

ჯ. ბერიძე, ტ. ბურკაძე, ა. ბურკაძე

მართვა და მარშრუტიზაცია
კომპიუტერულ ქსელებში

ჯ. ბერიძე, ტ. ბურკაძე, ა. ბურკაძე

მართვა და მარშრუტიზაცია
კომპიუტერულ ქსელებში



დამტკიცებულია სტუ-ს
სარედაქციო-საგამომცემლო
საბჭოს მიერ დამხმარე
სახელმძღვანელოდ ტელეკომუნიკაციის
სპეციალობის სტუდენტებისათვის

თბილისი

2009

დამხმარე სახელმძღვანელოში განხილულია კომპიუტერული ქსელების მართვის საკითხები და მარშრუტიზაციის მეთოდები.

კომპიუტერული ქსელების ეფექტურ მართვას, ანუ ადმინისტრირებას, უდიდესი მნიშვნელობა აქვს ქსელის მომხმარებლებისათვის მუშაობის სათანადო პირობების შესაქმნელად. ამასთანავე ადმინისტრირების ფუნქციაა ქსელში ინფორმაციის საიმედო დაცვა არასანქცირებული შეღწევისაგან, ასევე ინფორმაციის დაკარგვის შესაძლებლობის მინიმიზაცია. პირველი ამ ფუნქციებიდან მიიღწევა კოდირების, დაშიფვრისა და პაროლების მეთოდებით, ხოლო მეორე - მრავალგვარი ასლების დამზადებით. ასევე მნიშვნელოვანია ქსელის ქმედითუნარიანობის შენარჩუნება ისეთ დონეზე, რომელიც უზრუნველყოფს მომსახურებას სათანადო ხარისხით (QoS).

თანამედროვე კომპიუტერულ ქსელებში შეიძლება ორი ძირითადი სტრუქტურის ერთობლიობით წარმოვადგინოთ – მაგისტრალური ქსელი და გამანაწილებელი ქსელი. მაგისტრალის ქსელში ინფორმაციის მიმოცვლა ხდება პაკეტურ კომუტაციის მეთოდით, რომელიც დაფუძნებულია ინფორმაციული პაკეტების მარშრუტიზაციაზე.

წინამდებარე დამხმარე სახელმძღვანელოში განხილულია ზემოთმოყვანილი საკითხები სასწავლო კურსის “კომპიუტერული ქსელები” პროგრამით განსაზღვრული მოცულობით. ეს კურსი ეკითხება ტელეკომუნიკაციის სპეციალობის სტუდენტებს საბაზო განათლების დამასრულებელ (მეოთხე) კურსზე, როგორც არჩევითი საგანი, შემაჯავლი ინფოკომუნიკაციური ქსელების მოდულში.

დამხმარე სახელმძღვანელო სასარგებლო იქნება ტელეკომუნიკაციის და სხვა მონათესავე სპეციალობების ყველა სტუდენტისათვის, ვისი ინტერესების სფეროც ეხება კომპიუტერულ ქსელებს.

რეცენზენტი:

შ ი ნ ა ა რ ს ი

ბმ.

წინასიტყვაობა -----	4
თავი 1. ქსელის ადმინისტრირება და ინფორმაციის უსაფრთხოება ----	6
1.1. შესავალი -----	6
1.2. საადრინცხოვო ჩანაწერების მართვა -----	6
1.3. ქსელის წარმადობის მართვა -----	12
1.4. ინფორმაციის დაცვა ქსელში -----	18
1.5. მონაცემების დაკარგვის თავიდან აცილება -----	26
თავი 2. მარშრუტიზაცია გლობალურ ქსელებში -----	37
2.1. ქსელი დაგროვებითი კომუტაციის მეთოდით -----	37
2.2. მარშრუტიზაციის ალგორითმები -----	43
2.2.1. ზოგადი მიმოხილვა -----	43
2.2.2. მარშრუტიზაცია და გრაფთა თეორია -----	45
2.3. სტატიკური მარშრუტიზაციის ალგორითმები -----	46
2.3.1. უმოკლესი გზების მოძებნა ე. დეიქსტრას ალგორითმით	46
2.3.2. ავსება (flood) -----	54
2.4. დინამიური მარშრუტიზაციის ალგორითმები -----	56
2.4.1. მარშრუტიზაცია მანძილის ვექტორის მიხედვით -----	56
2.4.2. მარშრუტიზაცია არხების მდგომარეობის გათვალისწინებით -----	61
თავი 3. ქსელის მომსახურება -----	64
3.1. შესავალი -----	64
3.2. გადატვირთვის პრობლემები და მათი აღმოფხვრის გზები --	65
3.3. მომსახურების ხარისხი და მისი უზრუნველყოფა -----	78
3.4. ქსელის მონიტორინგი -----	88
3.5. საქსელო პრობლემების მოგვარება -----	93
ლიტერატურა -----	101

