ო. შონია, გ. ნარეშელაშვილი,
ი. ქართველიშვილი

უმავთულო ქსელების უსაფრთხოება

„ტექნიკური უნივერსიტეტი”

საქართველოს ტექნიკური უნივერსიტეტი

ო. შონია, გ. ნარეშელაშვილი,
ი. ქართველიშვილი

უმავთულო ქსელების უსაფრთხოება

დამტკიცებულია სტუ-ს
სარედაქციო-საგამომცემლო
საბჭოს მიერ

თბილისი
2009

ᲣᲓᲙ 681.3

სახელმძღვანელოში მოყვანილია ძირითადი ცნობები უმავთულო კომპიუტერული ქსელების ტექნოლოგიებისა და კომპონენტების შესახებ. განხილულია უმავთულო ქსელების ყველა ნაირსახეობა (პერსონალური, ლოკალური, რეგიონალური და გლობალური), აღწერილია მათი სტრუქტურის თავისებურებები და გამოყენების მეთოდები. განსაკუთრებული ყურადღება გამახვილებულია უმავთულო ქსელების უსაფრთხოების საკითხებზე. აღწერილია აუტენტიფიკაციისა და დაშიფვრის მექანიზმები.

სახელმძღვანელო განკუთვნილია ინფორმატიკის სპეციალობის სტუდენტებისათვის, აგრეთვე მაგისტრანტებისა და მეცნიერ-მუშაკებისთვის.

რეცენზენტი პროფ. **გ. სურგულაძე**

ISBN 978-9941-14-308-3
http://www.gtu.ge/publishinghouse/

შ ი ნ ა ა რ ს ი

შესავალი

უკვე რამდენიმე ათეული წელია, რაც ადამიანები იყენებენ კომპიუტერულ ქსელებს, რომლებიც უზრუნველყოფს კავშირს მომსახურე პერსონალს, კომპიუტერებსა და სერვერებს შორის. მიუხედავად ამისა, უფრო და უფრო იგრძნობა ტენდენცია იმისა, რომ ფართოდ იქნას გამოყენებული უმავთულო ქსელები. დღევანდელ რეალობაში ხელმისაწვდომია უმავთულო ინტერ-ფეისები, რომლებიც იძლევა ქსელური მომსახურეობების გამოყენების საშუალებას. მაგალითად, მომხმარებელს შეუძლია ელექტრონულ ფოსტასთან მუშაობა და WEB-გვერდების დათვა-ლიერება, დამოუკიდებლად იმისა, თუ სად იმყოფება იგი.

უმავთულო ქსელები ადამიანებს საშუალებას აძლევს გააფართოვონ თავიანთი სამუშაო ადგილები და ამის შედეგად მიიღონ ბევრი უპირატესობა. მომხმარებელთა უმრავლესობას, პერსონალური კომპიუტერებისა და ნოუთბუქების საშუალებით, მარტივად შეუძლია გამოიყენოს საერთო ინტერნეტ-კავშირები ყოველგვარი მავთულების გაყვანის გარეშე. სწორედ უმავთულო ქსელების კომპონენტებზე და ტექნოლოგიებზე, და მათ უსაფრთხოებაზე, რაც ასეთი სისტემების რეალიზების საშუალებას იძლევა, იქნება საუბარი.

თავი I. უმავთულო სამყარო

უმავთულო ქსელები ადამიანების ცხოვრებაში, სადაც არ უნდა იმყოფებოდნენ ისინი – სამსახურში, სახლში ან საზოგადოებრივი თავშეყრის ადგილებში, დიდ როლს თამაშობს. თუნდაც მაშინ, როცა უმავთულო ქსელი იქმნება მარტივი მიზნით – უზრუნველყოს კავშირი ადამიანსა და ინფორმაციის წყაროს შორის მავთულების გამოყენების გარეშე, საჭიროა გავერკვეთ უმავთულო ქსელების ძირითად კონცეფციაში, განვიხილოთ ძირითადი განსაზღვრებანი, შემდეგ კი ვნახოთ, თუ როგორ მუშაობს ისინი და რა სარგებლობა შეუძლია მოიტანოს ამა თუ იმ შემთხვევებში.

1.1. უმავთულო ქსელების კლასიფიკაცია

უმავთულო ქსელები ადამიანებს საშუალებას აძლევს დაუკავშირდნენ და მიიღონ კავშირის ნებართვა სხვადასხვა სისტემასთან და ინფორმაციასთან, შეამოწმონ ელექტრონული ფოსტა და დაათვალიერონ WEB-გვერდები, ყოველგვარი მავთულების გამოყენების გარეშე, მიუხედავად იმისა, თუ სად

იმყოფება ადამიანი – შენობის გარეთ, ქალაქგარეთ ან მსოფლიოს ნებისმიერ წერტილში.

უმავთულო ქსელები მრავალი წელია არსებობს ჩვენს გარშემო. უმავთულო კავშირის პრიმიტიულ ფორმას შეიძლება მივაკუთვნოთ გემებს შორის მორზეს ანბანით ინფორმაციის გადაცემა სპეციალური შუქურების საშუალებით (ასეთი მეთოდი იყო და რჩება ზღვაში ინფორმაციის გადაცემის ძირითად ფორმად). რა თქმა უნდა, პოპულარული მობილური ტელეფონები, რომლებიც ადამიანებს საშუალებას აძლევს დიდ მანძილზე დაამყრონ ერთმანეთთან კავშირები, აგრეთვე შეიძლება მივაკუთვნოთ უმავთულო კავშირების ჯგუფს.

არსებობს უმავთულო კავშირების სხვადასხვა სახეობა, მაგრამ უმავთულო ქსელების ძირითად თავისებურებად ითვლება ის, რომ კავშირი მყარდება კომპიუტერულ მოწყობილობებს შორის. ასეთებს მიეკუთვნება: პერსონალური ციფრული დამხმარეები *(Personal digital assistance, PDA)*, ნოუთბუქები, პერსონალური კომპიუტერები, სერვერები და პრინტერები. კომპიუტერულ მოწყობილობებში იგულისხმება ისეთები, რომელსაც გააჩნია პროცესორები, მეხსიერება და რომელიმე ქსელთან რეაგირების საშუალება. საერთოდ, მობილური ტელეფონები არ მიეკუთვნება კომპიუტერული მოწყობილობების რიცხვს, მაგრამ უახლეს ტელეფონებს გააჩნია განსაზღვრული გამოთვლითი საშუალებები და ქსელური ადაპტერები. აქედან გამომდინარე, ყველაფერი მიდის იმისკენ, რომ უახლოეს მომა-

ვალში ელექტრონული მოწყობილობების უმრავლესობა აღიჭურვება უმავთულო ქსელებში ჩართვის შესაძლებლობებით.

როგორც ჩვეულებრივი ქსელები, რომლებიც დაფუძნებულია მავთულების გამოყენებაზე, ასევე-უმავთულო ქსელებიც, ინფორ-მაციას გადასცემს კომპიუტერულ მოწყობილობებს შორის. ეს ინფორმაცია შეიძლება წარმოდგენილი იქნას სხვადასხვა სახით: ელექტრონული ფოსტა, WEB-გვერდი, მონაცემთა ბაზების ჩანაწერები, ვიდეოს ნაკადი ან ხმოვანი შეტყობინება. უმრავლეს შემთხვევაში უმავთულო ქსელები მონაცემებს *(data)* გადასცემს ელექტრონული ფოსტის საშუალებით და ფაილების სახით. უმავთულო ქსელების მახასიათებლების გაუმჯობესებასთან დაკავშირებით, შესაძლებელია ვიდეოსიგნალების გადაცემა, აგრეთვე- სატელეფონო კავშირების უზრუნველყოფა.

მომხმარებლების, სერვერებისა და მონაცემთა ბაზების ურთიერთქმედების უზრუნველსაყოფად უმავთულო ქსელები, როგორც გადამცემი საშუალება, იყენებს რადიოტალღებს ან ინფრაწითელ (ᲘᲬ) დიაპაზონს. ინფორმაციის გადაცემის ეს არეალი უხილავია ადამიანისათვის. დღეისათვის მწარმოებლების უმრავლესობა ქსელური ინტერფეისის პლატებს *(network interface card, NIC)*, რომლებიც ქსელური ადაპტერების სახითაა ცნობილი, და ანტენებს კომპიუტერულ მოწყობილობებში ინტეგრირებას უკეთებენ ისეთი სახით, რომ ისინი შეუმჩნეველია მომხმა-რებლებისათვის. ყოველივე ეს უმავთულო მოწყობილობას უფრო მობილურს და მოხერხებულს ხდის გამოყენებაში.

უმავთულო ქსელებს, რომლებიც უზრუნველყოფს კავშირს სხვადასხვა ზომის ფიზიკურ ზონაში, ყოფენ სხვადასხვა კატეგორიებად:

- უმავთულო პერსონალური ქსელი *(wireless personal-area network, PAN)*;
- უმავთულო ლოკალური ქსელი *(wireless lokal-area network, LAN)*;
- უმავთულო რეგიონალური ქსელი *(wireless metropolitan-area network, MAN)*;
- უმავთულო გლობალური ქსელი *(wireless wide-area network, WAN)*;

(ცხრილი 1.1)-ში მოცემულია უმავთულო ქსელების ნაირსახეობების მოკლე აღწერა. უმავთულო ქსელების ყველა სახეობას გააჩნია თავისებურებები, რისი წყალობითაც დაკმაყოფილებულია თითოეულისადმი წაყენებული სხვადასხვა მოთხოვნა.

ცხრილი 1.1. უმავთულო ქსელების ნაირსახეობები

სახეობა	**მოქმედების სფერო**	**თვისებები**	**სტანდარტი**
უმავთულო პერსონალური ქსელი	მომხმარებელთან უშუალო სიახლოვე	საშუალო	Bluetooth, IEEE 802.15, IRDA
უმავთულო ლოკალური ქსელი	შენობის ფარგლებში	უმაღლესი	IEEE 802.11 Wi-Fi
უმავთულო რეგიონალური ქსელი	ქალაქის ფარგლებში	უმაღლესი	IEEE 802.16
უმავთულო გლობალური ქსელი	მთელ მსოფლიოში	დაბალი	ფიჭური სისტემები

1.1.1. უმავთულო პერსონალური ქსელები

უმავთულო პერსონალური ქსელები გამოირჩევა ინფორ-მაციის პატარა მანძილზე გადაცემით (17 მეტრამდე), რაც მათ იდეალურს ხდის შენობის პატარა ტერიტორიაზე ან „პერსონალურ ზონაში“ გამოსაყენებლად(ნახ. 1.1). უმავთულო პერსონალური ქსელების თვისებები არის საშუალო, ინფორმაციის გადაცემის სიჩქარე არ ცილდება 2 მბ/წ-ს. ბევრ სიტუაციაში უმავთულო პერსონალური ქსელები წარმატებით ცვლის მავთულიან ქსელებს.

ნახ. 1.1. უმავთულო პერსონალური ქსელი უზრუნველყოფს კომპიუტერულ მოწყობილობებს შორის ინფორმაციის გადაცემას პატარა მანძილზე

ასეთი სახის ქსელს შეუძლია უზრუნველყოს, მაგალითად, მონაცემთა უმავთულო სინქრონიზაცია PDA მომხმარებელზე და მის პერონალურ კომპიუტერზე ან ნოუთბუქზე. ანალოგიურად შესაძლებელია უმავთულო კავშირი პრინტერთან. კომპიუტერულ მოწყობილობებს შორის მავთულიანი ქსელებით შეერთების უმავთულო ქსელებით შეცვლა მეტად სერიოზული უპირატესობაა, რაც მნიშვნელოვნად აადვილებს კომპიუტერული მოწყობილობების სამონტაჟო სამუშაოებს აუცილებლობის შემთხვევაში მათი სხვა ადგილას გადატანის დროსაც.

უმავთულო პერსონალური ქსელების მიმღებ-გადამცემების *(transceiver)* უმეტესობა გამოირჩევა კომპაქტური ზომით და სჭირდება მცირე სიმძლავრე, რაც მათ ეფექტურს ხდის პატარა სამომხმარებლო მოწყობილობებთან მიმართებაში, აგრეთვე საშუალებას აძლევს კომპიუტერულ მოწყობილობებს დიდი ხანი იმუშაოს ერთ ბატარეაზე. ყოველივე ეს მომხმარებელს იცავს აკუმულატორის ხშირად დატენვისაგან. გარდა ამისა, მცირე გამოყენებადმა სიმძლავრემ განაპირობა უმავთულო პერსონალური ქსელების წარმატებით დანერგვა მობილურ ტელეფონებში და PDA-ში. ტელეფონს შეუძლია უწყვეტად ურთიერთქმედებდეს PDA-ს სატელეფონო წიგნთან. სევე, ტელეფონზე საუბრის ან მუსიკის მოსმენისას, რომელიც ციფრული სახითაა ჩაწერილი PDA-ზე, შესაძლებელია გამოყენებული იქნეს ყურსასმენები. ყოველივე ეს შესაძლებელია მავთულების გამოყენების გარეშე.

უმავთულო პერსონალურ ქსელებს შეუძლია უზრუნველყოს ნოუთბუქებისა და პერსონალური კომპიუტერების ურთიერთქმედება იმ მიზნით, რომ ერთობლივად ჩაერთონ ინტერნეტში. ასეთი ქსელების მოქმედების არეალი განისაზღვრება ერთი ოთახით.

უმავთულო პერსონალური ქსელების უმრავლესობაში ინფორმაციის გადაცემისათვის გამოიყენება რადიოტალღები. ასეთი სპეციფიკაციით, რომელიც დაფუძნებულია Bluetooth-ზე, რეგლა-მენტირებულია უმავთულო პერსონალური ქსელების მუშაობა 2,4 გჰ დიაპაზონზე, მაძნილი - 17 მეტრამდე, გადაცემის სიჩქარე – 2მბ/წ.

უმავთულო პერსონალური ქსელებისთვის სტანდარტად ითვლება 802.15. აშშ-ს ცნობილმა საინჟინრო ინსტიტუტებმა ელექტროტექნიკისა და ელექტრონიკის დარგში *(Institute of Electrical and Electronics Engineers, IEEE)* თავიანთ სტანდარტ 802.15-ში უმავთულო პერსონალური ქსელებისთვის ჩართეს სპეციფიკაცია Bluetooth. ასეთი ტექნოლოგია უზრუნველყოფს საიმედო და ხანგრძლივ გადაწყვეტას ისეთი კომპიუტერული მოწყობილობებისთვის, რომლებიც შეერთებულია პატარა ზონაში, მცირე მანძილზე.

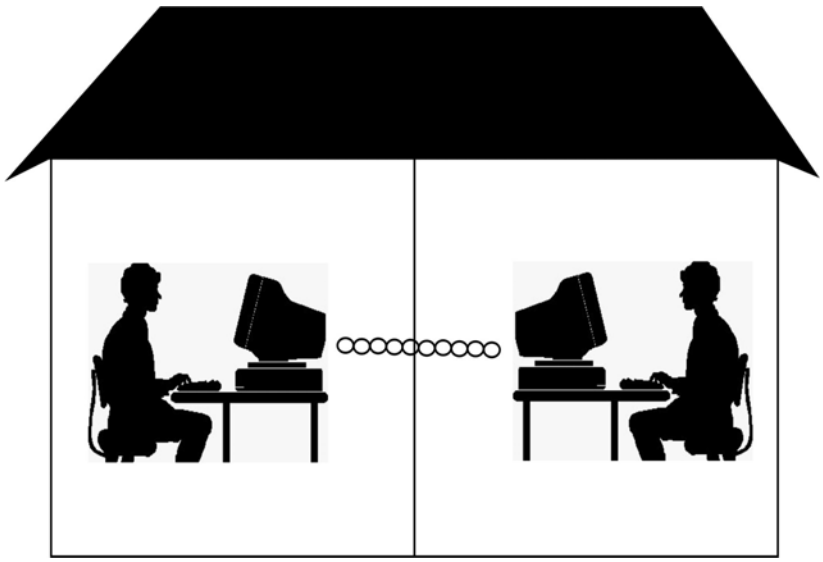
ზოგიერთ უმავთულო პერსონალურ ქსელებში ინფორმაციის ერთი წერტილიდან მეორეში გადასაცემად გამოიყენება (ᲘᲬ) გამოსხივება. ასეთი სპეციფიკაცია, რომელიც დაფუძნებულია (ᲘᲬ) დიაპაზონზე *(Infrared Data Association, IrDA)*, რეგლამენტირებას უკეთებს მიმართული (ᲘᲬ) სხივების გამოყენებას ინფორმაციის 1

მეტრამდე მანძილზე გადასაცემად, გადაცემის სიჩქარე – 4მბ/წ. ასეთი ხერხით ინფორმაციის გადაცემის უპირატესობა არის ის,რომ იცავს მას რადიოხარვეზებისგან, მაგრამ კომპიუტერული მოწყობილობების განლაგება აუცილებელია ერთმანეთის პირისპირ ახლო მანძილზე.

უმავთულო პერსონალური ქსელების ტექნოლოგიებისა და კომპონენტების შესახებ დაწვრილებით იქნება საუბარი II თავში.

1.1.2. უმავთულო ლოკალური ქსელები

უმავთულო ლოკალური ქსელები გამოირჩევა მაღალი თვისებებით. ის უზრუნველყოფს ინფორმაციის გადაცემას ოფისში და ოფისს გარეთ, რომელიც განლაგებულია ერთ დიდ შენობაში (ნახ. 1.2). ასეთი ქსელების მომხმარებლები ჩვეულებრივ იყენებენ PDA-ებს, ნოუთბუქებს და პერსონალურ კომპიუტერებს დიდი ეკრანებით და პროცესორებით, რომლებსაც გააჩნიათ დიდ სისტემებთან მუშაობის უნარი. ასეთი ქსელები სრულიად აკმაყოფილებს მოთხოვნებს, რომლებიც წაყენებულია ასეთი ტიპის კომპიუტერული მოწყობილობების შეერთების პარამეტრებისადმი.



ნახ. 1.2. უმავთულო ლოკალური ქსელები უზრუნველყოფს კომპიუტერულ მოწყობილობებს შორის ინფორმაციის გადაცემას შენობის ფარგლებში

მთელ რიგ ორგანიზაციებში, მაგალითად, უმავთულო ლოკალური ქსელი გამართულია იმ მიზნით, რომ მან უზრუნველყოს ნოუთბუქებიდან წვდომა კორპორატიულ სისტემებზე. ასეთი სახის სისტემებში მომხმარებელს, რომელიც,ვთქვათ, იმყოფება საკონფერენციო დარბაზში ან შენობის სხვა ადგილას, თავისუფლად შეუძლია გამოიყენოს ქსელური მომსახურეობები, რომელიც ეხმარება მას თავისი ვალდებულებების ეფექტურად შესრულებაში.

უმავთულო ლოკალური ქსელები მარტივად უზრუნველყოფს იმ თვისებებს, რომლებიც აუცილებელია მაღალი დონის სისტემების უწყვეტად შესრულებისათვის. ასეთი ქსელის მომხმარებლებს სერვერიდან შეუძლიათ მიიღონ დიდი მოცულობის ელექტრონული ფოსტა ან ვიდეოს ნაკადი. 54 მბ/წ სიჩქარით გადაცემის დროს უმავთულო ლოკალური ქსელები სრულიად აკმაყოფილებს ყველა საოფისე სისტემის მოთხოვნებს.

უმავთულო ლოკალური ქსელები თავისი თვისებებით, კომპონენტებით და ოპერაციების შესრულებით წააგავს Ethernet-ის ტიპის ტრადიციულ მავთულიან ლოკალურ ქსელებს. დღეს-დღეობით უმავთულო ლოკალური ქსელების ადაპტერები ნოუთბუქების უმრავლესობაშია ჩაშენებული.

უმავთულო ლოკალური ქსელებისთვის სტანდარტი არის IEEE 802.11. არსებობს ამ სტანდარტის სხვადასხვა ვერსია, რომელიც ინფორმაციის გადაცემას უზრუნველყოფს 2,4 და 5 გჰ დიაპაზონში. ასეთი სტანდარტის ძირითადი პრობლემა მდგომარეობს იმაში, რომ იგი ვერ უზრუნველყოფს სხვადასხვა ვერსიის მქონე კომპიუტერული მოწყობილობების ურთიერთ-ქმედებას. მაგალითად, კომპიუტერული მოწყობილობის ადაპტერები, რომლებიც შეესაბამება 802.11a სტანდარტის უმავთულო ლოკალურ ქსელებს, ვერ უკავშირდება კომპიუტერულ მოწყობილობებს, რომლებიც შეესაბამება 802.11b სტანდარტს. არსებობს კიდევ სხვა პრობლემები ამ სტანდარტთან

დაკავშირებით, როგორიცაა, მაგალითად, უსაფრთხოების არასაკმარისი ზომები.

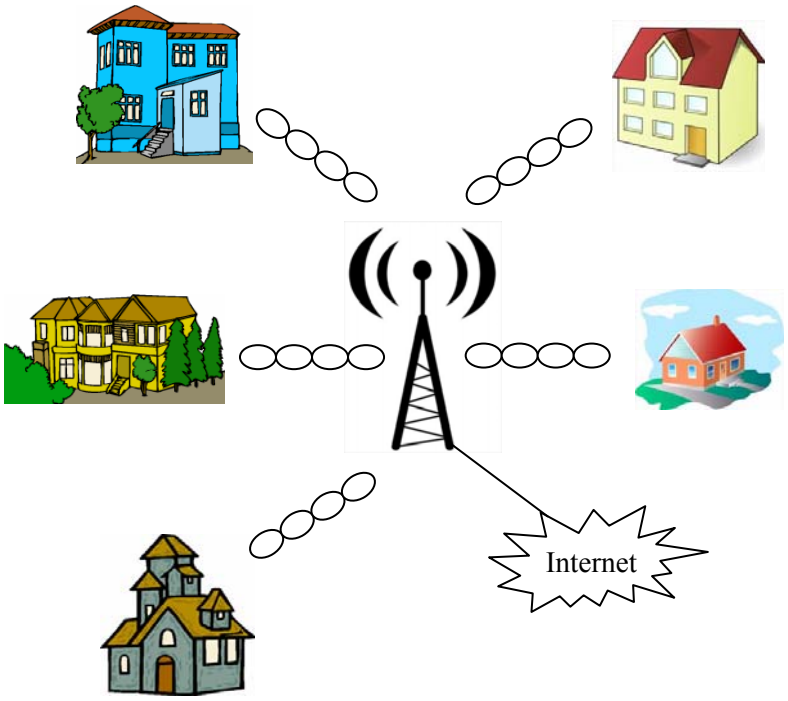
იმისათვის, რომ მოიხსნას 802.11 სტანდარტთან დაკავშირებული ზემოაღნიშნული პრობლემები, ორგანიზაციამ "ალიანსი Wi-Fi" ყველა შესაბამისი ფუნქცია შეიყვანა ერთ სტანდარტში, რომელიც ცნობილია სახელწოდებით – Wireless Fidelity *(Wi-Fi)*. აქედან გამომდინარე, თუ რომელიმე კომპიუტერული მოწყობილობა შეესაბამება სტანდარტ Wi-Fi-ს, მაშინ მათი ურთიერთქმედება გარანტირებულია.

უმავთულო ლოკალური ქსელების ტექნოლოგიებისა და კომპონენტების შესახებ დაწვრილებით იქნება საუბარი III თავში.

1.1.3. უმავთულო რეგიონალური ქსელები

უმავთულო რეგიონალური (ქალაქური) ქსელები ემსახურება ქალაქში შემავალ ზონებს. უმრავლეს შემთხვევაში სისტემის რეალიზაციის დროს საჭიროა ფიქსირებული შეერთება. მაგალითად, საავადმყოფოში ასეთი ქსელი უზრუნველყოფს ძირითად კორპუსსა და მოცილებულ კლინიკებს შორის მონაცემთა გადაცემას. ასევე, ენერგეტიკულ კომპანიას ქალაქის მასშტაბით შეუძლია გამოიყენოს ასეთი ტიპის ქსელები ძირითად შენობასა და

მოცილებულ ენერგეტიკულ პუნქტებს შორის დასაკავშირებლად. შედეგად, უმავთულო რეგიონალური ქსელები დააკავშირებს არსებულ ქსელურ ინფრასტრუქტურებს, ან საშუალებას მისცემს მობილურ მომხმარებლებს დაუკავშირდნენ უკვე არსებულ ქსელურ ინფრასტრუქტურას (ნახ. 1.3).



