არ გააჩნია მონაცემები, მაშინ მარკერი გადაეცემა შემდეგ სადგურს. სადგური კი, რომელმაც უნდა გადასცეს მონაცემები, მარკერის მიღებისას იღებს წრიდან მას, რაც გარემოსთან წვდომის და მონაცემების გადაცემის უფლებას აძლევს. შემდეგ ეს სადგური წრეში გადასცემს წინასწარ დადგენილი ფორმატის მონაცემთა კადრს ბიტობით თანმიმდევრულად. გადაცემული მონაცემები წრეში გაივლიან მხოლოდ ერთი და იგივე მიმართულებით ერთი სადგურიდან მეორემდე. კადრი შეიცავს მიმღებისა და გადამცემის მისამართებს.

FDDI (Fiber Distribused Data Interface) - განაწილებული მონაცემების ოპტობოჭკოვანი ინტერფეისი - ლოკალური ქსელების პირველი ტექნოლოგია, რომელშიც მონაცემების გადაცემის გარემოს ოპტიკურ-ბოჭკოვანი კაბელი წარმოადგენს. ამ ტექნოლოგიის გრძელი სახელწოდება ნაკლებად გამოიყენება, თვით შემოკლებულ აბრევიატურასაც FDDI (ანბანით ef-di-di-ai) იშვიათად იყენებენ, პრაქტიკულად გამოითქმება ერთი მთლიანი სიტყვის სახით „ფიდდი”.

სამუშაოები ისეთი ტექნოლოგიებისა და მოწყობილობების შესაქმნელად, რომლებიც ოპტიკურ-ბოჭკოვან კაბელებს გამოიყენებდნენ, დაიწყო მე-20 საკუნის 90-იან წლებში. FDDI ტექნოლოგია სტანდარტიზებული იქნა ANSI მიერ X3T9.5 სპეციფიკაციის სახით. FDDI სპეციფიკაციის დანიშნულება იყო მომსახურებოდა მაღალი წარმადობის მქონე კომპიუტერებს, რომელთათვისაც არსებული Ethernet ტექნოლოგიის 10მგბიტ/წმ და Tokenring-ის 16 მგბტ/წმ სიჩქარე უკვე მიუღებელი იყო.

FDDI ტექნოლოგია უკვე უზრუნველყოფდა მონაცემების გადაცემას 100 მგბტ/წმ სიჩქარით, გადაცემისათვის იყენებდა 100 კმ-იან ორ რგოლს და საშუალებას იძლეოდა რგოლში ჩართულიყო 500 კომპიუტერი.

ეს რგოლები ქმნიან მონაცემების გადაცემის ძირითად და სარეზერვო გზას ქსელის კვანძებს შორის. კომპიუტერები FDDI ქსელში შეიძლება მიერთებულნი იყვნენ როგორც ორივე რგოლთან, ასევე ერთმანეთთან. პირველ შემთხვევაში გვექნება A კლასის, მეორე შემთხვევაში კი B კლასის სადგური.

ორი რგოლის არსებობა - ეს არის მტყუნებამდგრადობის ამაღლების ძირითადი საშუალება FDDI ტექნოლოგიაში. კვანძები, რომლებიც დიდ იმედიანობას საჭიროებენ, მიერთებულნი უნდა იყვნენ ორივე რგოლთან, ე.ი. უნდა ქონდეთ A კლასის სადგურები (ნახ.6ა).

ქსელის მუშაობის ნორმალურ რეჟიმში მონაცემები გაივლიან ძირითადი (Primary) რგოლის ყველა კვანძსა და კაბელის ყველა უბანს, ხოლო სარეზერვო (Secondary) რგოლი ამ რეჟიმში არ გამოიყენება. რაიმე მტყუნების დროს (მაგალითად კაბელის გაწყვეტა ან კვანძის დაზიანება), როდესაც ძირითადი რგოლის რაღაც ნაწილი ვეღარ აწარმოებს მონაცემების გადაცემას, ძირითადი რგოლი ერთიანდება სარეზერვოსთან და კვლავ წარმოიქმნება ერთიანი რგოლი.

FDDI ტექნოლოგიის შედარება Ethernet და Token Ring ტექნოლოგიებთან

ცხრილში წარმოდგენილია FDDI ტექნოლოგიის შედარება Ethernet და Token Ring ტექნოლოგიებთან.