წინასიტყვაობა

მე-20 საუკუნის ბოლო ათწლეულებში ტელეკომუნიკაციური და კომპიუტერული ტექნოლოგიები ძლიერ დაუახლოვდნენ ერთმანეთს, დაიწყო ერთმანეთის შევსება-დამატება, რის შედეგად ჩამოყალიბდა ე.წ. ინფოკომუნიკაციის ცნება. კონცეფცია „კომპიუტერული ცენტრი“, რომლის შესაბამისადაც ერთი, იმ დროისათვის მძლავრი, კომპიუტერი ასრულებდა ყველა აუცილებელ სამუშაოს მონაცემების დამუშავებისათვის, მოძველდა.

იმ კონცეფციამ ადგილი დაუთმო ქსელურ ტექნოლოგიებს, როდესაც ცალკეული კომპიუტერები ტელეკომუნიკაციური საშუალებებით ერთვებიან სხვადასხვა რანგის ქსელებში: ლოკალურ – LAN (Local Area Network), მუნიციპალურ – MAN (Metropolitan Area Network), გლობალურ – WAN (Wide Area Network).

თანამედროვე მიდგომით კომპიუტერული ქსელები ერთიანდებიან იერარქიული პრინციპით – ცალკეული კომპიუტერები ერთვებიან და ქმნიან ლოკალურ ქსელებს, შემდგომ ლოკალური ქსელები ერთიანდებიან მუნიციპალურში, ეს უკანასკნელი კი ერთიანდებიან გლობალურ ქსელებში. თუმცა შესაძლებელია ცალკეული კომპიუტერის ჩართვა გლობალურ ქსელში (მაგალითად, ინტერნეტ ქსელში) სხვა ტექნოლოგიებითაც.

გარდა ქსელების აგების, ტექნიკური ასპექტების მნიშვნელოვანი პრობლემაა ქსელის ნორმალური ფუნქციონირების პირობების შექმნა და შენარჩუნება ხანგრძლივი პერიოდის განმავლობაში. ამ პროცესს, რომელიც ასევე ქსელის ექსპლუატაციას წარმოადგენს, ადმინისტრირებას ან მართვას უწოდებენ. ტელეკომუნიკაციის სპეციალობის სტუდენტისათვის აუცილებელია ქსელის ადმინისტრატორის ფუნქციების ცოდნა იმისათვის, რომ მას შეეძლოს ქსელის ტელეკომუნიკაციური კომპონენტის (ლითონის გამტარიანი და ოპტიკური კაბელების, მათ ბაზაზე შექმნილი არხებისა და ტრაქტების, რადიოარხებებისა და რადიოტრაქტების, საკომუტაციო სისტემებისა და კვანძების) გონივრული და ეფექტური ექსპლუატაცია.

კომპიუტერული ქსელების ადმინისტრირების ერთ-ერთ უმნიშვნელოვანეს საკითხს წარმოადგენს ინფორმაციული უსაფრთხოება. იგი გულისხმობს ქსელში ინფორმაციის დაცულობას არასანქცირებული შეღწევისაგან, ქსელიდან ინფორმაციის დაკარგვის (წაშლის) შეუძლებლობას და სხვ. ეს პრობლემები ქსელში წყდება შესაბამისი აპარატურულ-პროგრამული და სხვა ორგანიზაციული მეთოდების გამოყენებით. არანაკლებ მნიშვნელოვანი საკითხია ქსელის მომხმარებლის უზრუნველყოფა მომსახურების სათანადო ხარისხით. პაკეტური კომუტაციის ქსელში, რომელსაც მიეკუთვნება თანამედროვე კომპიუტერული ქსელების

უმრავლესობა, გადასაცემი მონაცემების ნაკადის ზრდა ხშირად იწვევს ზრდის ზეგავისებურ პროცესებს, რასაც მიყვავართ ე.წ. ქსელის გადატვირთვებთან, რაც თავის მხრივ აქვეითებს ინფორმაციის გადაცემის ხარისხს.