ნახ. 1.3. უმავთულო რეგიონალური ქსელები ქალაქის მასშტაბით უზრუნველყოფს მოცილებული შენობების კავშირს ინტერნეტთან

უმავთულო ინტერნეტის მომსახურების მომწოდებლები *(Wireless Internet Service Provider, WISP)* მომხმარებლებს ქალაქის მასშტაბით წარმოუდგენენ უმავთულო რეგიონალურ ქსელებს, რომლებიც უზრუნველყოფს მუდმივ უმავთულო კავშირს მოცილებულ შენობებს შორის. მსგავს ქსელებს გააჩნია არსებითი უპირატესობა ჩვეულებრივ მავთულიან ქსელებთან შედარებით, როგორიცაა,მაგალითად, ციფრული სააბონენტო ხაზები *(Digital Subscriber Line, DSL)*, ვინაიდან ხშირ შემთხვევაში მისი დამონტაჟება დიდ ეკონომიურ ხარჯებთანაა დაკავშირებული.

უმავთულო რეგიონალური ქსელების თვისებები სხვადასხვაა. კავშირს, რომელიც იყენებს (**ᲘᲕ**) ტექნოლოგიას, შეუძლია უზრუნველყოს ინფორმაციის გადაცემა სიჩქარით – 100 გბ/წ და მეტიც, ხოლო რადიოარხების შემთხვევაში გადაცემის სიჩქარეა 100 კბ/წ. თვისებები დამოკიდებულია იმაზე, თუ რა არჩევანი გაკეთდა სხვადასხვა ტექნოლოგიიდან და კომპონენტიდან.

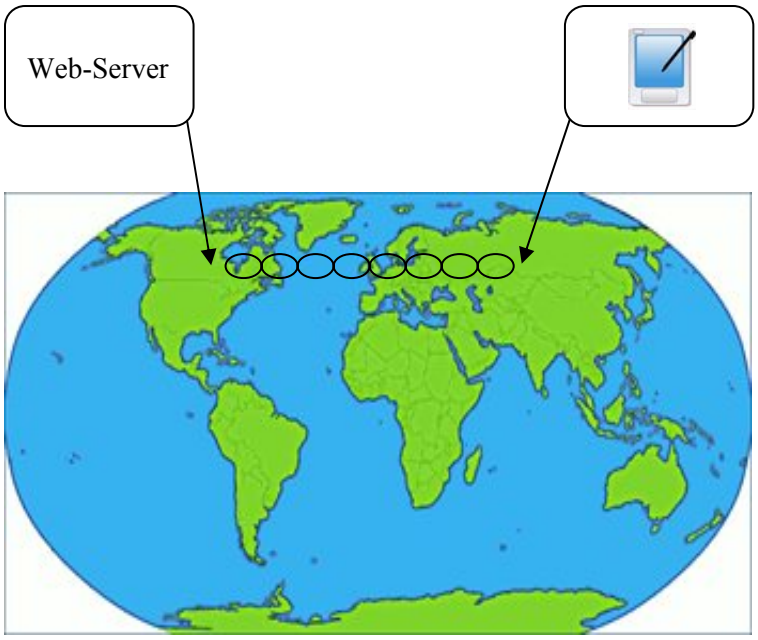
სამომხმარებლო ბაზარი გვთავაზობს სხვადასხვა დაპატენტებულ გადაწყვეტილებას უმავთულო რეგიონალური ქსელებისთვის, მაგრამ მწარმოებლები ყოველთვის ეყრდნობიან სტანდარტებს. ზოგიერთები მომწოდებელი იყენებს სტანდარტ 802.11 უმავთულო რეგიონალური ქსელების შექმნისთვის, მაგრამ ასეთი სტანდარტის სისტემები ოპტიმალურია და აკმაყოფილებს მოთხოვნებს შენობის შიგნით. მათ შეუძლია შენობის გარეთ კავშირის დამყარება მიმართული ანტენების დახმარებით.

დღეისათვის კომპანიების უმრავლესობა ირჩნევს სისტემებს სტანდარტით IEEE 802.16. ეს შედარებით ახალი სტანდარტია. დიდი ხანი არ არის, რაც ამ სტანდარტის შესაბამისი პროდუქცია გამოჩნდა ბაზარზე.

1.1.4. უმავთულო გლობალური ქსელები

უმავთულო გლობალური ქსელები უზრუნველყოფს ინფორმაციასთან წვდომას ქვეყნისა და კონტინენტის მასშტაბით. თუ ვიხელმძღვანელებთ ეკონომიკური გათვლებით, სატელეკომუნიკაციო კომპანიები დანერგავენ ძვირადღირებულ უმავთულო გლობალური ქსელების ინფრასტრუქტურას, რომელსაც შეეძლება უზრუნველყოს უამრავ მომხმარებელსს შორის კავშირი დიდ მანძილზე. ასეთი დანერგვის დანახარჯები შეიძლება გადანაწილებულ იქნას მომხმარებლებს შორის, აქედან გამომდინარე, სააბონენტო გადასახადი არ იქნება მაღალი.

უმავთულო გლობალურ ქსელებს გააჩნია მოქმედების შეუზღუდავი არეალი, რომელიც უზრუნველყოფილია სატელეკომუნიკაციო კომპანიების მიერ (ნახ. 1.4).



ნახ. 1.4. უმავთულო გლობალური ქსელები უზრუნველყოფს კავშირს მთელს მსოფლიოში

სატელეკომუნიკაციო ოპერატორების მიერ მიღწეული შეთანხმებები როუმინგთან დაკავშირებით შესაძლებელს ხდის კავშირების დიდ მანძილზე დამყარებას და უზრუნველყოფს მონაცემების სწრაფ გადაცემას მობილურ მომხმარებლებს შორის. მხოლოდ ერთ სატელეკომუნიკაციო კომპანიასთან ანგარიშ-სწორების შემდგომ მომხმარებელს უმავთულო გლობალური ქსელების მეშვეობით მსოფლიოს ნებისმიერი წერტილიდან

შეუძლია კავშირის დამყარება ინტერნეტის სხვადასხვა მომსახურეობებთან.

უმავთულო გლობალური ქსელების თვისებები (მახა-სიათებლები) მაღალი არ არის. მონაცემთა გადაცემის ტიპიური სიჩქარე შეადგენს 56 კბ/წ, ხანდახან 170 კბ/წ-მდე, მაგრამ შექმნილია სპეციალური Web-პორტალები, რომლებიც ინფორმაციული ნაკადების ეფექტურად გადაცემის საშუალებას იძლევა.

მონაცემების გადაცემის სიჩქარე ერთ მომხმარებელზე გადაანგარიშებისას უმავთულო გლობალურ ქსელებში მაღალი არ არის, მაგრამ მისაღებია პატარა მოწყობილობებისთვის (მობილური ტელეფონი, PDA), რომლებიც ეკუთვნით მომხმარებლებს და საჭიროებს ასეთი ქსელით კავშირს. მობილური ტელეფონების პატარა ეკრანი და შეზღუდული გამოთვლითი საშუალებები არ საჭიროებს ქსელის მაღალ თვისებებს. ვიდეოგამოსახულების გადაცემა მობილური ტელეფონის პატარა ეკრანზე შესაძლებელია ინფორმაციის გადაცემის პატარა სიჩქარის დროსაც.

სპეციალური სისტემები, რომლებიც ახასიათებს უმავთულო გლობალურ ქსელებს, უზრუნველყოფს მომხმარებლის წვდომას ინტერნეტთან,კორპორატიულ სისტემებთან და ელექტრონული ფოსტის მიღება-გადაცემას, მიუხედავად იმისა, თუ სად იმყოფება მომხმარებელი – ოფისში, სახლში თუ შენობის გარეთ. მაგალითად, ქსელის აბონენტებს თავისუფლად შეუძლიათ დაამყარონ კავშირი ტაქსით მგზავრობის ან ქალაქში გასეირნების

დროსაც. უმავთულო გლობალურ ქსელებს შეუძლიათ ფუნქციონირება ისეთი ადგილებიდან, საიდანაც სხვა ტიპის ქსელებისთვის წვდომა შეუძლებელია, რის გამოც მომხმარებელი ტერიტორიულად შეზღუდული არ არის.

უმავთულო გლობალური ქსელებისთვის არსებობს რამოდენიმე კონკურენტუნარიანი და მუდმივად განვითარებადი სტანდარტი. ყველაზე ძველი სტანდარტი არის ციფრული მონაცემების პაკეტების მობილურ სისტემაზე გადაცემის სტანდარტი *(Cellular Digital Packet Data,CDPD)*. მაგრამ ეს სისტემა უკვე გამოდის მოხმარებიდან, ვინაიდან სატელე-კომუნიკაციო ოპერატორები გადადიან ტელეკომუნიკაციის მესამე თაობის სისტემებზე *(third generation, 3G)*, რომლებსაც შეუძლია მონაცემების გადაცემა ისეთი სიჩქარით, რომელიც იზომება მბ/წ-ებში.

უმავთულო გლობალური ქსელების დანერგვასთან დაკავშირებული ერთ-ერთი პრობლემათაგანი არის ის, რომ მას არ შეუძლია კარგი კავშირით უზრუნველჰყოს რომელიმე შენობაში მყოფი მომხმარებლები, ვინაიდან ამ ქსელის ინფრასტრუქტურის ელემენტები მდებარეობს შენობის გარეთ, და რადიოსიგნალები შენობაში შესამჩნევად სუსტდება. შედეგად, უმავთულო გლობალური ქსელების მომხმარებლებს, რომლებიც იმყოფებიან შენობაში, შეუძლიათ საერთოდ დაკარგონ კავშირი, ან უკეთეს შემთხვევაში, კავშირის თვისებები შესამჩნევად გაუარესდება. ზოგიერთი სატელეკომუნიკაციო კომპანია უმავთულო გლო-

ბალური ქსელების სისტემებს შენობაში ამონტაჟებს, მაგრამ ყოველივე ეს დიდ ხარჯებთანაა დაკავშირებული და ტექნიკურად ყოველთვის გამართლებული არ არის.

1.1.5. საზღვრების დადგენა

უმავთულო პერსონალური, ლოკალური, რეგიონალური და გლობალური ქსელები ურთიერთშემავსებელიან და აკმაყოფილებს სხვადასხვა მოთხოვნას, მაგრამ ზოგჯერ ძნელია განასხვავო ერთი ქსელი მეორისგან. მაგალითად, უმავთულო ლოკალურ ქსელს შენობის შიგნით შეუძლია უზრუნველყოს ურთიერთკავშირი PDA-სა და პერსონალურ კომპიუტერს შორის, ანალოგიურად იმისა, როგორც ამას ასრულებს უმავთულო პერსონალური ქსელი.

მიღებული ტექნოლოგიები და სტანდარტები საშუალებას გვაძლევს მკაფიოდ დავადგინოთ უმავთულო ქსელების სხვადასხვა სახეობას შორის განსხვავებანი. უმავთულო პერსონალური ქსელები ძირითადად შეესაბამება IEEE 802.15 სტანდარტს (ან Bluetooth), უმავთულო ლოკალური ქსელები – IEEE 802.11 სტანდარტს (ან *Wi-Fi*) და ა.შ. მთავარია ის, რომ უმავთულო ქსელის გამართვის დროს, საჭიროა მთლიანად განისაზღვროს

სისტემის მიმართ წაყენებული მოთხოვნები და აირჩეს ისეთი სახეობა, რომელიც ყველაზე კარგად შეესაბამება მათ.

მომხმარებლის თვალსაზრისით რომ ვიმსჯელოთ მომავალ პერსპექტივებზე, მაშინ უმავთულო ქსელების სახეობებს შორის არსებული საზღვრები უნდა წაიშალოს. უკვე შექმნილია კომპიუტერული მოწყობილობების სპეციალური ქსელური ადაპტერები, რომელთაც გააჩნია უმავთულო ქსელების სხვადასხვა სახეობის მუშაობისადმი მხარდაჭერა. მაგალითად, ტურისტებს ან ბიზნესმენებს შეიძლება ჰქონდეთ თანამედროვე მობილური ტელეფონი, რომელიც ურთიერთქმედებს როგორც უმავთულო ლოკალურ ქსელთან, ასევე- უმავთულო გლობალურ ქსელთან. ყოველივე ეს უზრუნველყოფს უმავთულო კავშირს, აქედან გამომდინარე, მაგალითად, მომხმარებელი, რომელიც იმყოფება აეროპორტის შენობაში, მუშაობს თავის ელექტრონულ ფოსტასთან, რომელიც იყენებს საერთო კავშირის მქონე უმავთულო ლოკალურ ქსელს, შემდეგ, მგზავრობის დროს, ურთიერთქმედებს სხვა სახის მომსახურეობასთან, რომელიც დაფუძნებულია მობილური ქსელით მონაცემების გადაცემასთან.

1.2. უმავთულო ქსელების გამოყენების სფეროები

უმავთულო ქსელებს გააჩნია მხარდაჭერა ისეთი უამრავი სისტემის მიმართ, რომელიც ხელსაყრელია მომხმარებლებისთვის იმით, რომ უზრუნველყოფს მათ მობილურობას და კავშირის მაღალ საიმედოობას, განსხვავებით მავთულიანი სადენების ხარვეზებისაგან. უფრო მეტიც, ბევრ შემთხვევაში უმავთულო ქსელების გამოყენება ზრდის შრომის ნაყოფიერებას და ამცირებს იძულებითი უმოქმედობის პერიოდს, რომელიც წარმოიშვება მავთულიანი ქსელების გამოყენებისას. უმავთულო ქსელების ტექნოლოგიების უმრავლესობის გამოყენებას არ ჭირდება ლიცენზია, რაც მათ გამართვას მარტივს და ეკონომიურად ხელსაყრელს ხდის.

1.2.1. ძირითადი კონფიგურაციები

უმრავლეს შემთხვევაში უმავთულო ქსელი – ეს არის გაფართოება რომელიმე უკვე არსებული მავთულიანი ქსელისა. ამ შემთხვევაში მომსახურე პერსონალს შეუძლია შეასრულოს მისთვის განსაზღვრული დავალება ისე, რომ თვითონვე შეარჩიოს მისთვის ოპტიმალური ადგილი ამ დავალების შესასრულებლად და

დადგეს არა იქ, სადაც მას აქვს წვდომა მავთულიან ქსელთან. მაგალითად, საწყობის მომსახურე პერსონალს შეუძლია გამოიყენოს უმავთულო ხელის მოწყობილობა, რათა მოახდინოს სატვირთო ავტომობილიდან გადმოტვირთული ნივთების სკანირება, ნაცვლად იმისა,რომ ამოიწეროს ნივთების ნომრები მის პერსონალურ კომპიუტერში , რომელიც დგას შენობის რომელიღაც ადგილას, საწყობიდან მოშორებით, შეტანის მიზნით. რა თქმა უნდა, ასეთი მიდგომა უფრო ეფექტურია.

განვიხილოთ სხვა სიტუაცია – სპეციალიზებული უმავთულო ქსელი, რომელიც მთლიანად გამორიცხავს რაიმე მავთულის გამოყენების აუცილებლობას. მაგალითად, მაშველ რაზმს, რომელიც მისულია ავიაკატასტროფის ადგილას, შეუძლია სწრაფად გამართოს დროებითი უმავთულო ქსელი. მაშველი რაზმის ყველა წევრის კომპიუტერული მოწყობილობა ურთიერთკავშირში იქნება ერთმანეთთან, აქედან გამომდინარე, ნებისმიერ მათგანს ექნება ავიაკატასტროფასთან დაკავშირებულ აუცილებელ ინფორმაციასთან ცენტრალიზებული წვდომის შესაძლებლობა.

სისტემები, რომლებთანაც წვდომა შესაძლებელია უმავთულო ქსელების საშუალებით, მომხმარებლებს შეიძლება წარმოუდგეს ინდივიდუალურად ან ღიად. მაგალითად, კომპანიას, რომელიც პირადი მოხმარებისთვის მართავს უმავთულო ქსელს, ასეთ ქსელზე დადებული აქვს გარკვეული შეზღუდვები. როგორც წესი, წვდომა აქვთ მხოლოდ კომპანიის თანამშრომლებს. იმისათვის, რომ

მხოლოდ ავტორიზებულ მომხმარებლებს ჰქონდეთ წვდომა ასეთ ქსელთან, კომპანიები ყოველთვის იღებენ უსაფრთხოების ზომებს. სხვა მხრივ, საერთო კავშირის მქონე ქსელები უზრუნველყოფს ღია წვდომას თავის რესურსებთან. მაგალითად, ბიზნესმენს შეუძლია გამოიყენოს აეროპორტის უმავთულო ქსელი ინტერნეტში შესასვლელად. ასეთი „ცხელი“ თავისუფალი წვდომის მქონე ზონები არის ყველა აეროპორტში, სასტუმროში და სხვა ისეთ ადგილებში, სადაც არის ამის აუცილებლობა.

1.2.2. ინტერნეტთან კავშირი

უმავთულო ქსელის გამართვის ერთ-ერთი ძირითადი მიზეზი არის ის, რომ ერთობლივად იქნას გამოყენებული ერთი მაღალსიჩქარიანი არხი ინტერნეტთან კავშირისათვის. ასეთი სახით დაკონფიგურირებულ ქსელში ყველა ოფისის ან ოჯახის წევრს შეუძლია გამოიყენოს ერთი მაღალსიჩქარიანი კავშირი, რომელიც უზრუნველყოფილია კაბელური მოდემით ან ციფრული სააბონენტო ხაზით *(Digital Subscriber Line, DSL)*. ასეთი პრაქტიკა მიღებულია და ეკონომიას უკეთებს სახსრებს, ვინაიდან უმრავლესობას

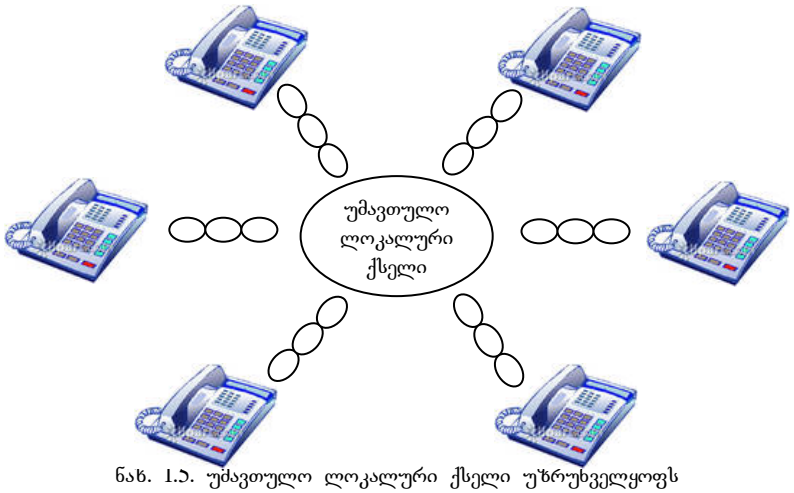
ერთდროულად შეუძლია ინტერნეტთან კავშირი, მიუხედავად იმისა, თუ ოფისის ან ბინის რა ადგილას იმყოფება მომხმარებელი.

ასეთ სიტუაციაში უმავთულო ქსელს გააჩნია ამაღლებული დრეკადობა იმიტომ, რომ ნებისმიერ დროს მასში შეიძლება შევიყვანოთ ახალი სამუშაო სადგური, მავთულების გაყვანის გარეშე. ასევე, თავისუფლად შეგვიძლია უმავთულო ქსელში ჩართული პერსონალური კომპიუტერების, პრინტერების და სერვერების ერთი ადგილიდან მეორეზე გადაადგილება.

კომპანია, რომელსაც გააჩნია უმავთულო ქსელი, საშუალებას აძლევს მომსახურე პერსონალს, რომელიც იმყოფება კომპანიის ტერიტორიის გარეთ, აგრეთვე, ოფისში მისულ კომპანიონებს, რომელთაც გააჩნიათ კომპიუტერული მოწყობილობა, სწრაფად ჩაერთონ კომპანიის ქსელში მინიმალური დაკონფიგურირების შედეგად. მომსახურე პერსონალის მიერ ინტერნეტრესურსების გამოყენება, როდესაც იგი იმყოფება შენობის გარეთ, მნიშვნელოვნად ზრდის მწარმოებლურობას. სევე, ოფისში მისულ კომპანიონს შეუძლია გახსნას თავისი ნოუთბუქი და მიიღოს წვდომა ელექტრონულ ფოსტასთან ან მისთვის საჭირო ინტერნეტსისტემებთან.

1.2.3. შეტყობინების გადაცემა მავთულების გარეშე

ერთ-ერთი საუკეთესო საშუალება ისაა, რომ უმავთულო ქსელები უზრუნველყოფს შეტყობინების გადაცემას, განსაკუთრებით ისეთ სიტუაციებში, როცა მომსახურე პერსონალმა მუდმივი კავშირი უნდა იქონიოს ერთმანეთთან. უმავთულო ლოკალურ ქსელს, რომელშიც გათვლილია ხმოვანი კაშირის დამყარების ხელშეწყობა, შეუძლია სრულად შეცვალოს ტრადიციული სატელეფონო მავთულიანი სისტემა ერთ დიდ შენობაში (ნახ. 1.5). უმავთულო ლოკალური ქსელი უზრუნველყოფს ხმოვანი შეტყობინებებისა და მონაცემების გადაცემის სრულ მობილურობას მცირე საექსპლუატაციო ხარჯებით.



ნახ. 1.5. უმავთულო ლოკალური ქსელი უზრუნველყოფს შენობაში სატელეფონო კავშირის ინფრასტრუქტურას

მაგალითად, სავაჭრო ქსელის მომსახურე პერსონალს შეუძლია გაარკვიოს მომხმარებლისთვის საჭირო პროდუქციის ადგილმდებარეობა ან ჩაატაროს ინვენტარიზაცია სპეციალური უმავთულო ტელეფონის საშუალებით, რომელიც ჩართულია უმავთულო ლოკალურ ქსელში. ასევე, ქსელს უნდა შეეძლოს შტრიხ-კოდების გადაცემის უზრუნველყოფა, რომელიც საჭიროა ინვენტარიზაციის ჩატარების დროს ან ფასის განსაზღვრისათვის უმავთულო ხელის სკანერების მეშვეობით. საკმარისია, კომპანიას გამართული ჰქონდეს მხოლოდ ერთი სატელეკომუნიკაციო სისტემა, რომელიც უზრუნველყოფს შეტყობინებებისა და მონაცემების გადაცემას,რომ შესაძლებელი გახდეს საექსპლოატაციო ხარჯების შემცირება.

ნალოგიურად, კომპანიის მფლობელს უმავთულო ლოკალური ქსელის გამართვით შეუძლია უზრუნველყოს შიდა სატელეფონო კავშირი. ეს აძლევს მომსახურე პერსონალს იმის შესაძლებლობას, რომ მუდმივად იქონიონ ტელეფონები და შენობის ნებისმიერ ადგილას ყოფნის დროს უპასუხონ სატელეფონო ზარებს.

1.2.4. მარაგების მართვა

კომპანიების უმრავლესობა წარმოების პროცესების მართვისათვის წარმატებით იყენებს უმავთულო ლოკალურ ქსელებს, რაც

ამცირებს საექსპლუატაციო ხარჯებს. ვინაიდან მწარმოებელ მოწყობილობებსა და მთავარ მმართველ სისტემას შორის კავშირი მყარდება მავთულების გამოყენების გარეშე, კომპანიას ნებისმიერი ადგილიდან და ნებისმიერ დროს შეუძლია რეორგანიზაცია გაუკეთოს შერჩევის პროცესს.