მახასიათებლები	FDDI (IEEE 802.2)	Ethernet (IEEE 802.3/u/z)	Token Ring (IEEE 802.5)
სიჩქარე	100მბიტ/წმ	10/100/1000მბიტ/წმ	4/16მბიტ/წმ
ტოპოლოგია	ხეების ორმაგი წრე	სალტე/ვარსკვლავი	ვარსკვლავი/წრე
მონაცემთა გადაცემის გარემო	ოპტიკურ-ბოჭკოვანი, მე-5 კატეგორიის არაეკრანირებული ხვეული წყვილი	მსხვილი კოაქსია-ლური, წვრილი კოაქსიალური, მე-3,5,6 კატეგორიის ხვეული წყვილი, ოპტიკურ-ბოჭკოვანი	ეკრანირებული და არაეკრანირებული ხვეული წყვილი, ოპტიკური ბოჭკო
წვდომის მეთოდი	მარკერის უკუ დროის ნაწილი	CSMA/CD	დარეზერვების პრიორიტეტული სისტემა
ქსელის მაქსიმალური სიგრძე (ხიდების გარეშე)	200 კმ (100 კმ რგოლზე)	2500 მ	1000 მ
მაქსიმალური სიგრაძე კვანძებს შორის	2 კმ (-11 dB დაწაკარი კვანძებს შორის)	2500 მ	100 მ
კვანძების მაქსიმალური რაოდენობა	500 (1000 კავშირი)	1024	260 ეკრანირებული/ 72 არ ეკრანირებული გრეხილი წყვილისთვის
ტაქტირება და აღდგენა მტყუნების შემდეგ	განაწილებული რეალიზაცია, ტაქტირება და აღდგენა მტყუნების შემდეგ	არ არის განსაზღვრული	აქტიური მონიტორი

კომპიუტერული ქსელის უსაფრთხოების პრინციპები. FireWall-ი.

უსაფრთხოების პოლიტიკა (security policies) - უსაფრთხოების სფეროში პრინციპების, წესების, პროცედურების და პრაქტიკული ღონისძიებების ერთობლიობაა, რომელებიც არეგულირებენ ძვირადღირებული ინფორმაციის მართვას, დაცვას და განაწილებას. უსაფრთხოების პოლიტიკა უნდა იყოს ცენტრალური წერტილი იმისათვის თუ როგორ დავიცვათ ქსელი, მოვახდინოთ მისი მონიტორინგი, ტესტირება და მისი გაუმჯობესება. სახლის მომხმარებლები არ სარგებლობენ ამ პოლიტიკით და რადგანაც ქსელი იზრდება, ამ პოლიტიკის აუცილებლობაც საგრძნობლად იზრდება.

უსაფრთხოების პოლიტიკის შემავალი ძირითადი ასპექტებია:

- იდენტიფიკაციისა და აუტენტიფიკაციის პოლიტიკა
- პაროლების პოლიტიკა,
- ქსელით სარგებლობის პოლიტიკა
- დისტანციური წვდომის პოლიტიკა
- ქსელის ექსპლუატაციის პოლიტიკა
- ინციდენტების მართვის პროცედურები.

გარდა იმისა, რომ მნიშვნელოვანია დაცული იყოს კომპიუტერები და სერვერები, რომლებიც დაკავშირებული არიან ქსელთან, არანაკლებ მნიშვნელოვანია ქსელში მოსეირნე ტრაფიკის მართვა და კონტროლი.

Firewall არის ყველა ეფექტური დაცვის საშუალება, რომელიც იცავს შიდა ქსელის მომხმარებლებს გარე შემოტევებისაგან. Firewall იმყოფება ქსელებს შორის და მართავს და აკონტროლებს ტრაფიკს მათ შორის. აღმოფხვრის არასანქცინირებულ წვდომას ქსელთან. Firewall იყენებს სხვადასხვა მეთოდებს იმის განსასაზღვრავად თუ რომელი წვდომაა ქსაელთან ნებადართული ან შეზღუდული.

- **პაკეტის ფილტრაცია** - აღმოფხვრის ან აძლევს წვდომის საშუალებას IP და MAC მისამრთებზე დაყრდნობით.
- **პროგრამის/ Web Site-ის ფილტრაცია** - აღმოფხვრის ან აძლევს წვდომის საშუალებას პროგრამებზე დაყრდნობით. Web Site შეიძლება დაიბლოკოს WebSite-ის URL მისამართების ან ძირითადი სიტყვების (keywords)მიხედვით.

- **Stateful Packet Inspection (SPI) (პაკეტის მდგომარეობის შემოწმება)** - შემომავალი პაკეტები გასცემენ ლეგიტიმურ პასუხებს შიდა ჰოსტების მოთხოვნებზე. არასასურველი პაკატები იბლოკება სპეციალური ნებართვის გარეშე. SPI -ის შეუძლია აგრეთვე ამოიცნოს და გაფილტროს DoS შემოტევებიც.

Firewall პროდუქტები უზრუნველყოფენ ერთ ან მეტი სახის ფილტრაციის საშუალებებს. დამატებით Firewall-ს შეუძლიათ აგრეთვე ქსელური მისამართის გარდაქმნა (Network Address Translation (NAT)). NAT გარდაქმნის შიდა მისამართს ან მისამრთების ჯგუფს გარე მისამრთად, რომელიც იგზავნება ქსელში. რის შედეგადაც შიდა IP მისამრთები მიუწვდომელია გარე მომხმარებლებისათვის.

ფაიერვოლის კონფიგურირება შეიძლება მოხდეს შემდეგი პრინციპების მიხედვით:

ა. დაშვებულია ის, რაც არ არის აკრძალული.

ბ. აკრძალულია ის, რაც არ არის დაშვებული.