უმავთულო ლოკალური ქსელების დახმარებით ინვენტარიზაციის მონაცემების განახლება მიმდინარეობს რეალურ დროში, რის გამოც შესამჩნევად იზრდება მათი სიზუსტე და ეფექტურობა. სხვადასხვა პროდუქციით ვაჭრობის პირობებში, რომელიმე საქონლის გაყიდვის დროს, უმავთულო მართვის სისტემა მაშინვე განაახლებს ინვენტარიზაციის მონაცემებს. წარმოების პირობებში, კომპანიის ხელმძღვანელებს რეალურ დროში შეუძლიათ მიიღონ ინფორმაცია ნებისმიერ პროდუქციაზე. კომპანიის მომსახურე პერსონალს უმავთულო შტრიხ-კოდების სკანერების დახმარებით შეუძლია შეამოწმოს ან შეცვალოს ფასი ნაწარმზე, აგრეთვე, შეამოწმოს საწყობში მათი რაოდენობა.

ინვენტარიზაციის დროს სიზუსტის ამაღლება, რომელიც მიიღწევა უმავთულო ლოკალური ქსელების დახმარებით, იწვევს წარმოების პროცესების გაუმჯობესების ჯაჭვურ რეაქციას. ვინაიდან ინფორმაცია მთავარ კომპიუტერში შეიტანება ხელის სკანერების საშუალებით და გამორიცხულია ქაღალდის გამო-ყენების აუცილებლობა, მკვეთრად მცირდება პერსონალის შეცდომები, რომლებიც შეიძლება წარმოიშვას ინფორმაციის შეტანის დროს, იზრდება ფინანსური ანგარიშების სიზუსტე. ეს

მნიშვნელოვანია კომპანიისთვის, ვინაიდან ზუსტი ფინანსური დოკუმენტაცია საშუალებას იძლევა სწორად იქნას გადახდილი სხვადასხვა გადასახადი, რის გამოც მინიმუმამდე იქნება დაყვანილი ჯარიმები(და, შესაძლოა, სასამართლო პროცესების სიხშირე).

1.2.5. ჯანდაცვა

საავადმყოფოების უმრავლესობა უმავთულო ქსელებს ნერგავს იმ მიზნით, რომ აამაღლოს ექსპლუატაციისა და მოხერხებულობის ეფექტურობა. უმრავლეს შემთხვევაში, ჯანდაცვის ორგანოები უმავთულო ლოკალურ ქსელებს მართავენ ისეთ ზონებში, სადაც მაღალია პაციენტების ნაკადი, მაგ., გადაუდებელი დახმარების ცენტრები, მძიმე ავადმყოფების პალატები, მედდების ოთახები, აგრეთვე ექიმების კაბინეტები და პაციენტების მოსაცდელი (მიმღები) ადგილები. ექიმებისა და მედდების ჯგუფს შეუძლია გამოიყენოს მობილური კომპიუტერული მოწყობილობები, რათა ამაღლებულ იქნას პაციენტების მომსახურების ეფექტურობა.

ჯანდაცვის ცენტრებმა ანგარიშებში ზუსტად უნდა შეიტანონ ავადმყოფის ისტორიები იმ მიზნით, რომ მეტი პასუხისმგებლობის პირობებში ჩატარდეს პაციენტების მაღალხა-

რისხიანი მკურნალობა. უყურადღებობის გამო დაშვებული ერთი შეცდომაც კი შეიძლება სიცოცხლის ფასად დაუჯდეს ვინმეს. აქედან გამომდინარე, ექიმები და მედდები ვალდებულები არიან ზუსტად დააფიქსირონ ანალიზის შედეგები, ფიზიკური მონაცემები, ფარმაცევტული ჩანაწერები და ქირურგიული პროცედურები. ასეთი "ქაღალდის" სამუშაო ხშირად ტვირთავს მედპერსონალს, იკავებს რა მათი დროის 50-70%-ს. მონაცემთა შეგროვების უმავთულო მობილური მოწყობილობის გამოყენებით ხდება ინფორმაციის გადაცემა ცენტრალიზებულ მონაცემთა ბაზებში, რაც მნიშვნელოვნად ამაღლებს სიზუსტეს და მონაცემთა თვალსაჩინოების ხარისხს იმათთვის, ვისთვისაც აუცილებელია ეს ინფორმაცია.

ექიმები და მედდები, რომლებიც გადაადგილდებიან ერთი პალატიდან მეორეში და ზრუნავენ ავადმყოფებზე, ხდებიან მაქსიმალურად მობილურები. ელექტრონული სამედიცინო რუქების გამოყენება, რომლის საშუალებითაც საავადმყოფოს ნებისმიერი ტერიტორიიდან შესაძლებელია პაციენტების შესახებ ინფორმაციის შეტანა, დათვალიერება და განახლება, ზრდის ინფორმაციის სიზუსტეს და ავადმყოფების მოვლის ოპერატიულობას. ასეთი გაუმჯობესება მიიღწევა იმის წყალობით, რომ თითოეულ ექიმს და ექთანს გაჩნია მინი-კომპიუტერი ან PDA, რომელიც უმავთულო ქსელის საშუალებით მიერთებულია ცენტრალიზებულ მონაცემთა ბაზასთან, სადაც თითოეული პაციენტის სამედიცინო ისტორია ინახება.

მაგალითად, მკურნალ ექიმს უმავთულო მოწყობილობის დახმარებით შეუძლია ლაბორატორიაში გააგზავნოს მოთხოვნა სისხლის ანალიზის აღების შესახებ. ლაბორატორია ელექტრონული სახით იღებს მოთხოვნას და თავის თანამშრომელს გზავნის ავადმყოფთან სისხლის ასაღებად. ანალიზის ჩატარების შემდეგ ლაბორატორიის პერსონალი შედეგებს შეიტანს ავადმყოფის ელექტრონულ სამედიცინო რუკაში, ხოლო მკურნალ ექიმს თავისი კომპიუტერული მოწყობილობის დახმარებით საავადმყოფოს ნებისმიერი ტერიტორიიდან შეუძლია გაეცნოს ანალიზის შედეგებს.

უმავთულო ქსელები საავადმყოფოებში აგრეთვე გამოიყენება წამლების მონიტორინგისთვის. მობილური ხელის მოწყობილობის გამოყენებით ხდება წამლების სკანირება, მათი ინვენტარიზაცია, განაწილება, დახარისხება და ვარგისიანობის თარიღის შემოწმება, რისი საშუალებითაც იზრდება ამ ოპერაციების ეფექტურობა და სიზუსტე. აგრეთვე მნიშვნელოვანია ის ფაქტი, რომ მედპერსონალი დროულად აწვდის საჭირო წამალს იმ პაციენტს, ვისთვისაც ის არის დანიშნული.

1.2.6. განათლება

სკოლების, კოლეჯების და უმაღლესების უმრავლესობა მიზანმიმართულად თვლის თავის ტერიტორიაზე გამართონ უმავთულო ლოკალური ქსელის გამართვას, რათა

პედაგოგებისათვის, მოსწავლეებისა და სტუდენტებისათვის უზრუნველყოფილ იქნას მობილური კავშირი ქსელურ სისტემებთან,რათა მიიღონ და გააგზავნონ ელექტრონული ფოსტა, დაათვალიერონ WEB-გვერდები, გამოიყენონ სპეციალიზებული ქსელური სისტემები, მოიძიონ თავიანთი შეფასებები და გაეცნონ სასწავლო კურსის კონსპექტებს. ყოველივე ეს ამაღლებს სასწავლო პროცესების ეფექტურობას და მოსწავლეებს და სტუდენტებს საშუალებას აძლევს რაციონალურად გაანაწილონ თავიანთი დრო.

1.2.7. უძრავ ქონებასთან დაკავშირებული ოპერაციები

უძრავი ქონების აგენტები თავიანთი სამუშაო დღის უმეტეს ნაწილს ოფისის გარეთ, კლიენტებთან ატარებენ. ოფისის დატოვებამდე აგენტი არჩევს რამოდენიმე ობიექტს, რომელიც შემდგომ უნდა ანახოს კლიენტს, ამობეჭდავს ინფორმაციას და მიემგზავრება პოტენციურ კლიენტებთან ამორჩეული ობიექტების შესათავაზებლად; თუ კლიენტს არ მოეწონა არც ერთი მათგანი, უძრავი ქონების აგენტი უნდა დაბრუნდეს ოფისში და შეარჩიოს სხვა ობიექტების სია; როდესაც კლიენტი გადაწყვეტს უძრავი

ქონების შეძენას, ისინი უნდა დაბრუნდნენ სააგენტოში, რათა გააფორმონ ხელშეკრულება.

უმავთულო ქსელები საშუალებას იძლევა ბევრად დაჩქარდეს უძრავი ქონების გაყიდვის პროცესი. აგენტს შეუძლია გამოიყენოს კომპიუტერული მოწყობილობა ოფისის გარეთ და მიიღოს ინფორმაცია უძრავი ქონების სააგენტოში არსებული ნებისმიერი ობიექტის შესახებ, შემდეგ კი, პორტატიული კომპიუტერისა და პრინტერის დახმარებით შეადგინოს და ამობეჭდოს ხელშეკრულება გარიგების დასადებად.

1.2.8. საერთო კავშირის მქონე ქსელები

ნოუთბუქების, PDA-ებისა და ციფრული ტელეფონების ფართო გავრცელებასთან დაკავშირებით სულ უფრო იზრდება ინტერნეტისა და კორპორატიული სისტემებისადმი მობილური წვდომის გამოყენების ტენდენცია. მომხმარებლებს სურთ ყველა ინფორმაციულ რესურსთან მუდმივი მობილური კავშირის მიღება მაღალი დონის თვისებებითა და საიმედოობით. უმავთულო ქსელები ქმნის ისეთი სახის ინფრასტრუქტურას, რომლებიც უზრუნველყოფს ზემოთაღნიშნულ მოთხოვნებს საერთო კავშირის მქონე ადგილებში, ოფისის ან სახლის გარეთ.

საერთო კავშირის მქონე უმავთულო ქსელი არის საშუალება მომხმარებლებისათვის, რომელიც უზრუნველყოფს ინტერნეტთან კავშირს მაშინ, როდესაც მომხმარებლები იმყოფებიან გადაადგილების სტადიაზე ერთი ადგილიდან მეორეში. ზოგადად რომ ვთქვათ, უმავთულო ლოკალური ქსელებისადმი წვდომა უზრუნველყოფილია ისეთი ადგილებიდან, სადაც იგრძნობა ხალხმრავლობა.

საერთო კავშირის მქონე უმავთულო ლოკალურ ქსელებს ძირითადად ამონტაჟებენ საზოგადოებრივ ადგილებში, მაგალითად, სასტუმროებსა და რესტორნებში, ასევე, მათი გამართვა შეიძლება ნებისმიერ ადგილას.

იმისათვის, რომ გამოყენებულ იქნას საერთო კავშირის მქონე უმავთულო ქსელების მომსახურება, მომხმარებელს უნდა ჰქონდეს კომმპიუტერული მოწყობილობა, მაგალითად, ნოუთბუქი, რომელსაც გააჩნია უმავთულო ლოკალური ქსელის ადაპტერი. საერთო კავშირის მქონე უმავთულო ქსელების მომწოდებლები (პროვაიდერები) ამონტაჟებენ ქსელებს, რომლებიც შეესაბამება Wi-Fi სტანდარტს. ინტერნეტთან კავშირის დასამყარებლად მომხმარებელი WEB-გვერდის დახმარებით უნდა დარეგისტრირდეს მომსახურებაზე. ზოგიერთი საერთო კავშირის მქონე უმავთულო ლოკალური ქსელი უფასოა, მაგრამ პროვაიდერების უმრავლესობას გააჩნია ფასიანი მომსახურება.

სხვა საერთო კავშირის მქონე უმავთულო ქსელებში გამოიყენება უმავთულო რეგიონალური ქსელების ტექნოლოგია,

რომელიც ძირითადად უზრუნველყოფს ოფისიდან ან სახლიდან ინტერნეტთან კავშირს. პროვაიდერები შენობაზე ამონტაჟებენ პარაბოლურ ანტენებს და მიმართავენ მათ ცენტრალიზებული კვანძისადმი. ასეთი სისტემა „წერტილი – რამდენიმე წერტილი“ უზრუნველფოს კავშირს ისეთ ადგილებში, სადაც შეუძლებელია ს კაბელური მოდემის ან ციფრული სააბონენტო ხაზის გამოყენება.

1.2.9. ადგილმდებარეობის განმსაზღვრელი სისტემები

უმავთულო ქსელების გამოყენებისას ჩნდება იმის შესაძლებლობა, რომ განისაზღვროს ადამიანების ან ნივთების ადგილმდებარეობა. მოძრავი ობიექტების თვალთვალი იძლევა რამოდენიმე საინტერესო სისტემის რეალიზების საშუალებას.შესაძლებელია მომხმარებლების კოორდინატების შეტანა იქნას ცენტრალური სერვერის პროგრამაში, რომელიც უზრუნველყოფს ადგილმდებარეობის განსაზღვრაზე დაფუძნებულ სერვისს. მაგალითად, უმავთულო ლოკალური ქსელის პროვაიდერს შეუძლია გამოიყენოს ასეთი კონცეფცია იმისათვის, რომ აეროპორტში ან რკინიგზის სადგურში მყოფ უცხოელ ტურისტებს წარუდგინოს ინფორმაცია, რომელიც დაეხმარება მათ უახლოესი სასტუმროს ან რესტორნის მოძებნაში.

საავადმყოფოებში ადგილმდებარეობის განმსაზღვრელი სისტემები *(Location-based service)* შეიძლება გამოყენებული იქნას ექიმებისა და მედდების ადგილმდებარეობის განსაზღვრისათვის ნებისმიერ დროს. ყოველივე ეს დაეხმარება საავადმყოფოს ადმინისტრაციას ექსტრემალური სიტუაციის დროს ავადმყოფს გაუგზავნოს შესაბამისი სპეციალისტი.

თავი II. უმავთულო პერსონალური ქსელები

უმავთულო პერსონალური ქსელების საშუალებით შესაძლებელია კომპიუტერულ მოწყობილობებს შორის უმავთულო კავშირის დამყარება პატარა მანძილზე, მაგალითად, მობილურ ტელეფონსა და ნოუთბუქს შორის. უმრავლეს შემთხვევაში ასეთი ქსელის მოქმედების არეალი არ აჭარბებს 9 მეტრს. ყოველივე ეს უმავთულო პერსონალურ ქსელებს მისაღებს ხდის უამრავი გადაწყვეტილების რეალიზაციისას. უმრავლეს შემთხვევაში ისინი გამოიყენება მავთულიანი კავშირების შესაცვლელად ან უბრალოდ ინფორმაციის გადასაცემად მომხმარებლებს შორის.

მეორე თავში გადმოცემულია უმავთულო პერსონალური ქსელების ძირითადი კომპონენტების განსაზღვრებანი. ნაჩვენებია, თუ როგორ ურთიერთქმედებს ეს კომპონენტები სხვადასხვა სისტემის ფორმირებისას და განხილულია სხვადასხვა ტექნოლოგია, რომლებიც დაფუძნებულია რადიო და IR სიგნალების გამოყენებაზე.

2.1. უმავთულო პერსონალური ქსელების კომპონენტები

უმავთულო პერსონალურ ქსელებში გამოიყენება ტექნოლო-გიები, რომლებიც დაფუძნებულია როგორც რადიოტალღების, ისე-ინფრაწითელი გამოსხივების გამოყენებაზე.

უმავთულო პერსონალური ქსელები მუშაობის დროს არ ითხოვს ბატარეების დიდ სიმძლავრეს, რაც მათ იდეალურს ხდის პატარა სამომხმარებლო მოწყობილობების გამოყენებისას, როგორებიცაა, მაგალითად, ყურსასმენები, მობილური ტელეფონები, PDA, სათამაშო მოწყობილობები, ციფრული კამერები, ნოუთბუქები და ა.შ. (ნახ. 2.1).

ნახ. 2.1. სამომხმარებლო მოწყობილობების უმრავლესობას შეუძლია უმავთულო პერსონალურ ქსელში მუშაობა

მაგალითად, უმავთულო პერსონალური ქსელი საშუალებას იძლევა მოვუსმინოთ მუსიკას ყურსასმენით, რომელიც უმავთულოდ შეერთებულია PDA-სთან, ან გადავაგზავნოთ სატელეფონო წიგნი ნოუთბუქიდან მობილურ ტელეფონში. ყველა შემთხვევაში უმავთულო პერსონალური ქსელები გამორიცხავს მავთულების

გამოყენებას, რომელიც ხშირად მოუხერხებელია მომხმარებლებისათვის.

2.1.1. ქსელის ინტერფეისის რადიოპლატები

უმავთულო პერსონალური ქსელებისთვის ქსელის ინტერფეისის რადიოპლატებს უშვებენ 2 ფორმით – PC Card და Compact Flash (CF). თუ, მაგალითად, გვაქვს ნოუთბუქი, CF-ის ჩაყენებით შევძლებთ მისთვის უმავთულო პერსონალურ ქსელში მუშაობის უნარის მინიჭებას. ნოუთბუქების უმრავლესობას გააჩნია უმავთულო პერსონალური ქსელის ერთი ან რამდენიმე ინტერფეისი. ყოველივე ეს ხდის მათ წინასწარ მომზადებულს იმისათვის, რომ შეუერთდეს სხვა მოწყობილობებს, მაგალითად, პრინტერებს, PDA და მობილურ ტელეფონებს, თუ, რა თქმა უნდა, მათაც გააჩნიათ უმავთულო პერსონალური ქსელის ინტერფეისი. დიდი გაბარიტის მქონე PC Card-ები იშვიათად გამოიყენება უმავთულო პერსონალურ ქსელებში. ყოველივე ეს ძირითადად გამოწვეულია იმით, რომ უმავთულო პერსონალური ქსელების მოწყობილობებს კარგად მიესადაგება პატარა გაბარიტის მქონე კვანძები.

2.1.2. USB ადაპტერები

ზოგიერთი კომპანია უმავთულო პერსონალური ქსელებისთვის გვთავაზობს USB-ადაპტერებს (ნახ. 2.2),რომელთაც სხვანაირად უმავთულო საცობებს *(Wireless dangle)* უწოდებენ. მაგალითად, თუ შევიძენთ USB-Bluetooth ადაპტერს და შევაერთებთ მას კომპიუტერის USB პორტში, ეს კომპიუტერსა და სხვა Bluetooth- კავშირის მქონე მოწყობილობებთან კავშირის დამყარების საშუალებას მოგვცემს. Bluetooth – ეს არის სპეციფიკაცია, რომელიც შემუშავებულია რადიოდიაპაზონის მიღება-გადაცემისთვის და რომელიც უზრუნველყოფს მოქმედების პატარა რადიუსს.

ნახ. 2.2. უმავთულო USB-Bluetooth ადაპტერი

2.1.3. მარშრუტიზატორები

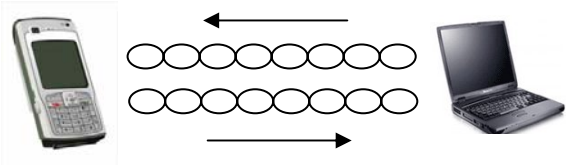
უმრავლეს შემთხვევებში უმავთულო პერსონალური ქსელი უბრალოდ ცვლის მავთულიან კავშირებს, მაგრამ ზოგიერთი მომწოდებელი გვთავაზობს Bluetooth ინტერფეისით მომმარაგებელ მარშრუტიზატორებს, რომლებიც უზრუნველყოფს უმავთულო შეერთებას ინტერნეტთან. მოქმედების პატარა რადიუსის გამო უმავთულო პერსონალური ქსელების მარშრუტიზატორები ძირითადად გამოიყენება ოფისისა და სახლის პირობებში. იმისათვის, რომ დააკმაყოფილოს შედარებით მაღალი მოთხოვნები, ზოგიერთი უმავთულო პერსონალური ქსელების მარშ-რუტიზატორები ასევე მხარს უჭერს უმავთულო ლოკალური ქსელების ინტერფეისებს, ისეთებს, როგორიცაა 802.11 სტანდარტის ქსელები.

2.2. უმავთულო პერსონალური ქსელების სისტემები

სისტემები, რომლებიც დაფუძნებულია უმავთულო პერ-სონალურ ქსელებზე, ძირითადად გათვლილია ცალკეულ მომხმარებელზე, თუმცა ზოგიერთები უზრუნველყოფს რამდენიმეს

ერთად. სისტემების ბევრი სხვადასხვა კონფიგურაცია, რომლებიც დაფუძნებულია უმავთულო პერსონალურ ქსელებზე, გამოიყენება პატარა ოფისისა და სახლის პირობებში.

ყველაზე ხშირად უმავთულო პერსონალური ქსელები გამოიყენება PDA-სა და მობილური ტელეფონების ნოუთბუქებთან და პერსონალურ კომპიუტერებთან სინქრონიზაციისათვის. (ნახ. 2.3)-ზე მოცემულია, თუ როგორ ურთიერთქმედებს ასეთი ტიპის სისტემის კომპონენტები. როდესაც მომხმარებელი აწვება პორტატიული მოწყობილობის სინქრონიზაციის კლავიშს, ამ მოწყობილობის ქსელის ინტერფეისის რადიოპლატა გადასცემს შესაბამის მონაცემებს ნოუთბუქისა ან პერსონალური კომპიუტერის ინტერფეისის რადიოპლატას. ანალოგიურად ხდება საპირისპიროდ.

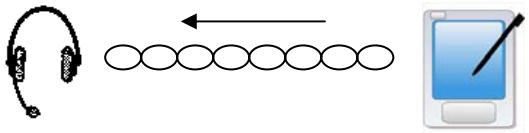


ნახ. 2.3. სინქრონიზაციის პროცესი

2.2.1. ინფორმაციული ნაკადების გადაცემა

უმავთულო პერსონალური ქსელების სისტემების უმრავლესობა გათვალისწინებულია აუდიო- და ვიდეოსიგნალების

ნაკადის გადაცემისთვის. მაგალითად, მომხმარებელს შეუძლია მოისმინოს MP3-ფაილების ნაკადი, რომელიც ინახება MP3 ფლეიერზე (ნახ. 2.4). ამისათვის აუცილებელი არაა, მომხმარებელი ახლოს იმყოფებოდეს ფლეიერთან და იდგეს ერთ ადგილას გაშეშებული. ანალოგიური კონფიგურაცია აქვს უმავთულო ყურსასმენებისა და მიკროფონის გამოყენებას მობილური ტელეფონით საუბრის დროს. ასეთი მიდგომის უარყოფითი მხარე არის ის, რომ უმავთულო კავშირის გამოყენებისას ბატარეის მუშაობა დიდხანს არ გრძელდება.



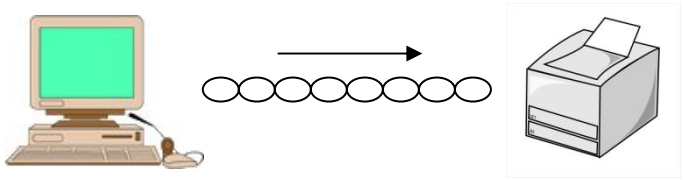
ნახ. 2.4. უმავთულო პერსონალური ქსელი საშუალებას იძლევა გამოყენებული იქნას ყურსასმენები

უმავთულო პერსონალური ქსელების სხვა უპირატესობა არის ნაკადური სისტემების გამოყენება – მოქნილი კავშირი ვიდეოკამერასა და სერვერს შორის. მაგალითად, კომპანიის მფლობელებს შეუძლიათ განათავსონ Web-კამერები შენობის სტრატეგიულ წერტილებში, რათა უზრუნველყონ კომპანიის უსაფრთხოება. ასეთ შემთხვევებში დამონტაჟების სამუშაოები

გაადვილებულია, ვინაიდან არ არის მავთულების გაყვანის აუცილებლობა.

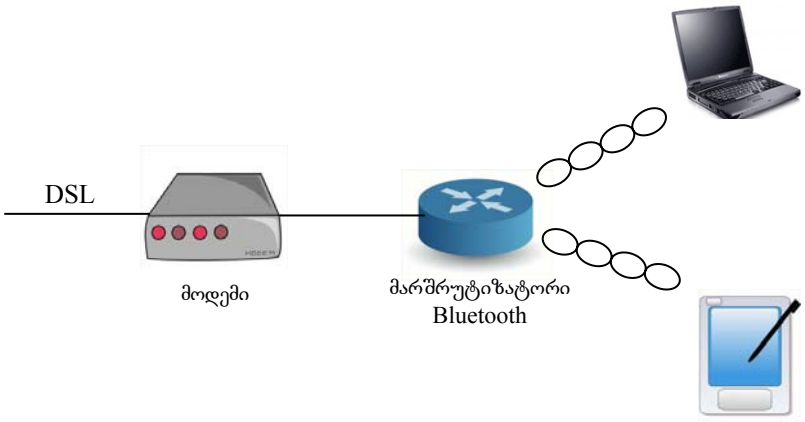
უმავთულო პერსონალური ქსელების საშუალებით შესაძლებელია დამყარდეს კავშირი კომპიუტერის პერიფერიულ მოწყობილობებსა და კომპიუტერს შორის, როგორიცაა მაგალითად, უმავთულო "მაუსი" და კლავიატურა, რაც ამცირებს მავთულების გამოყენებას.

კომპიუტერსა და პრინტერს შორის უმავთულო კავშირის დამყარება შესაძლებელია უმავთულო პერსონალური ქსელის დახმარებით, თუ ისინი განლაგებულნი არიან ერთ ოთახში (ნახ. 2.5). პრინტერის კაბელები ხშირ შემთხვევაში არის მოკლე, რაც საშუალებას არ გვაძლევს პრინტერი დავდგათ იქ, სადაც უფრო მოსახერხებელია. აქედან გამომდინარე, უმავთულო პერსონალური ქსელი საშუალებას იძლევა ოპტიმალურად განვათავსოთ პრინტერი.



ნახ. 2.5. უმავთულო პერსონალური ქსელი საშუალებას იძლევა ოპტიმალურად განვათავსოთ პრინტერი

მომხმარებელს ოთახის ნებისმიერი ადგილიდან შეუძლია იმუშაოს ელექტრონულ ფოსტასთან ან დაათვალიეროს Web-გვერდები, თუ უმავთულო პერსონალური ქსელი უზრუნველყოფს ინტერნეტთან კავშირს. მაგალითად, მომხმარებელს შეუძლია მოხერხებულად განთავსდეს მისთვის სასურველ ადგილას და ისარგებლოს ინტერნეტით. ყოველივე ეს კომპიუტერთან მუშაობას ხდის უფრო სასიამოვნოს. (ნახ. 2.6)-ზე მოცემულია სისტემის კონფიგურაცია, რომელიც უზრუნველყოფს ასეთ შესაძლებლობას.



ნახ. 2.6. უმავთულო პერსონალური ქსელის მარშრუტიზატორი უზრუნველყოფს ინტერნეტთან კავშირს

2.3. უმავთულო პერსონალური ქსელების ტექნოლოგიები

უმავთულო პერსონალურ ქსელებში გამოიყენება ტექნოლოგიები, რომლებიც დაფუძნებულია რადიოტალღებისა და IR გამოსხივების გამოყენებაზე, მიუხედავად იმისა, თუ რა მიზნით იმართება ქსელი.

2.3.1. სტანდარტი - 802.15

IEEE-ის სამუშაო ჯგუფი 802.15 სერიის სტანდარტებით აწარმოებს უმავთულო პერსონალური ქსელებისთვის სტანდარტების შემუშავებას და მათ კორდინაციას სხვა სტანდარტებთან, როგორიცაა,მაგალითად, სტანდარტი 802.11 უმავთულო ლოკალური ქსელისთვის.

802.15 სერიის სტანდარტები შედგება შემდეგი ჯგუფებისაგან:

– 802.15.1. სამუშაო ჯგუფი 1, უმავთულო პერსონალური ქსელისათვის განსაზღვრავს სტანდარტს, რომელიც დაფუძნებულია Bluetooth სპეციფიკაციის გამოყენებაზე. ინფორმაციის გადაცემის

სიჩქარე არ აჭარბებს 1 მბ/წ-ს. ამ სტანდარტის საფუძველზე მიმდინარეობს Bluetooth მოწყობილობების დამუშავება.

– 802.15.2. სამუშაო ჯგუფი 2, იძლევა პრაქტიკულ რეკომენდაციებს, რომლებიც ხელ უწყობს 802.15 და 802.11 ქსელთა სტანდარტების თანაარსებობას. პრობლემა მდგომარეობს იმაში, რომ ორივე ქსელი მუშაობს ერთ დიაპაზონზე - 2,4 გჰ, ამიტომ მათი სამუშაოების კოორდინაცია აუცილებელია. სამუშაო ჯგუფი აფასებს შესაძლო ხარვეზებს და გვთავაზობს მათი აღმოფხვრის მეთოდებს.

– 802.15.3. სამუშაო ჯგუფი 3, მუშაობს ახალი სტანდარტების პროექტზე - მაღალსიჩქარიან უმავთულო პერსონალურ ქსელებზე. მონაცემთა გადაცემის სიჩქარემ შეიძლება შეადგინოს 11, 22, 33, 44 და 55 მბ/წ, რაც კარგად აისახება მულტიმედიურ ინფორმაციასთან მიმართებაში. აღნიშნული ჯგუფი აგრეთვე მუშაობს ღირებულებისა და გამოსაყენებელი სიმძლავრის შემცირებაზე.

– 802.15.4. სამუშაო ჯგუფი 4, მუშაობს სტანდარტებზე, რაც ითვალისწინებს მონაცემთა გადაცემის დაბალ სიჩქარეს, სამაგიეროდ ბატარეის მუშაობა გათვლილია 1 თვეზე და 1 წელზეც კი. ინფორმაციის გადაცემის სიჩქარე შეადგენს – 20, 40 და 250 კბ/წ.

2.3.2. Bluetooth

კომპანიების Ericsson, IBM, Intel, Nokia და Toshiba ერთობლივი მუშაობის შედეგად 1998 წელს პირველად გამოჩნდა ტექნოლოგია Bluetooth. ისინი მუშაობენ ისეთი გადაწყვეტილების შექმნაზე, რომელიც უზრუნველყოფდა კომპიუტერულ მოწყობილობებს შორის უმავთულო კავშირს. სპეციფიკაცია Bluetooth იდეალურია პატარა მოწყობილობებისათვის, რომლებსაც ჭირდება პატარა სიმძლავრე და მუშაობს პატარა რადიუსის მასშტაბში. ყოველივე ეს Bluetooth-ს ხდის ეფექტურს პატარა გაბარიტის მქონე მოწყობილობების პატარა სამუშაო ზონაში შესაერთებლად. აქედან გამომდინარე, სამუშაო ჯგუფმა - 802.15-მა აირჩია Bluetooth, როგორც 802.15.1 სტანდარტისათვის ძირითადი ტექნოლოგია.

Bluetooth მოწყობილობა ინფორმაციის გადაცემას უზრუნველყოფს 9 მეტრამდე მანძილზე. Bluetooth მოდულები არის პატარ ზომის, აქედან გამომდინარე, მარტივია მათი ჩაყენება სხვადასხვა სამომხმარებლო მოწყობილობაში.

Bluetooth ტექნოლოგიას შეუძლია უზრუნველყოს Bluetooth მოწყობილობების ავტომატური შეერთება, რომლებიც ერთმანეთთან ახლოსაა. მომხმარებელს შეუძლია მიიღოს ან გაწყვიტოს კავშირი სხვა მომხმარებელთან.

Bluetooth მწარმოებლებს მომავალში შეუძლიათ შემოგვთავაზონ Bluetooth მარშრუტიზატორები, რომლებიც

იმუშავებს იმ რადიუსით, რომელსაც უზრუნველყოფს ქსელები სტანდარტით 802.11, თუმცა დღეისათვის Bluetooth მოწყობილობები 802.11 სტანდარტის ნაწარმს ჩამოუვარდებიან მოქმედების რადიუსით, გადაცემის სიჩქარით და მწარმოებლურობით.

თავი III. უმავთულო ლოკალური ქსელები

უმავთულო ლოკალური ქსელები სრულიად აკმაყოფილებს მოთხოვნებს, რომლებიც წაყენებულია უმავთულო შეერთებისთვის შენობის ფარგლებში კავშირის დასამყარებლად. ისინი გამოირჩევა მაღალი თვისებებით და დაცვის მაღალი დონით, რის საფუძველზეც უმავთულო ლოკალური ქსელები გამოიყენება სახლის პირობებში, პატარა ოფისებში, საწარმოებში და საერთო თავშეყრის ადგილებში.

მესამე თავში გადმოცემულია უმავთულო ლოკალური ქსელების ძირითადი კომპონენტები, ნაჩვენებია, თუ როგორ უნდა ურთიერთქმედებდნენ ეს კომპონენტები სხვადასხვა სისტემაში და განხილულია 802.11-ის სტანდარტები.

3.1. უმავთულო ლოკალური ქსელების კომპონენტები

უმავთულო ლოკალური ქსელები შედგება ისეთივე კომპონენტებისაგან, როგორისგანაც-ტრადიციული ლოკალური მავთულიანი Ethernet-ის ქსელები. ასევე ჰგვანან მათი ოქმები Ethernet-ის ოქმებს. განსხვავება მხოლოდ იმაშია, რომ უმავ-

თულო ლოკალური ქსელების გამართვის დროს მავთულების გამოყენება აუცილებელი არ არის.

უმავთულო ლოკალური ქსელების მომხმარებლები მუშაობენ ბევრ მოწყობილობასთან – პერსონალურ კომპიუტერებთან, ნოუთბუქებთან, PDA და ა.შ. მოწყობილობების ერთმანეთთან დასაკავშირებლად უმავთულო ლოკალური ქსელების გამოყენება პერონალური კომპიუტერებისათვის ეფექტურია იმიტომ, რომ გამორიცხავს მავთულების გაყვანის აუცილებლობას. სამომხმარებლო მოწყობილობებს შეიძლება აგრეთვე გააჩნდეთ სპეციფიური აპარატურული უზრუნველყოფა. მაგალითად, უმავთულო ლოკალურ ქსელებში ხშირად აერთებენ შტრიხ-კოდების სკანერებს, ან მოწყობილობებს, რომლებიც ყურადღებას აქცევს პაციენტის მდგომარეობას.

3.1.1. ქსელის ინტერფეისის რადიოპლატები

უმავთულო ლოკალური ქსელის ძირითადი კომპონენტია ქსელის ინტერფეისის რადიოპლატა, რომელიც რეალიზებულია 802.11 სტანდარტზე. ეს რადიოპლატები ჩვეულებრივ მუშაობს ერთ ფიზიკურ დონეზე – 802.11a ან 802.11b/g. რადიოპლატამ, რომელიც შეთავსებულია უმავთულო ლოკალურ ქსელთან, რეალიზება უნდა გაუკეთოს სტანდარტის ვერსიას. უმავთულო

ლოკალური ქსელის რადიოპლატები, რომლებიც უზრუნველყოფს და რეალიზაციას უკეთებს აღნიშნული სტანდარტის სხვადასხვა ვერსიას და გააჩნია ურთიერთქმედების მაღალი დონის შესაძლებლობა, ხდება უფრო და უფრო გავრცელებადი.

რადიოპლატებს აწარმოებენ სხვადასხვა ფორმ-ფაქტორით: ISA, PCI, PC card, mini-PCI და CF. პერსონალურ კომპიუტერებში ჩვეულებისამებრ იყენებენ ISA და PCI პლატებს, ხოლო PDA-სა და ნოუთბუქებში – PC card, mini-PCI და CF ადაპტერებს.

3.1.2. წვდომის წერტილები

წვდომის წერტილი შედგება რადიოპლატისაგან, რომელიც უზრუნველყოფს კავშირს უმავთულო ლოკალური ქსელის ცალკეულ სამომხმარებლო მოწყობილობასა და ქსელის ინტერფეისის მავთულიან პლატას შორის, რომელიც უზრუნ-ველყოფს განაწილებულ სისტემასთან ურთიერთქმედებას, როგორიც არის Ethernet. წვდომის წერტილების სისტემური პროგრამული უზრუნველყოფა განაპირობებს უმავთულო ლოკალური ქსელის ნაწილებსა და წვდომის წერტილების განაწილებულ სისტემას შორის ურთიერთქმედებას. ეს პროგრა-მული უზრუნველყოფა წვდომის წერტილებს დიფერენცირებას უკეთებს უზრუნველყოფილი მმართველობის ხარისხით და

უსაფრთხოების ფუნქციებით. (ნახ. 3.1)-ზე ნაჩვენებია წვდომის წერტილების აპარატურული მოწყობილობა.

ნახ. 3.1. წვდომის წერტილი უმავთულო ლოკალურ ქსელს აკავშირებს მავთულიან ქსელებთან

ბევრ შემთხვევაში წვდომის წერტილები უზრუნველყოფს http-ინტერფეისს, რომელიც საშუალებას იძლევა სამომხმარებლო მოწყობილობების საშუალებით, რომელსაც გააჩნია ქსელური ინტერფეისი და Web-ბრაუზერი, შეცვალოს მისი კონფიგურაცია.

განვიხილოთ ძირითადი პარამეტრები წვდომის წერტილის კონფიგურირებისათვის. ერთ-ერთი მათგანი, რომელიც უნდა ავირჩიოთ, არის მომსახურების ზონის იდენტიფიკატორი *(Service set identifier, SSID).* SSID იდენტიფიკატორი წარმოგვიდგენს სახელს კონკრეტული უმავთულო ლოკალური ქსელისათვის, რომელზედაც მიებმება მომხმარებელი. უსაფრთხოების მაღალი

დონის უზრუნველყოფის მიზნით SSID პარამეტრის მნიშვნელობა თავიდანვე შემოთავაზებულისაგან განსხვავებით ყენდება გამორჩეულად.

უმრავლეს შემთხვევაში წვდომის წერტილის გადამცემის სიმძლავრე ყენდება მაქსიმალურ დონეზე. ეს საშუალებას იძლევა გაიზარდოს უმავთულო ლოკალური ქსელის მოქმედების რადიუსი. ქსელის მოქმედების დროს აუცილებელია გავააქტიუროთ უმავთულო კავშირის დაშიფვრის ოქმის მუშაობა *(Wired equivalent privacy, WEP)*, იმისათვის, რომ უზრუნველვყოთ პირველი დონის უსაფრთხოების ზომები, ყენდება დაშიფვრის გასაღები, რომელიც აუცილებელია ყველა სამომხმარებლო მოწყობილობისათვის და რომელსაც აქვთ წვდომის წერტილთან ურთიერთქმედების უფლება, რისი საშუალებითაც მიიღება დაშიფრული მონაცემები.

3.1.3. მარშრუტიზატორები

სახელწოდების მიხედვით თუ ვიმსჯელებთ, მარშრუტიზატორი გადასცემს პაკეტებს ერთი ქსელიდან მეორეში, არჩევს რა შემდგომ საუკეთესო არხს უახლოეს წერტილში პაკეტის გადასაცემად. მარშრუტიზატორები გამოიყენებენ ინტერნეტ ოქმების (*Internet Protocol, IP*) პაკეტის სათაურებს და მარშრუტიზაციის ცხრილებს. აგრეთვე იყენებენ შიდა ოქმებს

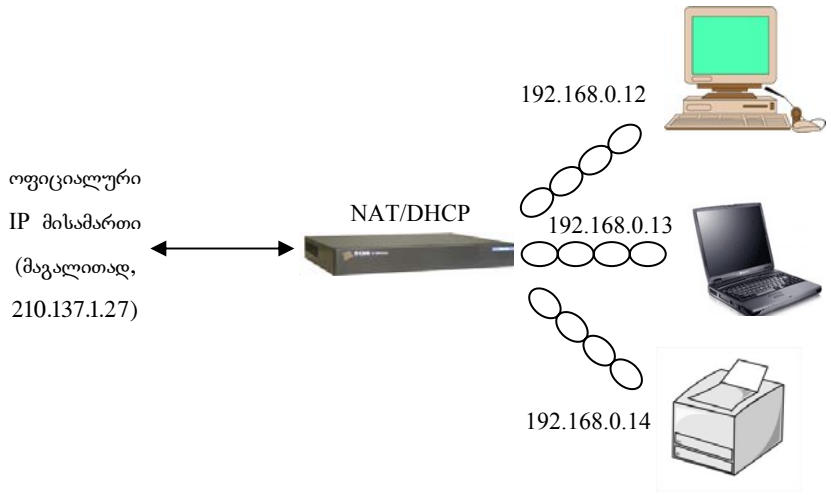
თითოეული პაკეტის გადასაცემად საუკეთესო გზის განსაზღვრისათვის (ნახ. 3.2).

ნახ. 3.2. მარშრუტიზატორი

უმავთულო ლოკალური ქსელის მარშრუტიზატორი ანიჭებს შესაძლებლობას Ethernet-ის მრავალპორტიან მარშრუტიზატორს შეასრულოს ჩაშენებული წვდომის წერტილის ფუნქციები. ამის წყალობით შესაძლებელია Ethernet-ისა და უმავთულო ქსელების კომბინირება. უმავთულო ლოკალური ქსელის ტიპიურ მარშრუ-ტიზატორს გააჩნია 4 პორტი, 802.11 სტანდარტის წვდომის წერტილი და ხშირ შემთხვევაში- პარალელური პორტი, ამიტომ მას აგრეთვე შეუძლია შეასრულოს სერვერის ბეჭდვის ფუნქცია. ყოველივე ეს უმავთულო ქსელის მომხმარებლებს აძლევს საშუალებას ისევე მიიღოს და გააგზავნოს პაკეტები ბევრ მავთულიან ქსელში, თითქოს ისინი შეერთებულნი არიან ერთ-ერთ მათგანში.

მარშრუტიზატორები იყენებს ქსელების მისამართების ტრანსლაციის ოქმებს *(network address translation, NAT)*, რომელიც ბევრ ქსელურ მოწყობილობას აძლევს საშუალებას ერთობლივად გამოიყენოს ერთი *IP* მისამართი, წარმოდგენილი

ინტერნეტ მომსახურების პროვაიდერის მიერ (*Internet service provider, ISP*). ეს კონცეფცია წარმოდგენილია (ნახ. 3.3)-ზე. მარშრუტიზატორები აგრეთვე იყენებენ დინამიკური კვანძის კონფიგურირების ოქმს (*dynamic host configuration protocol, DHCP*) ყველა მოწყობილობის მომსახურებისათვის, რომელიც იძლევა საშუალებას ყველა მოწყობილობას წარმოუდგინოს ცალკეული IP მისამართები. ერთობლივი ძალებით NAT და DHCP შესაძლებელს ხდის რამოდენიმე ქსელური მოწყობილობის (როგორიცაა, პერსონალური კომპიუტერები, ნოუთბუქები და პრინტერები) მუშაობას ინტერნეტში მხოლოდ ერთი IP მისამართის გამოყენებით.



ნახ. 3.3. NAT და DHCP – ძირითადი ოქმები, რომლებიც გამოიყენება მარშრუტიზატორების მიერ

უმავთულო ლოკალური ქსელების მარშრუტიზატორებს, დაყენებულ იქნებიან რა შემდგომში სახლში ან ოფისში, გააჩნია არსებითი უპირატესობა. მაგალითად, შესაძლებელია ხელის მოწერა პროვაიდერის მიერ საკაბელო მოდემის საშუალებით შემოთავაზებულ მომსახურებაზე. ამ შემთხვევაში მომხმარებელს მარშრუტიზატორისთვის, რომელიც მუშაობს DHCP ოქმზე, გამოეყოფა ერთი IP მისამართი. შემდეგ, იმავე DHCP ოქმის დახმარებით მარშრუტიზატორი ყველა ლოკალური ქსელის მომხმარებელს წარმოუდგენს ცალკეულ IP მისამართებს. შემდეგ NAT დაადგენს შესაბამისობას ლოკალური ქსელის კონკრეტულ მომხმარებლებსა და ინტერნეტ-პროვაიდერის IP მისამართს შორის, ნებისმიერ დროს, როცა მომხმარებელს ესაჭიროება ინტერნეტთან კავშირი. მაშასადამე, როცა საჭიროა ინტერნეტთან კავშირი ჰქონდეს ლოკალური ქსელის ერთზე მეტ მომხმარებელს და გამოყენებულ იქნას პროვაიდერის მიერ წარმოდგენილი ერთი IP მისამართი, აუცილებელია მარშრუტიზატორის გამოყენება, მაგრამ მარშუტიზატორები იშვიათად გამოიყენება დიდ ქსელებში (მაგალითად, საავადმყოფოების ან დიდი კომპანიების ქსელები). ასეთ შემთხვევებში რაციონალურია წვდომის წერტილების გამოყენება, ვინაიდან ასეთ ქსელებში ხშირ შემთხვევაში არის მავთულიანი კომპონენტები IP მისამართებით.

3.1.4. განმმეორებლები

წვდომის წერტილები, რომელთა მუშაობისთვისაც საჭიროა შემაერთებელი მავთულები, ძირითად როლს თამაშობს უმრავლეს შემთხვევაში უმავთულო ლოკალური ქსელების გამართვისას აუცილებელი სამუშაო ზონების მომსახურების უზრუნველყოფაში. არსებული უმავთულო ლოკალური ქსელის მოქმედების რადიუსის გასაფართოვებლად მასში შეყავთ დამატებითი წვდომის წერტილები. მეორე ვარიანტი – სარგებლობენ უმავთულო განმმეორებლებით *(Repeaters)*. მწარმოებლები ლოკალური ქსელებისთვის გვთავაზობენ ავტონომიური უმავთულო განმმეორებლის რამოდენიმე მოდელს, თუმცა ზოგიერთ წვდომის წერტილს გააჩნია ჩაშენებული განმმეორებლები.

განმმეორებელი, არსებულ ქსელურ ინფრასტრუქტურაში, მოქმედების რადიუსის გასაფართოვებლად, უბრალოდ რეგენერირებას უკეთებს სიგნალებს, რომლებიც ვრცელდება ქსელში. უმავთულო ლოკალური ქსელის განმმეორებელს არ გააჩნია ფიზიკური კონტაქტი (ხორციელდება მავთულების გამოყენებით) რომელიმე ქსელის ნაწილთან. ის იღებს წვდომის წერტილისაგან რადიოსიგნალებს და განმეორებით გადასცემს მიღებულ მონაცემთა ფრეიმებს. ყოველივე ეს განმმეორებელს, რომელიც განთავსებულია წვდომის წერტილსა და მოცილებულ მომხმარებელს შორის, აძლევს იმის საშუალებას, რომ იფუნქციონიროს, როგორც ფრეიმების რეტრანსლატორმა, რომელიც გადასცემს მომხმა-

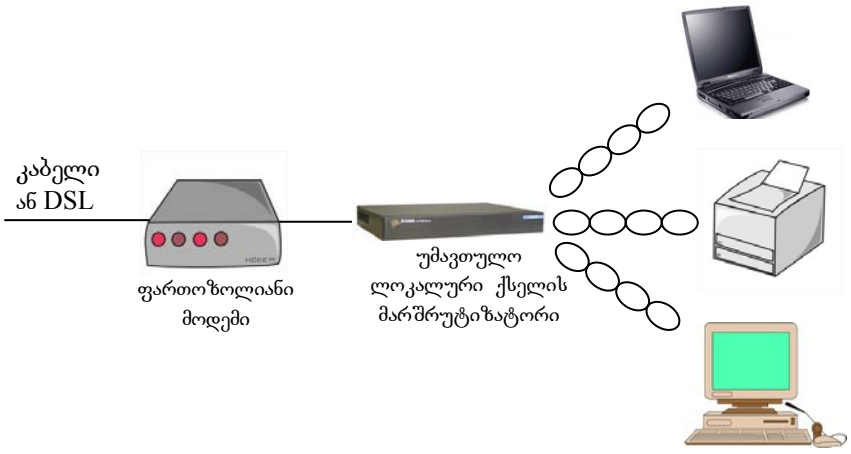
რებლიდან წვდომის წერტილისაკენ და პირიქით. აქედან გამომდინარე, უმავთულო განმმეორებლები წარმოადგენს ეფექტურ გადაწყვეტილებას რადიოხარვეზებით გამოწვეული სიგნალების დასუსტების პრობლემის გადასაჭრელად.

3.2. უმავთულო ლოკალური ქსელების სისტემები

სისტემების ბევრი სხვადასხვა კონფიგურაცია, რომლებიც დაფუძნებულია უმავთულო ლოკალურ ქსელებზე, გამოიყენება დიდი ორგანიზაციების, ოფისებისა და სახლის პირობებში.

სახლისა და პატარა ოფისის პირობებში უმავთულო ლოკალური ქსელის გამართვის დროს იყენებენ ერთ მარშრუტიზატორს, რისი საშუალებითაც ხდება ფართოზოლიანი კავშირის დამყარება ინტერნეტთან (DSL ან კაბელური მოდემით). ასეთი მარშრუტიზატორის ტიპიური მოქმედების რადიუსი ჩვეულებისამებრ საკმარისია სახლის ან პატარა ოფისის ფარგლებში კავშირის დასამყარებლად. მარშრუტიზატორი აუცილებელია მაშინ, თუ გათვალისწინებულია ერთ ქსელური მოწყობილობაზე მეტის გამოყენება. მაგალითად, თუ სახლში არის უმავთულო პერსონალური კომპიუტერი, ნოუთბუქი და პრინტერი, მაშინ ყველა ამ

მოწყობილობის ერთმანეთთან კავშირის დასამყარებლად აუცილებელია NAT და DHCP ოქმები (ნახ. 3.4).



ნახ. 3.4. სახლისა და პატარა ოფისის უმავთულო ლოკალურ ქსელს აქვს მარტივი კონფიგურაცია

სახლისა და პატარა ოფისის პირობებში უმავთულო ლოკალური ქსელის გამართვის დროს ერთი წვდომის წერტილის გამოყენება აგრეთვე უზრუნველყოფს ქსელის მუშაობას, მაგრამ ის მხოლოდ ერთ მოწყობილობას მისცემს საშუალებას, რომ მიიღოს IP მისამართი და შესაბამისად- ინტერნეტთან კავშირი. ეს გამოწვეულია იმით, რომ წვდომის წერტილების უმრავლესობა არ მუშაობს NAT და DHCP ოქმებით, მაგრამ წვდომის წერტილისა და მავთულიანი მარშრუტიზატორის კომბინაციას შეუძლია შეცვალოს უმავთულო ლოკალური ქსელის მარშრუტიზატორი და

ეს ნაკლებად ძვირადღირებული გადაწყვეტილებაა, ვიდრე უმავთულო ლოკალური ქსელის მარშრუტიზატორის შეძენა, თუ თქვენ უკვე გაქვთ წვდომის წეტილი ან მავთულიანი მარშრუ-ტიზატორი (ნახ. 3.5).

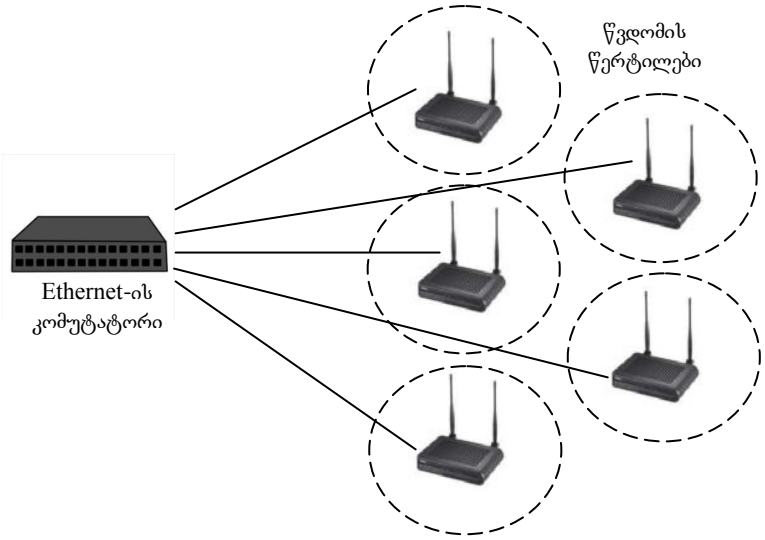
ნახ. 3.5. წვდომის წერტილისა და მავთულიანი მარშრუტიზატორის კომბინაცია

უმავთულო ლოკალური ქსელის წვდომის წერტილში და მარშრუტიზატორში უსაფრთხოების პარამეტრები, როგორიცაა WEP, თავიდანვე გათიშულია, ამიტომ უმავთულო ლოკალური ქსელის დაყენების დროს აუცილებელია უსაფრთხოების სისტემის აქტივიზაცია.

3.2.1. უმავთულო ლოკალური ქსელები საწარმოებში

უმავთულო ლოკალური ქსელის სტრუქტურა საწარმოში ბევრად უფრო რთულია, ვიდრე სახლისა და პატარა ოფისის პირობებში. ძირითადი მიზეზი არის ის, რომ საწარმოს ქსელი

შეიცავს ბევრ წვდომის წერტილს, რომლის დასაკავშირებლადაც აუცილებელია მძლავრი განაწილებული სისტემა (ნახ. 3.6).



ნახ. 3.6. საწარმოში უმავთულო ლოკალური ქსელის სტრუქტურა

წვდომის წერტილები ქმნის გადამფარავ რადიორგოლებს, რომლებიც საშუალებას აძლევს მომხმარებლებს გადაადგილდნენ საწარმოს შიგნით და იქონიონ კავშირი მის რესურსებთან უმავთულო ქსელის გამოყენებით. ასეთი კონფიგურაცია ან ინფრასტრუქტურის რეჟიმი ტიპიურია უმავთულო ლოკალური ქსელისთვის, რომლის მომსახურების ზონა შეადგენს 1800 $მ^2$-ს.

საავადმყოფოს უმავთულო ლოკალური ქსელი შეიძლება შეიცავდეს 100-მდე წვდომის წერტილს, რომლებიც განლაგებულია მთელი შენობის ტერიტორიაზე. ყოველივე ამის

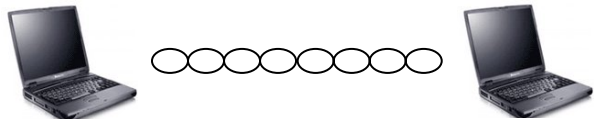
დასაკავშირებლად საჭირო იქნება ბევრი მავთულის გამოყენება. როგორც საწარმოს შემთხვევაში, საავადმყოფოშიც უკვე არსებობს აპარატურული მოწყობილობა, რომელზეც სრულდება DHCP. ამიტომ გამოიყენება წვდომის წერტილები და არა უმავთულო ლოკალური ქსელის მარშრუტიზატორები.

დიდი ორგანიზაციების უმავთულო ლოკალური ქსელები საჭიროებს მოხერხებული დაცვის მექანიზმების გამოყენებას, რომლებიც უზრუნველყოფს უსაფრთხოებას. ორგანიზაციებში გაცილებით დიდი ყურადღება უნდა დაეთმოს აუტენტიფიკაციასა და დაშიფვრას, ვიდრე უმავთულო ლოკალური ქსელის გამოყენებას სახლისა და პატარა ოფისის პირობებში. უსაფრთხოების შესახებ დაწვრილებით იქნება საუბარი VI თავში.

3.2.2. დაუგეგმავი უმავთულო ლოკალური ქსელები

დაუგეგმავ (ზოგჯერ მას ეძახიან შემთხვევითს ან სპეციალურს) უმავთულო ლოკალურ ქსელში *(ad hoc wireless LAN)* არ არსებობს წვდომის წერტილი. თითოეული ცალკეული სამომხმარებლო მოწყობილობა უშუალოდ უკავშირდება სხვა სამომხმარებლო მოწყობილობას. ასეთი კონფიგურაციის უპირატესობა მდგომარეობს იმაში, რომ მომხმარებლებს შეუძლიათ

სპონტანურად და სწრაფად ჩამოაყალიბონ უმავთულო ლოკალური ქსელი (ნახ.3.7).



ნახ. 3.7. დაუგეგმავი უმავთულო ლოკალური ქსელი

დაუგეგმავი უმავთულო ლოკალური ქსელი საშუალებას იძლევა ერთმა მომხმარებელმა სწრაფად გადასცეს დიდი ზომის ფაილი მეორე მომხმარებელს, რომელიც შორიახლოს იმყოფება მაგ., საკონფერენციო დარბაზში და არა აქვს წვდომა უმავთულო ლოკალური ქსელის ინფრასტრუქტურასთან. თითოეული მომხმარებელი უბრალოდ დააკონფიგურირებს ქსელის ინტერფეისის რადიოპლატას ისეთი სახით, რომ მას შეეძლოს მუშაობა დაუგეგმავი ქსელის რეჟიმში *(ad hoc mode),* საჭირო დაკავშირება კი ხორციელდება ავტომატურ რეჟიმში.

დაუგეგმავი ქსელის რეჟიმი აგრეთვე სასარგებლოა საავარიო მომსახურეობების დასახმარებლად, სადაც შესაბამისი ოპერაციები უნდა შესრულდეს ადგილზე და აუცილებელია, რომ ჯგუფის წევრებმა ერთმანეთთან იქონიონ კავშირი.

3.3. უმავთულო ლოკალური ქსელების ტექნოლოგიები

ყველაზე ხშირად უმავთულო ლოკალურ ქსელებს ქმნიან 802.11 სტანდარტის შესაბამისობით. სტანდარტი IEEE 802.11 აღწერს წვდომის მართვის საერთო ოქმს გადაცემის არეში *(Media Access Control, MAC)* და უმავთულო ლოკალური ქსელების რამოდენიმე ფიზიკურ დონეს. 802.11 სტანდარტის პირველი რედაქცია მიღებულ იქნა 1997 წელ, მაგრამ მაშინ უმავთულო ლოკალური ქსელები ფართო გამოყენებაში არ იყო. სიტუაცია მკვეთრად შეიცვალა 2001 წელს, როდესაც ქსელის კომპონენტებზე ფასებმა მკვეთრად დაიწია. IEEE 802.11 სტანდარტის შემმუშავებელი სამუშაო ჯგუფი აქტიურად მუშაობს უმავთულო ლოკალური ქსელების თვისებებისა და უსაფრთხოების გაუმჯობესების მიზნით.

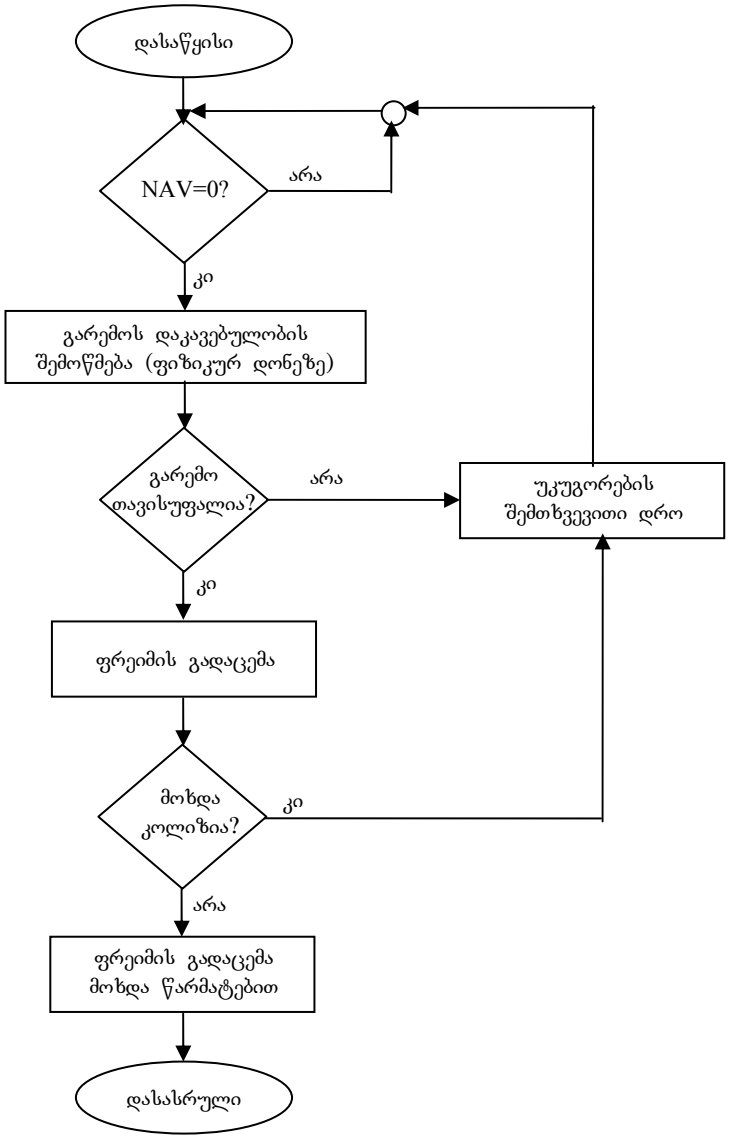
3.3.1. სტანდარტი 802.11

802.11 სტანდარტი აღწერს MAC-ის ერთ დონეს, რომლითაც უზრუნველყოფილია მრავალი ფუნქციის შესრულება 802.11 სტანდარტის უმავთულო ლოკალური ქსელების მუშაობის უნარის უზრუნველყოფის მიზნით. MAC დონე ახორციელებს

მართვას და ხელს უწყობს 802.11 სტანდარტის სადგურებს შორის კავშირს (ქსელის ინტერფეისის რადიოპლატასა და წვდომის წერტილებს შორის), აწარმოებს რა წვდომის კოორდინირებას ერთობლივად გამოსაყენებელ გარემოში. 802.11 სტანდარტის MAC დონე მართავს 802.11 სტანდარტის ფიზიკურ დონეებს, როგორიცაა 802.11a, 802.11b და 802.11g, გარემოს დაკავებულობისა და დაუკავებლობის განსაზღვრის მიზნით, 802.11 სტანდარტის ფრეიმების გადაცემისა და მიღების განხორციელებით.

ფრეიმის გადაცემამდე სადგურმა უნდა მიიღოს წვდომა გარემოსადმი, ანუ სადგურების მიერ ერთდროულად გამოყენებულ რადიოარხთან. 802.11 სტანდარტი ითვალისწინებს გარემოსადმი წვდომის 2 ფორმას: კოორდინაციის გამანაწილებელ ფუნქციას *(distributed coordination function, DCF)* და კოორდინაციის წერტილოვან ფუნქციას *(point coordination function, PCF).*

DCF რეჟიმის ხელშეწყობა აუცილებელია და დაფუძნებულია ოქმზე, რომელიც უზრუნველყოფს მრავალგვარ წვდომას საარსებო კონტროლთან და აღმოფხვრის კოლიზიას *(Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA).* DCF რეჟიმის მუშაობის დროს სადგურები შედიან კონკურენციაში გარემოსადმი წვდომისათვის და ცდილობენ გადასცენ ფრეიმი, თუ ამ დროს არცერთი სხვა სადგური არ ახორციელებს ფრეიმის გადაცემას. თუ რომელიმე სადგური გადასცემს ფრეიმს, დანარჩენები ელოდებიან არხის განთავისუფლებას (ნახ. 3.8).



ნახ. 3.8. რეჟიმი DCF გვთავაზობს გარემოსადმი წვდომის გამანაწილებელ ფორმას

გარემოსადმი წვდომისათვის, MAC დონე ამოწმებს ქსელის განაწილების ვექტორის მნიშვნელობას *(network allocation vektor, NAV)*, რომელიც წარმოადგენს ყველა სადგურზე განლაგებულ მთვლელს, რომლის მნიშვნელობა შეესაბამება წინა ფრეიმის გადასაცემად აუცილებელ დროს. NAV-ის მნიშვნელობა უნდა იყოს ნულის ტოლი,იმისთვის, რომ სადგური შეეცადოს ფრეიმის გადაგზავნას. ვიდრე ფრეიმი გადაიგზავნება, მისი მოცულობის მიხედვით სადგური გამოთვლის გადაგზავნისთვის საჭირო დროსა და ქსელში მონაცემთა გადაგზავნის სიჩქარეს. სადგური ათავსებს მნიშვნელობებს ფრეიმის თავში. როდესაც სადგური იღებს ფრეიმს, ის ამოწმებს მნიშვნელობას და გამოიყენებს თავისი NAV-ის დასაყენებელ საფუძვლად. ამ პროცესის წყალობით ხდება იმ გარემოს რეზერვირება, რომელიც გამოიყენება გადამცემი სადგურის მიერ.

DCF რეჟიმის მთავარი ასპექტი არის უკუგორების ტაიმერი *(back-off timer)*, რომელსაც სადგური იყენებს იმ შემთხვევაში, როცა გადაცემის გარემო დაკავებულია. როდესაც არხი გამოიყენება სხვა სადგურის მიერ, გადაცემის სურვილის მქონე სადგური რაღაც დროის განმავლობაში უნდა იმყოფებოდეს ლოდინის რეჟიმში, შემდეგ კი კვლავ შეეცადოს მიიღოს წვდომა გარემოსადმი. ამის წყალობით გამოირიცხება იმის შესაძლებლობა, რომ რამოდენიმე სადგურმა პარალელურ რეჟიმში დაიწყოს ფრეიმების გადაცემა. უკუგორების ტაიმერი მნიშვნელოვნად ამცირებს კოლიზიების და განმეორებით გადაცემების რიცხვს,

განსაკუთრებით მაშინ, როდესაც აქტიური მომხმარებლების რაოდენობა ძალზედ დიდია.

ლოკალური ქსელების გამოყენებისას, რაც დაფუძნებულია რადიოარხებზე, მონაცემების გაგზავნის დროს გადამცემ სადგურს არ შეუძლია მოუსმინოს გარემოს კოლოზიის წარმოშობისას, ვინაიდან მას არ გააჩნია უნარი გამოიყენოს თავისი მიმღები მონაცემთა გადაცემის დროს. ამიტომ მიმღებმა სადგურმა უნდა გააგზავნოს იმის დასტური *(acknowledgement, ACK)*, რომ მან ვერ აღმოაჩინა მიღებულ ფრეიმში შეცდომა. თუ გადამცემი სადგური რაღაც განსაზღვრული დროის განმავლობაში არ მიიღებს ACK-ს, ის დაასკვნის, რომ წარმოიშვა კოლოზია ან რადიოხარვეზების გამო ფრეიმი იყო დაზიანებული და გადააგზავნის განმეორებით.

ფრეიმების ოპერატიულად გადაცემის ხელშეწყობის მიზნით (მაგალითად, ვიდეოსიგნალების) 802.11 სტანდარტი გვთავაზობს PCF მექანიზმს. მისი გამოყენებით წვდომის წერტილი კონკრეტულ სადგურს აძლევს გარემოსადმი წვდომის გარანტიას, როდესაც სადგურებს შორის კონკურენციას არა აქვს ადგილი. სადგურებს არ შეუძლიათ ფრეიმების გადაცემა იქამდე, ვიდრე წვდომის წერტილი არ გამოკითხავს მათ გადმოსაცემი ფრეიმების არსებობის შესახებ.

წვდომის წერტილი გამოკითხავს სადგურებს, შემდეგ გადადის კონკურენციის რეჟიმში, რომლის დროსაც სადგურები

იყენებენ DCF მექანიზმს. ამის წყალობით ხდება ორივე რეჟიმისათვის მუშაობის ხელშეწყობა.

3.3.2. სკანირება და აუტენტიფიკაცია

802.11 სტანდარტი რეგლამენტირებას უკეთებს სკანირების 2 ვარიანტს – აქტიურს და პასიურს. ამ პროცესის მსვლელობისას ქსელის ინტერფეისის რადიოპლატა მოიძიებს წვდომის წერტილს. პასიური სკანირება არის აუცილებელი, მისი განხორციელებისას ქსელის ინტერფეისის თითოეული პლატა სკანირებას უკეთებს ცალკეულ არხს იმ მიზნით, რომ წვდომის წერტილიდან აღმოაჩინოს საუკეთესო სიგნალი. წვდომის წერტილები პერიოდულად და მრავლისმაუწყებელ რეჟიმში აგზავნის შუქურა სიგნალებს *(beacon)*. ქსელის ინტერფეისის რადიოპლატები იღებს ამ შუქურა სიგნალებს და ითვალისწინებს შესაბამისი სიგნალების დონეს. შუქურა სიგნალები შეიცავს ინფორმაციას წვდომის წერტილის შესახებ, მისი მომსახურების ზონების იდენტიფიკატორის ჩათვლით *(service set identifier, SSID)* და ხელს უწყობს მონაცემთა გადაცემის სიჩქარეს. ქსელის ინტერფეისის რადიოპლატა გამოიყენებს ამ ინფორმაციას და იღებს გადაწყვეტილებას იმის შესახებ, თუ რომელ წდომის წერტილს მიუერთდეს.

აქტიური სკანირება ხდება მსგავსი ხერხით იმ გამონაკლისით, რომ ეს პროცესი ინიცირდება ქსელის ინტერფეისის რადიოპლატით. იგი აგზავნის მრავლისმაუწყებელ ზონდირებულ ფრეიმს *(probe frame)*, ხოლო ყველა წვდომის წერტილი, რომელიც იმყოფება მოქმედების რადიუსში, უგზავნის მას ზონდირებულ ფრეიმზე პასუხს. აქტიური სკანირების წყალობით, ქსელის ინტერფეისის რადიოპლატას შეუძლია სწრაფად მიიღოს წვდომის წერტილებიდან პასუხები და არ დაელოდოს შუქურა სიგნალებს. თუმცა, აქტიური სკანირებისას ქსელში წარმოიშობა არამწარმოებლური დანახარჯები, განპირობებული ზონდირებული ფრეიმების გაგზავნით და მათზე პასუხების გადაცემით.

სადგურებს, რომლებიც მუშაობს დაუგეგმავი ქსელების რეჟიმში, 802.11 სტანდარტით, ეწოდებათ დამოუკიდებელი მომსახურების საბაზისო ზონა *(independent basic service set, IBSS)*. ამ რეჟიმში მუშაობის დროს ერთ-ერთი სადგური ყოველთვის უგზავნის შუქურა სიგნალებს სხვა სადგურებს ქსელის არსებობის შეტყობინებით. შუქურა სიგნალების გადაცემის პასუხისმგებლობა აკისრია ყველა სადგურს, რომელიც უცდის შუქურა ინტერვალის გასვლას. სადგური აგზავნის შუქურა სიგნალს იმ შემთხვევაში, როდესაც შუქურა ინტერვალის გასვლის შემდეგ ეს სდგური სხვა რომელიმე სადგურისგან არ მიიღებს შუქურა სიგნალს. აქედან გამომდინარე, შუქურა სიგნალების გადაცემის პასუხისმგებლობა გადანაწილებულია ყველა სადგურზე.

აუტენტიფიკაცია – ეს არის პროცესი, რომლის მსვლელობისას მოწმდება იდენტიფიკაცია. 802.11 სანდარტი რეგლამენტირებას უკეთებს შემოწმების 2 ფორმას: აუტენტიფიკაციის ღია სისტემას და აუტენტიფიკაციას ერთობლივად გამოსაყენებელი გასაღებით. აუტენტიფიკაციის ღია სისტემა არის აუცილებელი და მიმდინარეობს 2 ეტაპად. ქსელის ინტერფეისის რადიოპლატა ინიცირებას უკეთებს აუტენტიფიკაციის პროცესს და წვდომის წერტილს აუტენტიფიკაციაზე უგზავნის შეკითხვის ფრეიმს. წვდომის წერტილი უპასუხებს შეკითხვაზე, რომელიც შეიცავს თანხმობას ან უარს აუტენტიფიკაციაზე და მიეთითება ფრეიმის სტატუსის კოდის ველში *(status code)*.

აუტენტიფიკაცია ერთობლივად გამოსაყენებელი გასაღებით ხორციელდება 4 ეტაპად: პროცესი დაფუძნებულია იმის განსაზღვრისათვის, გააჩნია თუ არა აუტენტიფიკაციაზე მყოფ მოწყობილობას სწორი WEP-გასაღები. პროცესი იწყება ქსელის ინტერფეისის რადიოპლატიდან, იგი წვდომის წერტილს უგზავნის შეკითხვის ფრეიმს აუტენტიფიკაციაზე. წვდომის წერტილი ათავსებს გამოძახების ტექსტს ფრეიმის პასუხის ველში და უგზავნის მას ქსელის ინტერფეისის რადიოპლატას. ქსელის ინტერფეისის რადიოპლატა გამოძახების ტექსტის ამოშიფვრისათვის გამოიყენებს თავის WEP-გასაღებს და უბრუნებს ისევ წვდომის წერტილს სხვა ფრეიმის სახით აუტენტიფიკაციაზე. წვდომის წერტილი ამოშიფვრას უკეთებს გამოძახების ტექსტს და ადარებს თავდაპირველს. თუ ორივე ტექსტი ექვივალენტურია,

წვდომის წერტილი ასკვნის, რომ ქსელის ინტერფეისის რადიოპლატას გააჩნია კორექტული გასაღები. წვდომის წერტილი ასრულებს თანამიმდევრულად გაცვლის პროცესს და ქსელის ინტერფეისის რადიოპლატას უგზავნის თანხმობას ან უარს აუტენტიფიკაციაზე. ბევრმა ჰაკერმა იცის, თუ როგორ გადალახოს აუტენტიფიკაციის მეშვეობით შექმნილი ბარიერი, ამიტომ თუ საჭიროა უსაფრთხოების მაღალი დონის უზრუნველყოფა, მარტო ასეთ სისტემაზე დაყრდნობა არ ღირს.

აუტენტიფიკაციის პროცესის დასრულების შემდეგ ქსელის ინტერფეისის რადიოპლატა უნდა მიებას წვდომის წერტილს, რის შემდეგაც შესაძლებელი იქნება მონაცემთა ფრეიმების გადაცემა. ეს პროცესი იმისთვისაა აუცილებელი, რომ შემდეგ მოხდეს აუცილებელი ინფორმაციის გაცვლა ქსელის ინტერფეისის რადიოპლატასა და წვდომის წერტილებს შორის. ქსელის ინტერფეისის რადიოპლატა წვდომის წერტილს უგზავნის შეკითხვის ფრეიმს მიბმის შესახებ, შემდეგ წვდომის წერტილი ფრეიმის სახით უგზავნის შეკითხვაზე პასუხს, რომელიც შეიცავს ინფორმაციას იდენტიფიკატორისა და წვდომის წერტილის შესახებ. იმის შემდეგ, რაც ქსელის ინტერფეისის რადიოპლატა და წვდომის წერტილი დაასრულებენ მიბმის პროცესს, მათ შეეძლებათ ერთმანეთში გადასცენ მონაცემთა ფრეიმები.

ქსელის ინტერფეისის რადიოპლატას შეუძლია გადავიდეს ეკონომიის რეჟიმში. ამ დროს მომხმარებელს ენერგორესურსების ეკონომიის მიზნით შეუძლია გამორთოს ქსელის ინტერფეისის

რადიოპლატა, თუ მას არ სჭირდება მონაცემების გადაცემა. ამ პროცესის დროს ქსელის ინტერფეისის რადიოპლატა აცნობებს წვდომის წერტილს, რომ ის გადავიდეს „ძილის“ რეჟიმში. წვდომის წერტილი ითვალისწინებს ამ ყველაფერს და ბუფერიზაციას უკეთებს მონაცემთა პაკეტებს, რომლებიც გათვალისწინებულია „მძინარე“ სადგურისათვის. იმისათვის, რომ სადგურმა მიიღოს მისთვის განკუთვნილი მონაცემთა პაკეტები, ქსელის პლატა პერიოდულად უნდა მოვიდეს მოქმედებაში და მიიღოს წვდომის წერტილიდან რეგულარულად გამოგზავნილი შუქურა სიგნალი. სწორედ ამ სიგნალში ინახება ინფორმაცია იმის შესახებ, გააჩნია თუ არა წვდომის წერტილს „მძინარე“ სადგურისთვის ბუფერიზებული მონაცემთა ფრეიმები. ამის შემდეგ ქსელის ინტერფეისის რადიოპლატამ წვდომის წერტილს უნდა მოსთხოვოს მონაცემთა ფრეიმები. მონაცემთა ფრეიმების მიღების შემდეგ ქსელის ინტერფეისის რადიოპლატას შეუძლია დაუბრუნდეს „ძილის“ რეჟიმს.

802.11 სტანდარტის სადგურებს შეუძლიათ შეასრულონ ფრაგმენტაციის ფუნქცია, რაც ითვალისწინებს მონაცემთა ფრეიმების დაყოფას პატარა ფრეიმებად. ეს იმით არის კარგი, რომ რადიოხარვეზების დროს აუცილებელი არაა განმეორებით გადაიცეს დიდი ფრეიმები, ვინაიდან რადიოხარვეზებისაგან გამოწვეული შეცდომები იმოქმედებს მხოლოდ პატარა ფრეიმზე. აქედან გამომდინარე, ფრეიმების განმეორებით გადაცემისგან გამოწვეული არამწარმოებლური ხარჯებიც იქნება გაცილებით მცირე. ა

მომხმარებელსაც შეუძლია თვითონ დააყენოს გადასაცემი ფრეიმის მაქსიმალური ზომა, რისი გადაცილების შემთხვევაშიც სადგური აამოქმედებს ფრაგმენტაციის მექანიზმს.

3.4. ალიანსი Wi-Fi

ალიანსი Wi-Fi *(Wi-Fi Alliance)* წარმოადგენს საერთაშორისო არაკომერციულ ორგანიზაციას, რომელიც მუშაობს 802.11 სტანდარტის უმავთულო ლოკალური ქსელების კომპონენტების ურთიერთქმედების პრობლემებზე. ალიანსი Wi-Fi – ეს არის ჯგუფი, რომელიც ცნობილია ბრენდით „Wi-Fi“, რომლის გავლენაშიც ექცევა 802.11 სტანდარტის უმავთულო ქსელების ყველა ნაირსახეობა (802.11a, 802.11b და 802.11g), აგრეთვე ასეთი ტიპის ყველა სტანდარტი, რომელიც გაჩნდება მომავალში. ალიანსი Wi-Fi წინ წევს ტექნოლოგიას – დაცული წვდომა Wi-Fi-სადმი (Wi-Fi Protected Access, WPA), რომელიც არის დამაკავშირებელი რგოლი მრავალჯერ გაკრიტიკებულ WEP მექანიზმსა და 802.11 დაცვის სტანდარტს შორის.

ალიანსს Wi-Fi გააჩნია შემდეგი მიზნები:

– უზრუნველყოს მთელ მსოფლიოში სერტიფიცირება, რომელიც უბიძგებს მწარმოებლებს უმავთულო ლოკალური ქსელების კომპონენტების შემუშავებისას დაეყრდნონ 802.11 სტანდარტებს;

– ხელი შეუწყოს სერტიფიცირებული Wi-Fi ნაკეთობების გასაღებას იმისათვის, რომ წარმატებით იქნან გამოყენებული სახლის, ოფისებისა და სწარმოების პირობებში;

– გაუკეთოს ტესტირება და სერტიფიცირება Wi-Fi ნაკეთობებს ქსელების ურთიერთქმედების მიზნით.

3.4.1. რას ნიშნავს Wi-Fi?

სერტიფიკაცია Wi-Fi – ეს არის პროცესი, რისი წყალობითაც უზრუნველყოფილია უმავთულო ლოკალური ქსელების კომპონენტების ურთიერთქმედება, როგორებიცაა წვდომის წერტილები და რადიოპლატები, რომლებიც სრულდება სხვადასხვა ფორმ-ფაქტორებით. იმისათვის, რომ კომპანიამ თავის ნაწარმზე მიიღოს სერთიფიკატი, ის უნდა გახდეს ალიანსი Wi-Fi-ს წევრი.

ალიანსი ხელმძღვანელობს დამტკიცებულ ტესტირების პროგრამებს ნაკეთობების სერტიფიცირებისათვის, იმისათვის, რომ უზრუნველყოს ურთიერთქმედება სხვა სერტიფიცირებულ Wi-Fi კომპონენტებთან. მას შემდეგ, რაც ნაკეთობა წარმატებით გაივლის ტესტირების პროცესს, მისი მწარმოებელი იღებს იმის უფლებას,

რომ ყველა ცალკეული ნაკეთობისთვის, აგრეთვე მის შესაფუთ ყუთზე და მოხმარების ინსტრუქციაზე გამოიყენოს ლოგოტიპი „სერტიფიცირებულია Wi-Fi“.

სერტიფიკაცია Wi-Fi მომხმარებლებს არწმუნებს იმაში, რომ მათ შეიძინეს უმავთულო ლოკალური ქსელის ისეთი კომპონენტები, რომლებიც ურთიერთქმედებს ან შეესაბამება სხვა უამრავი მწარმოებლების ნაკეთობებს. ნაკეთობაზე მიმაგრებული ლოგოტიპი "Wi-Fi" ნიშნავს იმას, რომ მას ერთობლივად შეუძლია იმუშაოს სხვა მწარმოებლის მიერ Wi-Fi-სერტიფიცირებულ ნაკეთობებთან.

3.4.2. დაცული წვდომა Wi-Fi-სადმი

WEP მექანიზმი უმავთულო ლოკალური ქსელების სისტემების უმრავლესობისათვის საკმარისად ვერ უზრუნველყოფს უსაფრთხოების საჭირო ნორმებს, ვინაიდან ამ დროს გამოიყენება სტატიკური WEP გასაღები, რომლის გატეხვაც არსებული პროგრამული საშუალებების გამოყენებით მარტივია. ყოველივე ეს ინფორმაციული ტექნოლოგიების მენეჯერებს აიძულებს გამოიყენონ WEP-ის უფრო დინამიური ფორმები.

თუმცა დაცვის ეს გაუმჯობესებული მექანიზმები დაპატენტებულია, რაც ართულებს მათ მხარდაჭერას სამომხმარებლო

მოწყობილობებისთვის სხვა მომწოდებლებისაგან. აქედან გამომდინარე, Wi-Fi ალიანსმა მიიღო მნიშვნელოვანი ზომები უმავთულო ლოკალური ქსელების ეფექტური სტანდარტიზებული დაცვისათვის და განსაზღვრა WPA მექანიზმი, რომელიც უზრუნველყოფს ქსელების ურთიერთქმედებას. WPA-ს მოქმედების დროს, ქსელურ გარემოს, რომელიც ყალიბდება 802.11 სტანდარტის სხვადასხვა ტიპის ქსელის ინტერფეისის რადიოპლატების მიერ, შეუძლია გამოიყენოს დაშიფვრის გაფართოებული ფორმების უპირატესობები.

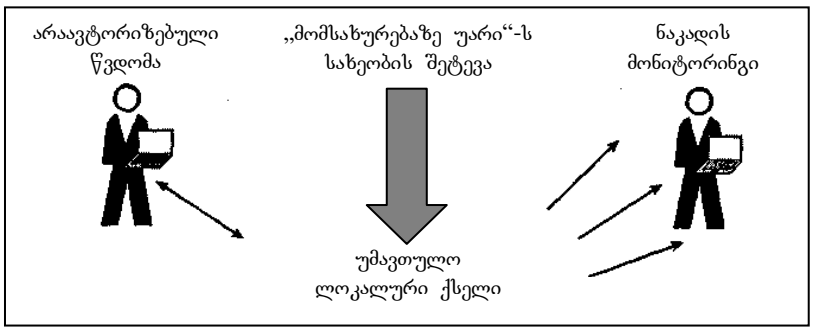
WPA 1.0 წარმოადგენს თავდაპირველ ვარიანტს, 802.11 სტანდარტის არარატიფიცირებულ ვერსიას, რომელიც შეიცავს გასაღების მთლიანობის დროებითი ოქმების *(temporal key integrity protocol, TKIP)* მექანიზმებს და 802.1x. ამ ორი მექანიზმის კომბინაცია საშუალებას იძლევა უზრუნველყოს დაშიფვრა ცვალებადი გასაღებით და ურთიერთქმედებითი აუტენტიფიკაცია, რომელიც ზოგჯერ აუცილებელია უმავთულო ლოკალური ქსელებისთვის.

თავი IV. უმავთულო ქსელების უსაფრთხოება

უსაფრთხოება უაღრესად მნიშვნელოვანი საკითხია უმავთულო ქსელებისათვის, ვინაიდან გარემოში გავრცელებული საკომუნიკაციო სიგნალები ხელმისაწვდომია დასაჭერად. აქედან გამომდინარე, კომპანიებმა და ინდივიდუალურმა მომხმარებლებმა უნდა შეიცნონ პოტენციურად არსებული პრობლემები და მიიღონ შესაბამისი ზომები. მეოთხე თავში განხილულია უმავთულო ქსელების გამოყენებასთან დაკავშირებული საფრთხეები და უმავთულო ქსელების დაცვის ხერხები დაშიფვრისა და აუტენტიფიკაციის მექანიზმების გამოყენებით.

4.1. არსებული საფრთხეები

არსებობს უმავთულო ქსელების გამოყენებასთან დაკავშირებული საფრთხეების სხვადასხვა ფორმა (ნახ. 4.1).



ნახ. 4.1. უმავთულო ქსელების გამოყენებასთან დაკავშირებული საფრთხეების სხვადასხვა ფორმა

მაგალითად, ჰაკერებს *(hackers)* შეუძლიათ მოახდინონ არაავტორიზებული შეღწევა ქსელური სისტემებში, ან თუნდაც დაარღვიონ ქსელის მუშაობა და მოიტაცონ კომპანიის ინფორმაცია.

4.1.1. ნაკადის მონიტორინგი

გამოცდილ ჰაკერს ან სულაც შემთხვევით სნუპერს (*snooper* – პირი, რომელსაც უყვარს ფარულად თვალთვალი) პროგრამული საშუალებების გამოყენებით შეუძლია ადვილად მოიძიოს უმავთულო ქსელის დაუცველი პაკეტები და მთლიანად გახსნას მასში არსებული მონაცემები. მაგალითად, სნუპერებს, რომლებიც იმყოფებიან რამდენიმე ასეული მეტრით დაშორებით შენობიდან, სადაც ფუნქციონირებს უმავთულო ლოკალური ქსელი, შესწევთ ძალა მოიძიონ ყველა ტრანზაქცია, რომელიც სრულდება უმავთულო ქსელის ნაწილში. რა თქმა უნდა, ძირითადი საფრთხე მდგომარეობს იმაში, რომ შეტევების შედეგად ვიღაცას შეიძლება ხელში ჩაუვარდეს ისეთი მნიშვნელოვანი ინფორმაცია, როგორიცაა მომხმარებლების სახელები და პაროლები, კრედიტ-კარტების ნომრები და სხვა.

ამ პრობლემის გადაწყვეტა მდგომარეობს იმაში, რომ მინიმუმ მოხდეს იმ ინფორმაციის დაშიფვრა, რომელიც გადაეცემა

უმავთულო მოწყობილობებსა და საბაზისო სადგურებს შორის. დაშიფვრის პროცესის დროს მონაცემთა ბიტები იცვლება საიდუმლო გასაღების დახმარებით. რადგანაც გასაღები საიდუმლოა, ჰაკერს არ შეუძლია მონაცემების ამოშიფვრა. აქედან გამომდინარე, ეფექტური მექანიზმების გამოყენების ხარჯზე დაშიფვრას შეუძლია აამაღლოს მონაცემთა დაცულობა.

4.1.2. არაავტორიზებული შეღწევა

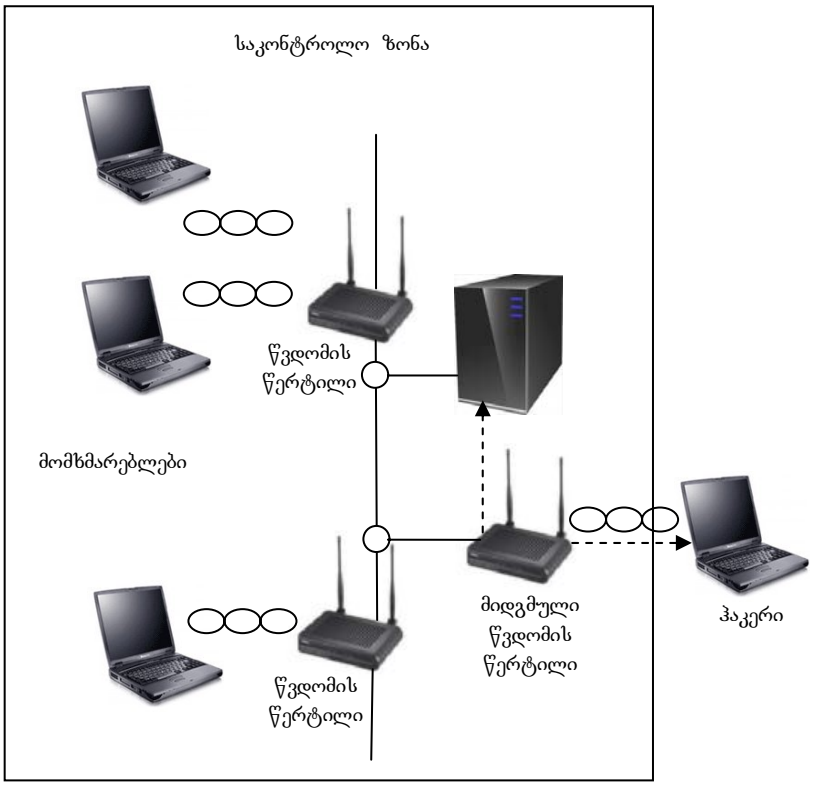
ანალოგიურად ნებისმიერს, რომელიც იმყოფება შენობის შორიახლოს, ყოველგვარი ძალისხმევის გარეშე, შეუძლია მონიტორინგის ჩატარება უმავთულო ქსელში არსებული სისტემების მიმართ, თუ არ არის მიღებული სიფრთხილის წინასწარი ზომები. მაგალითად, ვინმეს, რომელიც იმყოფება შენობის მახლობლად მდგარ ავტომობილში, შეუძლია მიებას შენობაში განლაგებული საბაზისო სადგურებიდან ერთ-ერთს. თუ არ არის მიღებული საჭირო დაცვის საჭირო ზომები, ასეთ პირს შეუძლია შეაღწიოს სერვერზე და სისტემებში, რომლებიც სრულდება კორპორატიულ ქსელში.

სამწუხაროდ, კომპანიების უმრავლესობა უმავთულო ქსელების გამართვის დროს იყენებს საბაზისო სადგურების კონფიგურაციას, რომელიც თავიდანვეა დაყენებული *(default)* და

ვერ უზრუნველყოფს უსაფრთხოების საჭირო ზომებს, რაც წინასწარ განსაზღვრავს სისტემების სერვერთან დაუბრკოლებელ ურთიერთქმედებას.

ოპერაციული სისტემა Windows XP, Vista საშუალებას იძლევა ადვილად დამყარდეს კავშირი უმავთულო ქსელებთან, განსაკუთრებით საერთო კავშირის მქონე ქსელებთან. როდესაც ნოუთბუქი მიებმება უმავთულო ლოკალურ ქსელს, მის მფლობელს შეუძლია შეაღწიოს ნებისმიერ სხვა ნოუთბუქში, რომელიც ჩართულია იმავე უმავთულო ლოკალურ ქსელში. თუ არ არის გამოყენებული პერსონალური ბრანდმაუერი, ნებისმიერს შეუძლია გაეცნოს ასეთი ნოუთბუქის მყარ დისკზე არსებულ ყველა ინფორმაციას,რაც წარმოადგენს უზარმაზარ საფრთხეს.

ხშირად, როდესაც წვდომის წერტილში ამოქმედებულია დაცვის მექანიზმები, არსებულ საფრთხეს წარმოადგენს მიდგმული წვდომის წერტილის *(rogue access point)* ჩართვის შესაძლებლობა. ასეთი წერტილი ითვლება არაავტორიზებულ წვდომის წერტილად, რომელიც მიერთებულია ქსელში. მაგალითად, რომელიმე მომსახურე პერსონალს შეუძლია შეიძინოს წვდომის წერტილი, არ გაითვალისწინოს ქსელის უსაფრთხოების ნორმები და დააყენოს იგი თავის ოფისში. სევ,ე ჰაკერს შეუძლია შენობაში განათავსოს წვდომის წერტილი, განზრახ შეაერთოს დაუცველი წვდომის წერტილი კორპორატიულ ქსელში (ნახ. 4.2).



ნახ. 4.2. მიდგმული წვდომის წერტილი ჰაკერებისთვის წარმოადგენს ღია პორტს

მიდგმულ წვდომის წერტილში, როგორც წესი, არ არის აქტივირებული დაშიფვრის სისტემა. აქედან გამომდინარე, იგი წარმოადგენს ყველასათვის ღია კარს, ვინც კი მოინდომებს შენობის გარედან შეაღწიოს კორპორატიულ ქსელში. ამიტომ კომპანიებმა ყოველთვის უნდა შეამოწმონ მიდგმული წვდომის წერტილების არსებობა. ეს პრობლემა აქტუალურია დამოუ-

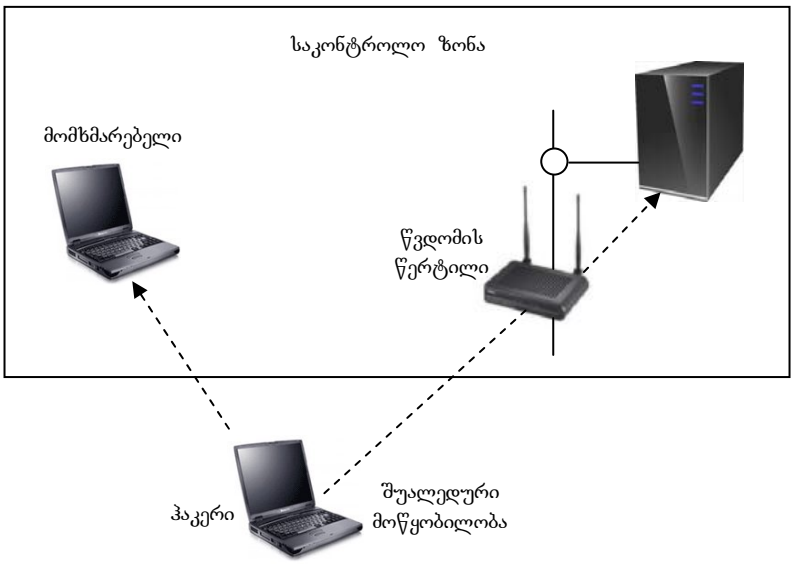
კიდებლად იმისა, დაყენებულია უმავთულო ქსელი თუ არა, ვინაიდან ვინმეს შეუძლია მიდგმული წვდომის წერტილი მიუერთოს მავთულიან ქსელს.

არაავტორიზებული შეღწევის საწინააღმდეგოდ უმავთულო ქსელში გამოიყენება ურთიერთქმედებითი აუტენტიფიკაცია, რომელიც ხორციელდება ქსელის მოწყობილობებსა და წვდომის წერტილებს შორის. აუტენტიფიკაცია – მოწმდება მომხმარებლის ან მოწყობილობის იდენტურობა. უმავთულო ქსელში უნდა გამოიყენებოდეს მეთოდები, რომლის საშუალებითაც ხდება საბაზისო სადგურის დარწმუნება ქსელის მოწყობილობის იდენტურობაში და პირიქით. ეს აუცილებელია იმისთვის, რომ მოხდეს ლეგიტიმურ საბაზისო სადგურებსა და მოწყობილობებს შორის შეერთება. გარდა ამისა, წვდომის წერტილები უნდა გადიოდნენ აუტენტიფიკაციის პროცედურებს კომუტატორზე, რაც ქსელში გამორიცხავს მიდგმული წვდომის წერტილების გამოჩენას.

4.1.3. „ადამიანი შუაში“ სახეობის შეტევა

აუტენტიფიკაციისა და დაშიფვრის მექანიზმების გამოყენების წყალობით იზრდება უმავთულო ქსელების უსაფრთხოება, მაგრამ გამოცდილი ჰაკერები ძებნიან სუსტ მხარეებს, იციან რა, თუ როგორ მუშაობს ქსელის ოქმები. განსაკუთრებულ საშიშროებას

წარმოადგენს „ადამიანი შუაში“ *(man-in-the-middle attacks)* სახეობის შეტევები. ჰაკერი განათავსებს ფიქტიურ მოწყობილობას ლეგალურ მომხმარებლებსა და უმავთულო ქსელს შორის (ნახ. 4.3). მაგალითად, სტანდარტული „ადამიანი შუაში“ სახეობის შეტევის განხორციელების დროს გამოიყენება მისამართების გარდამქმნელი ოქმი *(address resolution protocol, ARP)*, რომელიც გამოიყენება ყველა TCP/IP *(Transmission Control Protocol/Internet Protocol* – გადაცემის მართვის ოქმი/ინტერნეტ ოქმი) ქსელში. ჰაკერს, რომელიც შეიარაღებულია აუცილებელი პროგრამული საშუალებებით, ARP-ს გამოყენებით შეუძლია დაამყაროს კონტროლი უმავთულო ქსელზე.



ნახ. 4.3. შუალედური მოწყობილობა საშუალებას იძლევა განხორციელდეს „ადამიანი-შუაში“ სახეობის შეტევა

ARP ნებას რთავს შესრულდეს მთავარი ფუნქცია, რის-თვისაც იგზავნება მოთხოვნა უმავთულო ან მავთულიანი ქსელის ინტერფეისის პლატის მიმართ იმ მიზნით, რომ გამოვლინდეს პლატის ფიზიკური მისამართი – ეს იგივეა, რაც MAC-მისამართი, რომელიც მინიჭებულია პლატაზე მისი მწარმოებელის მიერ და განსხვავდება ქსელის სხვა ნებისმიერი კომპონენტის მისამარ-თისაგან, ანუ ის უნიკალურია. აქედან გამომდინარე, გადამცემმა ქსელის ინტერფეისის პლატამ უნდა იცოდეს მიმღების MAC-მისამართი. ეს პლატა ამოიცნობს და რეაგირებას ახდენს მხოლოდ ფიზიკურ MAC-მისამართზე.

გამოყენებით პროგრამებს, რომლებიც საჭიროებენ მონა-ცემების გადასაცემად, უნდა გააჩნდეს მიმღების IP მისამართი, ხოლო გადამცემი ქსელის ინტერფეისის პლატა იყენებს ARP ოქმს იმისათვის, რომ გამოავლინოს შესაბამისი ფიზიკური მისამართი. ის იღებს მისთვის საჭირო მისამართს, აგზავნის რა მრავლისაღმთქმელ ARP პაკეტებს, სადაც ცხადდება მიმღების ქსელის ინტერფეისის პლატის IP მისამართი. ყველა სადგურს აქვს შეხება მოთხოვნასთან და სადგურმა შესაბამისი IP მისამართით უნდა დააბრუნოს პასუხის პაკეტი ARP ოქმით, რომელიც შეიცავს MAC და IP მისამართებს. შემდეგ გადამცემი სადგური ჩართავს MAC-მისამართს გადასაცემ ფრეიმში, როგორც მიმღების მისამართს, აგრეთვე, რაღაც პერიოდის განმავლობაში ცხრილის სახით ინახავს შესაბამის MAC და IP მისამართებს

(ინახავს იქამდე, ვიდრე სადგური არ მიიღებს სხვა ARP პასუხს იმ სადგურისაგან, რომელსაც გააჩნია ეს IP მისამართი).

ARP ოქმთან დაკავშირებული პრობლემა არის ის, რომ დაცვის სისტემისთვის ის წარმოადგენს საფრთხეს, ვინაიდან ადგილი აქვს სპუფინგის (*spoofing* – კავშირის იმიტაცია, წვდომის მიღება მოტყუებითი გზით) შესაძლებლობას. ჰაკერს შეუძლია შუალედური მოწყობილობის საშუალებით სადგურს გაუგზავნოს ფიქტიური ARP-პასუხი, რომელიც შეიცავს ლეგიტიმური ქსელური მოწყობილობის IP მისამართს და შუალედური მოწყობილობის MAC მისამართს და სადგური შეიყვანოს შეცდომაში. ყველაფერი ეს მიიყვანს იქამდე, რომ ყველა ლეგიტიმური ქსელის სადგური ავტომატურად განაახლებს თავიანთ ARP-ცხრილებს, სადაც შეიტანება მცდარი მონაცემები. შედეგად სადგურები დაიწყებს პაკეტების გადაცემას შუალედური მოწყობილობის მისამართით და არა ლეგიტიმური წვდომის წერტილისკენ. სწორედ ეს არის კლასიკური შეტევა „ადამიანი შუაში“, რის შედეგადაც ჰაკერი იღებს იმის შესაძლებლობას, რომ მართოს მომხმარებელთან დაკავშირებული სეანსები. ის მიიღებს პაროლებს, მნიშვნელოვან მონაცემებს და შეძლებს კორპორატიულ სერვერებთან ურთიერთქმედებას ისე, რთითქოს ის არის ლეგიტიმური მომხმარებელი.

შეტევების თავიდან არიდების მიზნით ARP მომწოდებლები გვთავაზობენ დაცულ ARP-ს *(secure ARP, SARP)*. ასეთი გაუმჯობესებული ARP უზრუნველყოფს სპეციალურ დაცულ

გვირაბს ყველა მომხმარებელსა და წვდომის წერტილებსა ან მარშრუტიზატორებს შორის, რომელიც იგნორირებას უკეთებს ყველა იმ ARP-პასუხს, რომლებიც დაკავშირებული არაა იმ მომხმარებლებთან, რომლებიც იმყოფებიან გვირაბის მეორე ბოლოში. მაშასადამე, მხოლოდ ლეგიტიმური ARP-პასუხები მოემსახურება ARP-ცხრილების განახლების დაფუძნებას. სადგურებს, რომლებიც იყენებს SARP ოქმებს, მიდრეკილება არა აქვთ სპუფინგისადმი.

SARP ოქმის გამოყენებისთვის საჭიროა, რომ ყველა სამომხმარებლო მოწყობილობაზე დაყენდეს სპეციალური პროგრამული უზრუნველყოფა, ამიტომ SARP არ გამოიყენება საერთო კავშირის მქონე ქსელებისთვის, მაგრამ საწარმოებს თავიანთ სამომხმარებლო მოწყობილობებზე შეუძლიათ დააყენონ SARP, რათა თავი აირიდონ „ადამიანი შუაში“ სახეობის შეტევისაგან.

4.1.4. მომსახურებაზე უარი

„მომსახურებაზე უარი“ სახეობის შეტევა *(denial of service, DoS)* – ეს არის თავდასხმა, რის შედეგადაც უმავთულო ქსელი ხდება გამოუსადეგარი ან მისი მუშაობა იბლოკება. ასეთი შეტევის შესაძლებლობა უნდა გაითვალისწინოს ყველამ, ვინც კი გამართავს უმავთულო ქსელს. აუცილებელია დაფიქრება იმაზე, თუ რა

მოხდება, როდესაც ქსელი გახდება მიუწვდომელი განუსაზღვრელი დროით.

DoS შეტევის სერიოზულობა დამოკიდებულია იმაზე, თუ რა შედეგს გამოიწვევს უმავთულო ქსელის მწყობრიდან გამოსვლა. მაგალითად, ჰაკერს შეუძლია გახადოს მიუწვდომელი უმავთულო ლოკალური ქსელი, რომელიც გამართულია სახლში, ხოლო ამის შედეგი იქნება მხოლოდ სახლის მეპატრონის შეწუხება, მაგრამ საწარმოს ინვენტარიზაციის უმავთულო სისტემის მწყობრიდან გამოსვლა მნიშვნელოვან ფინანსურ დანაკარგებს გამოიწვევს.

DoS შეტევის სახესხვაობიდან ერთ-ერთს წარმოადგენს მეთოდი „უხეში ძალა“ *(brute-force attack)*. ინფორმაციული პაკეტების მასიური გაგზავნის დროს ამოქმედებულია ქსელის ყველა რესურსი და შედეგად ქსელი წყვეტს მუშაობას – ეს არის DoS შეტევის ვარიანტი, რომლის შესრულება ხდება მეთოდით „უხეში ძალა“. ინტერნეტში შეიძლება მოიძებნოს ისეთი პროგრამული საშუალებები, რომელიც შეაძლებინებს ჰაკერს უმავთულო ქსელში გამოიწვიოს ინფორმაციული პაკეტების ინტენსიური გადაცემა. ჰაკერს შეუძლია განახორციელოს DoS შეტევა მეთოდით „უხეში ძალა“ სერვერზე ქსელის სხვა კომპიუტერებიდან გამოუსადეგარი პაკეტების გაგზავნის გზით. ყოველივე ეს იწვევს ქსელში არამწარმოებლურ დანახარჯებს და ლეგიტიმურ მომხმარებლებს არ აძლევს საშუალებას გამოიყენოს ქსელში შესასვლელი შესაძლებლობა.

უმავთულო ქსელების მუშაობის გაჩერების სხვა ხერხს წარმოადგენს მეთოდი „შეგრძნების აღმოჩენა“ *(carrier sense access)*, სადაც გამოიყენება მძლავრი რადიოსიგნალი, რომელიც ახშობს სხვებს და აკეთებს ისე, რომ წვდომის წერტილები და ქსელის ინტერფეისის რადიოპლატები გამოუსადეგარი ხდება. მაგალითად, 802.11b-ს ოქმები გამოირჩევა „თავაზიანობით“, რაც საშუალებას აძლევს DoS შეტევის სიგნალს გადაცემის არეში ჰქონდეს წვდომა იმდენი ხანი, რამდენიც სურს ჰაკერს.

თუმცა, ქსელზე შეტევის განხორციელების მცდელობა მძლავრი რადიოსიგნალის გამოყენებით შეიძლება ჰაკერისთვის აღმოჩნდეს მეტად სარისკო, ვინაიდან ასეთი შეტევის განხორციელებისას მძლავრი გადამცემი უნდა განთავსდეს იმ შენობის უშუალო სიახლოვეს, სადაც ფუნქციონირებს უმავთულო ქსელი. აქედან გამომდინარე, უმავთულო ქსელის მფლობელს შეუძლია აღმოაჩინოს ჰაკერი აღმომჩენი საშუალებების გამოყენებით, რომლებიც მიეკუთვნება ქსელური ანალიზატორების ჯგუფს. მას შემდეგ, რაც აღმოჩენილი იქნება წინასწარგანსაზღვრული ხარვეზების წყარო, მისი მფლობელი იძულებული გახდება შეწყვიტოს შეტევა, ან სულაც განსასჯელის სკამზე აღმოჩნდესს.

გარდა ამისა, Dos შეტევას ხელს უწყობს დაცვის ზოგიერთი მექანიზმი. მაგალითად, WPA მექანიზმმა შეიძლება გამოიწვიოს „მომსახურებაზე უარი“ სახეობის შეტევა. WPA ქსელის მომხმარებლები აუტენტიფიკაციისათვის იყენებს მათემატიკურ ალგორითმებს. თუ რომელიმე მომხმარებელი შეეცდება

მიიღოს მისადმი წვდომა და ერთი წამის განმავლობაში გააგზავნის არაავტორიზებული მონაცემების ორ პაკეტს, WPA ჩათვლის, რომ გახდა შეტევის ობიექტი და ქსელის მუშაობას შეწყვეტს.

შედარებით მოქმედ დაცვას Dos შეტევის წინააღმდეგ წარმოადგენს უსაფრთხოების მკაცრი წესების შემუშავება და შესრულება, მაგალითად, როგორიც არის ბრანდმაუერების სისტემების დაყენება და განახლება, ანტივირუსული სისტემების მუდმივად განახლება, სიმბოლოების დიდი რაოდენობით პაროლების გამოყენება, არაგამოყენებადი ქსელური მოწყობილობების ქსელიდან გათიშვა და სხვა ყველა ის ქმედება, რომლებიც მკაცრად უნდა დაიცვას უმავთულო ქსელის ყველა მომხმარებლებმა.

უმავთულო ქსელის დაცვა შესაძლებელია გარედან რადიოსიგნალების შეღწევისაგან შენობის წინააღმდეგობის გაწევის უნარის უზრუნველყოფის გზით. არსებობს ზოგიერთი რეკომენდაცია, რომლის საშუალებითაც შესაძლებელია შენობაში რადიოსიგნალების ნაკადის შემცირება:

– თუ შენობის შიდა კედლებს გაჩნია ლითონის გამძლე ზედაპირი, სასურველია მოხდეს მისი დამიწება;

– სასურველია დაყენდეს თერმოიზოლაციის მქონე ფანჯრები და მოხდეს მისი მოლითონება;

– შენობის შიდა და გარე კედლებზე გამოყენებული იქნას ლითონის მინარევის საღებავი;

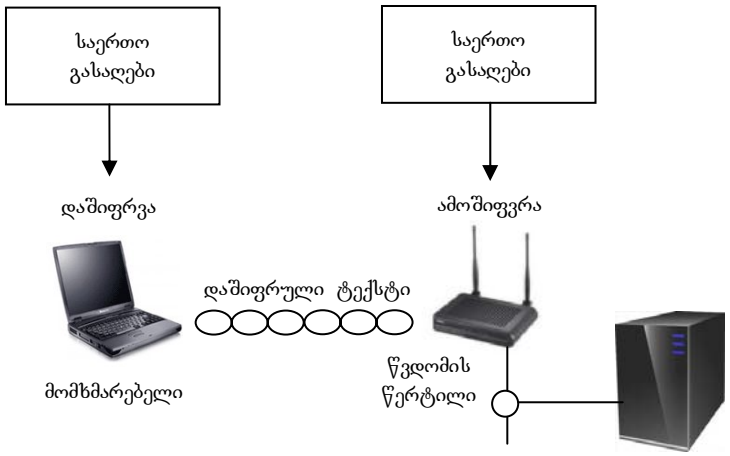
– მოხდეს გადამცემის სიმძლავრის დარეგულირება ისეთი სახით, რომ მთლიანად გამოირიცხოს სიგნალის გაჟონვა ან მისი დონე დაიწიოს ისეთ მნიშვნელობამდე,რომ შესაძლებელი იქნეს ჰაკერის ადვილად გამოვლინება.

უნივერსალური ხერხი, რომელიც გაუწევს წინააღმდეგობას Dos შეტევის ყველა სახეობას, არ არსებობს. აქედან გამომდინარე, თუ Dos შეტევის შედეგად ქსელი გამოვიდა მწყობრიდან, სასურველია მოხდეს გადასვლა ქაღალდის დოკუმენტების დამუშავებაზე, ვიდრე უმავთულო ქსელის პოტენციური ნაკლოვანებების გამო კომპანია მივიდეს გაკოტრების პირას.

4.2. დაშიფვრა

დაშიფვრა ცვლის მონაცემთა პაკეტის თითოეულ ბიტს იმ მიზნით, რომ ბოროტგანმზრახველმა ვერ შეძლოს მისი დეკოდირება. არადაშიფრულ მონაცემებს ეძახიან ღია ტექსტს *(plaintext)*, რომლის დეკოდირებაც მარტივია. დაშიფვრის პროცესში ღია ტექსტი გარდაიქმნება დაშიფრული სახით, ხოლო მისი დეკოდირება შეიძლება მხოლოდ საიდუმლო გასაღების დახმარებით.

დაშიფვრის მეთოდების უმრავლესობა, როგორიცაა, მაგალითად, 802.11 სტანდარტის WEP მეთოდი, რომელიც იძლევა დაცვის გარანტიას, სიმეტრიულია. ეს იმას ნიშნავს, რომ დაშიფვრისა და ამოშიფვრისათვის გამოიყენება ერთი და იგივე გასაღები (ნახ. 4.4).



ნახ. 4.4. სიმეტრიული დაშიფვრისას გამოიყენება საერთო გასაღები

მაგალითად, ქსელის ინტერფეისის რადიოპლატას მონაცემთა პაკეტის დაშიფვრისათვის შეუძლია გამოიყენოს *xyz* გასაღები, ხოლო წვდომის წერტილი *xyz* გასაღების დახმარებით მოახდენს მის ამოშიფვრას. ამისათვის საჭიროა, რომ გადამცემი და მიმღები სადგურები ერთმანეთს ენდობოდნენ, რასაც ადგილი აქვს პირადი უმავთულო ქსელის გამოყენებისას, როგორიცაა, მაგალითად, საწარმოს უმავთულო ქსელი. თუმცა, აზრი არა აქვს სიმეტრიული გასაღებების გამოყენებას საერთო კავშირის მქონე ქსელებში, ვინაიდან ის შეუძლია მიიღოს ნებისმიერმა აბონენტმა, მათ შორის-ჰაკერმაც.

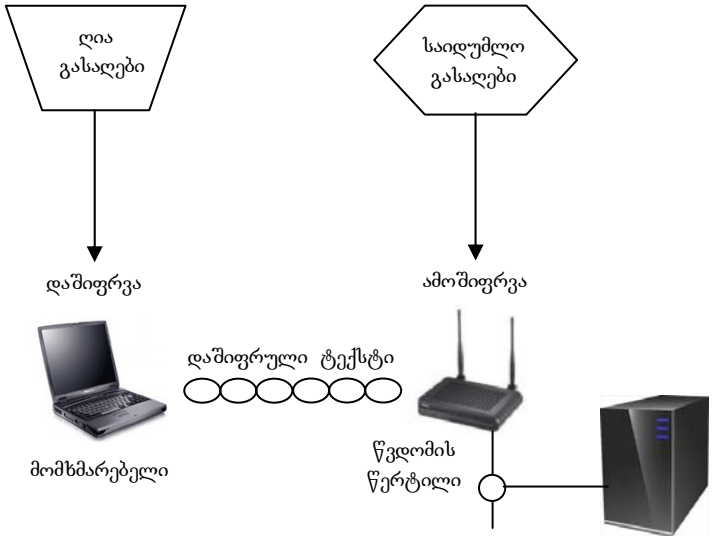
იმისათვის, რომ სიმეტრიული დაშიფვრის მეთოდი იყოს ეფექტური, საჭიროა გასაღების განმეორებით გამოყენების მინიმიზაცია გასაღების ხშირად გამოცვლის გზით, სასურველია, თითოეული ფრეიმის გადაცემის შემდეგ. ყოველივე ეს ხელს უწყობს იმას, რომ ჰაკერს ქსელში შეღწევის დრო გაუხანგრძლივდეს (ან შეღწევა შეუძლებელი გახდეს) და აბრკოლებს ქსელში დაცვის სისტემის დარღვევას.

კრიპტოგრაფია ღია გასაღებით დაფუძნებულია ასიმეტრიული გასაღებების გამოყენებაზე, რომელთაგან ერთ-ერთი წარმოადგენს საიდუმლოს, ხოლო მეორე – ღიას. როგორც დასახელებიდან იგულისხმება, საიდუმლო გასაღები ხელმისაწვდომია მხოლოდ მისი მფლობელისთვის, ხოლო ღია გასაღები ცნობილია ყველასთვის. ეს საშუალებას იძლევა შევქმნათ დაშიფვრისა და

აუტენტიფიკაციის შედარებით ეფექტური მექანიზმები, ვინაიდან მარტივდება ღია გასაღების განაწილების მეთოდები.

მნიშვნელოვან პირობას, წაყენებულს ღია გასაღებით დაშიფვრის მეთოდისადმი, წარმოადგენს შემდეგი: წყვილი „საიდუმლო გასაღები – ღია გასაღები“ უნდა იყოს თანასწორუფლებიანი კრიპტოგრაფიული თვალსაზრისით. მაგალითად, გადამცემ სადგურს შეუძლია მონაცემების დაშიფვრა ღია გასაღების დახმარებით, მაშინ მიმღები სადგური გამოიყენებს თავის საიდუმლო გასაღებს, რათა ამოშიფროს მონაცემები. ასევე შესაძლებელია საპირისპირო ვარიანტიც. გადამცემი სადგური მონაცემებს დაშიფრავს საიდუმლო გასაღების დახმარებით, ხოლო მიმღები სადგური გამოიყენებს ღია გასაღებს და ამოშიფრავს მონაცემებს.

თუ მიზანს წარმოადგენს მონაცემების დაშიფვრა, მაშინ გადამცემი სადგური მონაცემების გადაცემამდე მის დასაშიფრად გამოიყენებს ღია გასაღებს. მიმღები სადგური გამოიყენებს შესაბამის საიდუმლო გასაღებს მიღებული მონაცემების ამოსაშიფრად (ნახ. 4.5). თითოეული სადგური მალავს თავის საიდუმლო გასაღებს სხვებისგან, რათა დაშიფრული მონაცემების არასანქცირებულად ამოშიფვრით საფრთხეში არ ჩაიგდოს თავი. აქედან გამომდინარე, ზემოთაღნიშნული პროცესი ყველა სადგურს საშუალებას აძლევს გამოიყენოს ყველასათვის ცნობილი გასაღები დაშიფრული მონაცემების გადასაცემად სხვა ნებისმიერი სადგურისაკენ.



ნახ. 4.5. დაშიფვრა ღია გასაღებით

კრიპტოგრაფია ღია გასაღებით ეფექტურია მონაცემების დაშიფვრისათვის, ვინაიდან ღია გასაღები ადვილად გადაეცემა ყველას, ვისაც სურს განსაზღვრულ სადგურს გადასცეს დაშიფრული მონაცემები. სადგურს, რომელიც აგენერირებს ახალ საიდუმლო გასაღებს, შეუძლია ქსელით ნებისმიერს გადასცეს მისთვის შესაბამისი ღია გასაღები, ან განათავსოს ინტერნეტში.

4.2.1. მექანიზმი WEP

მექანიზმი WEP – ეს არის დაშიფვრისა და აუტენტიფიკაციის სტანდარტი, რომელიც გამოიყენება MAC დონეზე. მას შეესაბამება მწარმოებლების უმრავლესობის მიერ გამოშვებული

ქსელის ინტერფეისის რადიოპლატები და წვდომის წერტილები. უმავთულო ქსელის გამართვისას საჭიროა მტკიცედ ვიცოდეთ, თუ რა შესაძლებლობებს იძლევა WEP დაცვის ასამაღლებლად.

თუ მომხმარებელი გააქტიურებს WEP მექანიზმს, მონაცემების გადაცემამდე ქსელის ინტერფეისის რადიოპლატა შიფრავს 802.11 სტანდარტის თითოეულ ფრეიმს. კონტროლი ხორციელდება ციკლური მოჭარბებული კოდის გამოყენებით *(cyclical redundancy check, CRC)*. გადაცემის დროს გამოიყენება დაშიფვრის ნაკადური მექანიზმი, რომელიც უზრუნველყოფილია დაცვის სისტემით RSA (ალგორითმი – ასიმეტრიული დაშიფვრა ღია გასაღებით). მიმღები სადგური (მაგალითად, წვდომის წერტილი ან სხვა ქსელის ინტერფეისის რადიოპლატა) ამოშიფრავს მიღებულ ფრეიმს. მაშასადამე, 802.11 სტანდარტის WEP შიფრავს მხოლოდ იმ მონაცემებს, რომელიც გადაეცემა 802.11 სტანდარტის სადგურებს შორის. როგორც კი ფრეიმი მიაღწევს მავთულიან ნაწილს, როგორც ეს ხდება ხოლმე ერთი წვდომის წერტილიდან მეორეში გადაცემის დროს, WEP უკვე აღარ მუშაობს.

WEP მონაცემების დაშიფვრისა და ამოშიფრისათვის რეგლამენტირებას უკეთებს საერთო გასაღების გამოყენებას. WEP-ის გამოყენების დროს მიმღებმა სადგურმა ამოშიფრისათვის უნდა გამოიყენოს იგივე გასაღები. მაშასადამე, თითოეული წვდომის წერტილი და ქსელის ინტერფეისის რადიოპლატა უნდა იყოს რ ხელით დაკონფიგურირებული ერთი და იგივე გასაღებით.

WEP-ს გააჩნია თავისი ნაკლოვანებები, ვინაიდან დაშიფვისათვის გამოიყენება მოკლე ინიციალიზაციის ვექტორები *(initialization vector, IV)* და შეუცვლელი გასაღებები. WEP-ის გამოყენებასთან დაკავშირებული პრობლემები განპირობებულია დაშიფვრის ალგორითმის გამოყენებასთან. WEP იყენებს 24-თანრიგიან ინიციალიზაციის ვექტორს (IV) და ადრე თუ გვიან გამოიყენებს იგივე IV-ს სხვა მონაცემთა პაკეტისათვის. საწარმოს დიდ ქსელებში IV განმეორება შეიძლება მოხდეს ერთი საათის განმავლობაში. თუ ჰაკერი დააგროვებს საკმარის ფრეიმებს, რომლებიც დაფუძნებულია ერთი და იგივე IV-ზე, მას შეუძლია განსაზღვროს ერთობლივად გამოსაყენებელი საიდუმლო გასაღები. ეს კი გამოიწვევს იმას, რომ ჰაკერი შეძლებს 802.11 სტანდარტის ნებისმიერი ფრეიმის ამოშიფვრას.

802.11 სტანდარტს არ გააჩნია არანაირი ფუნქცია, რომელიც უზრუნველყოფს სადგურებს შორის გასაღებების გაცვლას. აქედან გამომდინარე, სისტემური ადმინისტრატორები და მომხმარებლები იყენებენ ერთი და იგივე გასაღებს კვირების ან თვეების განმავლობაში. ყოველივე ეს დამნაშავეებს აძლევს საკმარის დროს, რომ ჩაატარონ ნაკადის მონიტორინგი და შეაღწიონ ქსელში.

მიუხედავად WEP-ის ნაკლოვანებებისა, მისი გამოყენება სასურველია, რათა მოხდეს უსაფრთხოების მინიმალური დონის უზრუნველყოფა. უმრავლესობას გააჩნია ღია უმავთულო ქსელი, სადაც გამოიყენება ოქმების ანალიზატორები და არ არის ჩართული WEP მექანიზმი. აქედან გამომდინარე, ჰაკერებს ყოველ-

გვარი ძალიხსმევის გარეშე შეუძლიათ გამოავლინონ ასეთი ქსელები და შეაღწიონ მასში.

4.2.2. გასაღების მთლიანობის დროებითი ოქმი

802.11 სტანდარტი იძლევა უმავთულო ლოკალური ქსელების დაცვის მექანიზმების გაუმჯობესების საშუალებას. ერთ-ერთი უახლესი არის გასაღების მთლიანობის დროებითი ოქმი *(temporal key integrity protocol, TKIP),* რომელიც თავიდან იწოდებოდა WEP2. TKIP ოქმი, ეს არის გადაწყვეტა, რომელიც დაფუძნებულია 128-თანრიგიანი გასაღების გამოყენებაზე, რომელიც ერთობლივად გამოიყენება მომხმარებლებისა და წვდომის წერტი-ლების მიერ. TKIP კომბინირებას უკეთებს დროებით გასაღებს და სამომხმარებლო მოწყობილობის MAC-მისამართს, ხოლო შემდგომ ამატებს 16-თანრიგიან ინიციალიზაციის ვექტორს, რისი საშუა-ლებითაც მოხდება მონაცემების დაშიფვრა. ეს პროცედურა იძლევა იმის გარანტიას, რომ ყველა სადგური მონაცემების დასაშიფრად გამოიყენებს სხვადასხვა გასაღებების ნაკადს.

TKIP დაშიფვრისათვის იყენებს ასიმეტრიული დაშიფვრის ალგორითმს, რომელიც ანალოგიურია WEP-ისა. მათ შორის ძირითადი განსხვავება მდგომარეობს იმაში, რომ TKIP 10 ათასი

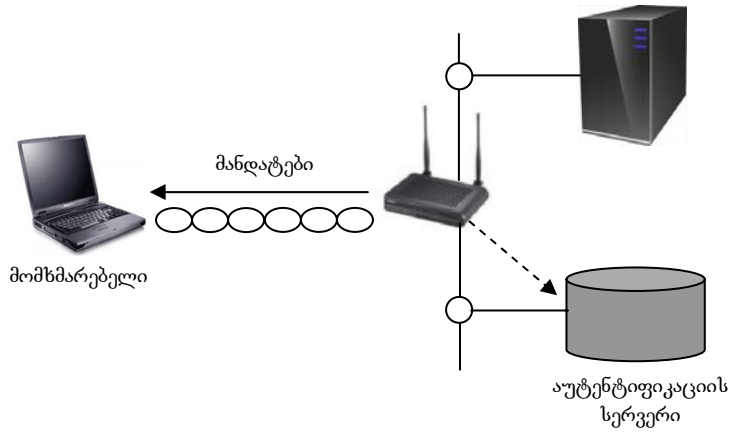
პაკეტის გადაცემის შემდეგ ცვლის დროებით გასაღებებს, რისი წყალობითაც მნიშვნელოვნად იზრდება ქსელის უსაფრთხოება.

TKIP-ის დაშიფვრის გამოყენების უპირატესობა მდგომარეობს იმაში, რომ კომპანიების, რომლის წვდომის წერტილები და ქსელის ინტერფეისის რადიოპლატები დაფუძნებულია WEP მექანიზმზე, მოდერნიზება TKIP დონეზე შესაძლებელია მარტივი ქმედებებით. მაგრამ ექსპერტების აზრით TKIP – ეს არის დროებითი გადაწყვეტა და აუცილებელია დაშიფვრის ძლიერი მეთოდების შექმნა.

4.3. აუტენტიფიკაცია

უმავთულო ქსელში აუცილებელია გამოყენებულ იქნას ორმხრივი აუტენტიფიკაცია. მისი წყალობით შესაძლებელია უამრავი პრობლემების გადაწყვეტა, რომლებიც დაკავშირებულია უსაფრთხოებასთან. მაგალითად, შესაძლებელია წარმატებით აღვუდგეთ წინ შეტევას „ადამიანი შუაში“. ორმხრივი აუტენტიფიკაციის დროს უმავთულო მომხმარებელი და უმავთულო ქსელი ერთმანეთს უმტკიცებს თავიანთ იდენტურობას (ნახ. 4.6). ამ პროცესის კვალდაკვალ გამოიყენება აუტენტიფიკაციის სერვერი

RADIUS (remote authentification dial-in user service – მომხმარებლების დისტანციური აუტენტიფიკაციის სამსახური).



ნახ. 4.6. აუტენტიფიკაციის დროს მოწმდება მოწყობილობების იდენტურობა

4.3.1. აუტენტიფიკაციის მექანიზმის ნაკლოვანება

WEP უზრუნველყოფს მხოლოდ ქსელის ინტერფეისის რადიოპლატის აუტენტიფიკაციის მეთოდს წვდომის წერტილისადმი, საპირისპირო ოპერაცია არ სრულდება. აქედან გამომდინარე, ჰაკერს შეუძლია მონაცემების გადაგზავნა სხვა გზით, დაცვის სხვა მექანიზმების გვერდის ავლით. ასეთი შესაძლებლობა რომ აღმოიფხვრას, უმავთულო ქსელებში უნდა გამოიყენებოდეს არა ერთმხრივი, არამედ ორმხრივი აუტენტიფიკაცია.

როდესაც უმავთულო მომხმარებელი გადადის აქტიურ ფაზაში, ის იწყებს გადასაგზავნი გარემოს ძებნას შუქურა სიგნალებით, რომელსაც წვდომის წერტილები მრავლისმაუწყებელ რეჟიმში პერიოდულად აგზავნის. შუქურა სიგნალები შეიცავს წვდომის წეტილის მომსახურების ზონის იდენტიფიკატორს (SSID) და სხვა პარამეტრებს. წვდომის წერტილი მასზე მიბმის ნებართვას იძლევა მხოლოდ მაშინ, როდესაც მომხმარებლისა და წვდომის წერტილის SSID-ები ერთმანეთს შეესაბამება. სწორედ ეს წარმოადგენს აუტენტიფიკაციის ძირითად (თუმცა სუსტ) ფორმას.

ამ პროცესის ნაკლოვანება ძირითადად გამოწვეულია იმით, რომ SSID გადაიცემა არადაშიფრული ფორმით, რაც უმავთულო მონაცემთა პაკეტებზე სპეციალური დაკვირვების პროგრამების საშუალებით ხდის მათ ხილვადს. აქედან გამომდინარე, ჰაკერს შეუძლია შუქურა ფრეიმში ადვილად აღმოაჩინოს SSID და აუტენტიფიკაცია მოახდინოს უმავთულო ქსელთან.

801.11 სტანდარტი გვთავაზობს აუტენტიფიკაციის ფორმას, რომელსაც ქვია „ღია აუტენტიფიკაციის სისტემა“. ასეთ რეჟიმში მუშაობის დროს წვდომის წერტილი აუტენტიფიკაციაზე ნებისმიერი მოთხოვნის შესრულების გარანტიას იძლევა. მომხმარებელი უბრალოდ აგზავნის მოთხოვნის ფრეიმს აუტენტი-ფიკაციაზე, ხოლო წვდომის წერტილი იძლევა დადებით პასუხს. ეს აძლევს ნებისმიერს, რომელმაც იცის კორექტული SSID, იმის საშუალებას, რომ მიებას წვდომის წერტილს.

801.11 სტანდარტი აგრეთვე რეგლამენტირებას უკეთებს აუტენტიფიკაციას ერთობლივად გამოსაყენებელი გასაღებით, რომელიც წარმოადგენს აუტენტიფიკაციის შედარებით თანამედროვე ფორმას. პროცესის შესრულება მიმდინარეობს 4 ეტაპად:

1) მომხმარებელი აგზავნის მოთხოვნის ფრეიმს აუტენტიფიკაციაზე;

2) წვდომის წერტილი უპასუხებს ფრეიმით, რომელიც შეიცავს ტექსტს და ეწოდება „გამოძახების ტექსტი“ (challenge text);

3) მომხმარებელი დაშიფვრის WEP საერთო გასაღების გამოყენებით შიფრავს გამოძახების ტექსტს და დაშიფრულ ტექსტს უბრუნებს წვდომის წერტილს, რომელიც აგრეთვე საერთო გასაღების დახმარებით ამოშიფრავს ამ ტექსტს და შედეგს ადარებს გამოძახების ტექსტს;

4) თუ ტექსტები ემთხვევა, მომხმარებელი მიებმება წვდომის წერტილს.

ყოველივე ეს სრულიად საკმარისია აუტენტიფიკაციის თვალსაზრისით, მაგრამ პრობლემა მდგომარეობს იმაში, რომ ერთობლივად გამოსაყენებელი გასაღების არსებობა ამტკიცებს მხოლოდ იმას, რომ მომხმარებელს გაჩნია კორექტული WEP-გასაღები.

4.3.2. MAC-ფილტრები

ზოგიერთი უმავთულო საბაზისო სადგურე გვთავაზობს ფილტრაციას გარემოსადმი წვდომის მართვის დონეზე (MAC-დონეზე). MAC-ფილტრაციის გამოყენების დროს წვდომის წერტილი ამოწმებს თითოეული მიღებული ფრეიმის წყაროს MAC-მისამართს და უარს ამბობს ისეთი ფრეიმების MAC-მისამართების მიღებაზე, რომლებიც არ შეესაბამება ქსელის ადმინისტრატორის მიერ დაპროგრამებული სიიდან არცერთს.

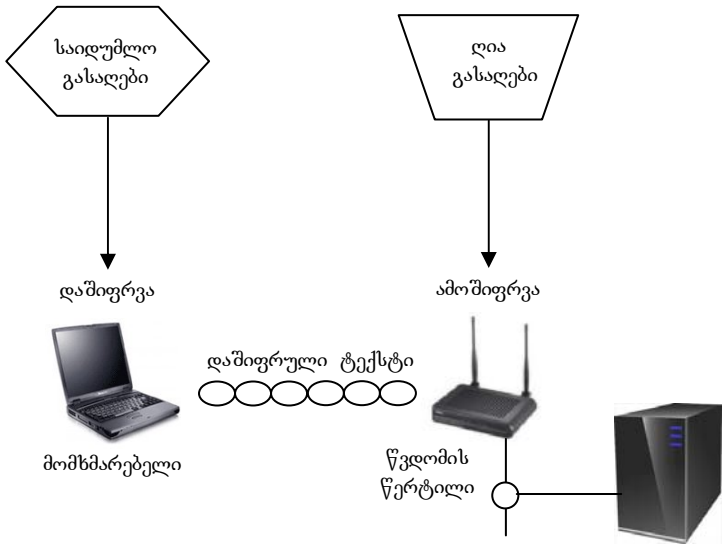
მაგრამ MAC-ფილტრაციას გააჩნია სუსტი ადგილები. მაგალითად, WEP-დაშიფვრის დროს ფრეიმის ველის მნიშვნელობა, რომელიც შეიცავს MAC-მისამართს, არ იშიფრება. ეს საშუალებას აძლევს ჰაკერს დააკვირდეს ფრეიმების გადაცემას და გამოავლინოს მოქმედი MAC-მისამართები, ან შეუძლია არსებული პროგრამული უზრუნველყოფის დახმარებით შეცვალოს თავისი ქსელის ინტერფეისის რადიოპლატის MAC-მისამართი ისეთი სახით, რომ შეესაბამებოდეს მოქმედ MAC-მისამართს. ეს ჰაკერს აძლევს იმის საშუალებას, რომ „მოატყუოს“ წვდომის წერტილი იმ დროს, როდესაც ლეგალური მომხმარებელი გასულია ქსელიდან.

გარდა ამისა, ყველა მომხმარებლისათვის MAC-ფილტრაციის მექანიზმის ამოქმედება ქსელში ძალზედ დამღლელი პროცესია. ქსელის ადმინისტრატორმა თითოეული მომხმარებლისათვის ცხრილში უნდა შექმნას ჩანაწერი მათი MAC-მისამართებით და ახალი

მომხმარებლის შემთხვევაში ცხრილში მოახდინოს შესაბამისი ცვლილება.

4.3.3. აუტენტიფიკაციის ღია გასაღების სისტემა

ინფორმაციის დაცვის ერთ-ერთ დამატებით საშუალებას წარმოადგენს ის, რომ სადგურებს შეუძლია გამოიყენოს ღია გასაღების სისტემა სხვა სადგურებთან ან წვდომის წერტილებთან აუტენტიფიკაციისათვის (ნახ. 4.7).



ნახ. 4.7. ღია გასაღების სისტემა საშუალებას იძლევა განხორციელდეს აუტენტიფიკაცია

ყოველი ეს პროცესი აუცილებელია იქამდე, ვიდრე წვდომის წერტილი საშუალებას მისცემს განსაზღვრულ სადგურს დაიწყოს ურთიერთქმედება ქსელის დაცულ ნაწილთან. სადგური აუტენტიფიკაციას უკეთებს თავის თავს მონაცემთა პაკეტში საიდუმლო გასაღების დახმარებით ტექსტის დაშიფვრის გზით. მიმღები სადგური ღია გასაღების დახმარებით ამოშიფრავს გადამცემი სადგურის ტექსტს. თუ ამოშიფრული ტექსტი დაემთხვა რომელიმე წინასწარგანსაზღვრულ ტექსტს (მაგალითად, სადგურის სახელი), მიმღები სადგური ჩათვლის, რომ გადამცემი სადგური არის ლეგიტიმური.

4.3.4. სტანდარტი 802.1x

802.1x სტანდარტის გამოყენების ხარჯზე საფუძველი ჩაეყარა ავტომატური აუტენტიფიკაციის ეფექტურ სისტემებს და დაცული ქსელის მომხმარებლების ნაკადის კონტროლს, აგრეთვე დინამიურად ცვალებადი დაშიფვრის გასაღების გამოყენებას. 802.1x სტანდარტი მავთულიან და უმავთულო ქსელის ნაწილებში იყენებს აუტენტიფიკაციის გამაფართოებელ ოქმს *(extensible authentication protocol, EAP)* და მხარს უჭერს ორმხრივი აუტენტიფიკაციის მეთოდებს, როგორებიცაა ერთჯერადი პარო-

ლები *(one-time passwords)*, სერტიფიკატები *(certificates)* და აუტენტიფიკაცია ღია გასაღებით *(public key authentication)*.

802.1x სტანდარტის შესაბამისად კავშირის დამყარება იწყება იმით, რომ მთხოვნელი *(supplicant)*, ანუ უმავთულო სამომხმარებლო მოწყობილობა, ცდილობს მიუერთდეს უმავთულო საბაზისო სადგურს, რომელიც მთხოვნელს უპასუხებს იმით, რომ იგი წარმოუდგენს მას პორტს აუტენტიფიკაციის სერვერზე მხოლოდ EAP-პაკეტების გადასაცემად, რომელიც განთავსებულია საბაზისო სადგურის მავთულიან ნაწილში. საბაზისო სადგური ბლოკავს სხვა დანაჩენ ნაკადებს, როგორიცაა HTTP, DHCP და POP3 პაკეტები, იქამდე, ვიდრე აუტენტიფიკაციის სერვერის დახმარებით არ დარწმუნდება მთხოვნელის იდენტურობაზე. წარმატებული აუტენტიფიკაციის შემდეგ საბაზისო სადგური ხსნის პორტს ყველა დანარჩენი ნაკადისათვის, ამასთან ერთად ხელმძღვანელობს აუტენტიფიკაციის სერვერის მითითებებით.

იმისათვის, რომ საფუძვლიანად გავერკვეთ იმაში, თუ როგორ ხორციელდება აუტენტიფიკაციის პროცესი 802.1x სტანდარტის შესაბამისად, განვიხილოთ თითოეული ეტაპი და ვნახოთ, თუ როგორ ურთიერთქმედებს უმავთულო ქსელის მოწყობილობები ერთმანეთის მიმართ:

1) მომხმარებელი საბაზისო სადგურს უგზავნის სასტარტო EAP-შეტყობინებას აუტენტიფიკაციის მიზნით;

2) საბაზისო სადგური უპასუხებს შეტყობინებით, რომელიც შეიცავს EAP-იდენტიფიკაციის მოთხოვნას;

3) მომხმარებელი აგზავნის პაკეტს EAP-პასუხით, რომელიც შეიცავს აუტენტიფიკაციის სერვერისათვის აუცილებელ მონაცემებს;

4) აუტენტიფიკაციის სერვერი მომხმარებლის იდენტიფიკაციისათვის იყენებს განსაკუთრებულ აუტენტიფიკაციის ალგორითმს. შემოწმების პროცესი შეიძლება განხორციელდეს ციფრული სერტიფიკატების გამოყენებით ან სხვა EAP აუტენტიფიკაციის მექანიზმებით;

5) აუტენტიფიკაციის სერვერი საბაზისო სადგურს უგზავნის შეტყობინებას მომხმარებლის იდენტიფიკაციის შესახებ – თანხმობას ან უარს;

6) საბაზისო სადგური მომხმარებელს უგზავნის შეტყობინების პაკეტს წარმატებული აუტენტიფიკაციის შესახებ;

7) თუ აუტენტიფიკაციის სერვერი იღებს მომხმარებელს, საბაზისო სადგურმა მისთვის გამოყოფილი პორტი უნდა გადაიყვანოს ავტორიზებულ მდგომარეობაში და უზრუნველყოს დამატებითი ნაკადის გადაცემა.

802.1x სტანდარტის ძირითადი ოქმი უზრუნველყოფს ეფექტურ აუტენტიფიკაციას დამოუკიდებლად იმისა, გამოიყენება თუ არა WEP-გასაღები ან დაშიფვრის მეთოდები. უმავთულო ქსელების ძირითადი მომწოდებლების უმრავლესობა გვთავაზობს დინამიური გასაღებების მართვის დაპატენტებულ ვერსიებს, რომელსაც იყენებს 802.1x სტანდარტი, როგორც მათი განაწილების მექანიზმი.

დაცვის სისტემა – ეს არის უმავთულო ქსელის ერთ-ერთი მნიშვნელოვანი და რთული ელემენტი. ჰაკერების გამოცდილება იძლევა იმას, რომ მათ შეუძლიათ თვალი ადევნონ ინფორმაციულ ნაკადებს, მიიღონ არაავტორიზებული წვდომა ქსელის რესურსებზე და გამოიწვიონ „მომსახურებაზე უარი“-ს ან „ადამიანი შუაში“ ტიპის შეტევები – აი, ყველა ის პრობლემა, რომელთა გადაჭრაც საჭიროა. აუტენტიფიკაციისა და ეფექტური დაშიფვრის მექანიზმების გამოყენება საშუალებას იძლევა, რომ მნიშვნელოვნად შემცირდეს საფრთხეები. ამასთანავე, გასათვალისწინებელია ის გარემოება, რომ უმავთულო ქსელების უსაფრთხოების აუცილებელი დონე დამოკიდებულია ქსელებისადმი წაყენებულ მოთხოვნებზე.

ლიტერატურა

1) გ. ჩოგოვაძე, გ გოგიჩაიშვილი, გ. სურგულაძე, თ. შეროზია, ო. შონია. მართვის ავტომატიზებული სისტემების დაპროექტება და აგება, თბილისი, 2001წ.

2) გ. გოგიჩაიშვილი, კ. ოდიშარია, ო. შონია. ინფორმაციის დაცვა ავტომატიზებულ სისტემებში, თბილისი, საქართველოს ტექნიკური უნივერსიტეტი, 2008წ.

3) კ. ბოტჰე, გ. სურგულაძე, თ. დოლიძე, ო. შონია, თანამედროვე პროგრამული პლატფორმები და ენები, თბილისი, 2003.

4) ო. შონია, თ. შეროზია. ინფორმაციული ტექნოლოგიები და უსაფრთხოება. თბილისი, საქართველოს ტექნიკური უნივერსიტეტი, 2008წ.

5) გ. სურგულაძე, ო.შონია, ლ. ყვავაძე, მონაცემთა განაწილებული ბაზების მართვის სისტემები, თბილისი 2004.

6) Джим Гейер. Беспроводные сети, первый шаг. М. 2005

7) Владимиров А. Гавриленко К. Михаиловскй А. Wi-фу: "боевые" приемы взлома и защиты беспроводных сетей. NT Press M. 2005.

8) ო. შონია, სახელმწიფო უსაფრთხოების უზრუნველყოფის გადაწყვეტილებათა მიღების მხარდამჭერი ავტომატიზებული სისტემა, საქართველოს ტექნიკური უნივერსიტეტი, თბილისი 2004.

იბეჭდება ავტორთა მიერ წარმოდგენილი სახით

გადაეცა წარმოებას 30.01.2009. ხელმოწერილია დასაბეჭდად 18.02.2009. ქაღალდის ზომა 60X84 1/16. პირობითი ნაბეჭდი თაბახი 7. ტირაჟი 100 ეგზ.

საგამომცემლო სახლი „ტექნიკური უნივერსიტეტი“, თბილისი, კოსტავას 77

Verba volant, scripta manent

ი.მ. „გოჩა დალაქიშვილი“, ვარკეთილი 3, კ. 333, ბ. 38