წინამდებარე დამხმარე სახელმძღვანელის I და III თავი მიძღვნილია ზემოაღნიშნული პრობლემებისადმი. აქ ტელეკომუნიკაციის სპეციალობის სტუდენტს მასალა ეძლევა იმ დონითა და მოცულობით, რომელიც საჭიროა აგებული კომპიუტერული ქსელის მართვისა და ექსპლუატაციისათვის.

კომპიუტერული ქსელები იერარქიის ნებისმიერ დონეზე იყენებენ პაკეტური გადაცემისა და კომუტაციის მეთოდებს. გადასაცემი ინფორმაციის შემადგენელი ნაწილის – პაკეტის დროული და დაუმახინჯებელი მიტანა მიმდებამდე განისაზღვრება, როგორც გამოყენებული ტელეკომუნიკაციური არხებისა და ტრაქტების ხარისხით, ასევე სწორი მარშრუტიზაციით. დამხმარე სახელმძღვანელოს II თავი მიძღვნილია მარშრუტიზაციის პრობლემებისადმი. სტუდენტს საშუალება ეძლევა მარშრუტიზაციის კონკრეტულ მაგალითზე შეისწავლოს ამ პროცესში წამოჭრილი კოლიზიებისა და მათი ბლოკირების ხერხების შესახებ.

დამხმარე სახელმძღვანელო შედგენილია ტელეკომუნიკაციის სპეციალობის სტუდენტებისათვის საგანში “კომპიუტერული ქსელები”. იგი ისწავლება როგორც ტელეკომუნიკაციისა და ენერგეტიკის ფაკულტეტზე ტელეკომუნიკაციის სპეციალობის სტუდენტებისათვის, ტელეკომუნიკაციური ქსელების სასწავლო-სამეცნიერო მიმართულებაზე, საბაზო განათლების დამასრულებელი კურსზე არჩევითი მოდულის “ინფოკომუნიკაციური ქსელების” შემადგენელი საგანი.

თავი I

ქსელის ადმინისტრირება და ინფორმაციის უსაფრთხოება

1.1 შესავალი

კომპიუტერული ქსელის და საერთოდ ნებისმიერი ტელეკომუნიკაციური ქსელის ეფექტური ფუნქციონირებისათვის დიდი მნიშვნელობა აქვს ქსელის მუშა მდგომარეობის შექმნას და შემდგომ მის შენარჩუნებას. ამ მიზანს ემსახურება ქსელის ადმინისტრირება, რამაც უნდა უზრუნველყოს მისი მუშა მდგომარეობა სათანადო მახასიათებლების პირობებში.

ქსელის ადმინისტრირებამ ასევე უნდა უზრუნველყოს ქსელში მომხმარებელთა შედარებით ნორმალური პირობები, მათი საქსელო სტატუსის გათვალისწინებით.

ქსელის ადმინისტრირების ამოცანაა აგრეთვე მისი წარმადობის მონიტორინგი.

თანამედროვე კომპიუტერულ ქსელებში გადასცემენ, მიიღებენ და ინახავენ მომხმარებელთა მრავალფეროვან ინფორმაციას, ხშირ შემთხვევაში სასიცოცხლოდ მნიშვნელოვანსაც, ამიტომ საჭიროა მისი საიმედო შენახვა, ასლების გადაღებით და სხვადასხვა მატარებელზე მათი განლაგებითა და სხვადასხვა პირობებში მათი შენახვით. ყოველივე ამის შედეგად უნდა გამოირიცხოს ინფორმაციის დაკარგვა და არასანქციონირებული ხელყოფა.

ადმინისტრირების საკითხებს მიეკუთვნება ასევე ქსელის მოწყობილობა-დანადგარების გარანტირებული ელექტროკვების უზრუნველყოფა.

მოყვანილი ამოცანების გადაწყვეტას ემსახურება:

- საადრიცხვო ჩანაწერების მართვა;
- ქსელის წარმადობის მართვა;
- ინფორმაციის დაცვა ქსელში;
- მონაცემების დაკარგვის თავიდან აცილება.

ყველა აქ ჩამოთვლილი საკითხი ქსელის ადმინისტრირებას ეხება და მათ ან თვითონ ქსელის ადმინისტრატორი წყვეტს, ან იგი აქტიურად მონაწილეობს მათ მოგვარებაში.

1.2. საადრიცხვო ჩანაწერების მართვა

ქსელის ადმინისტრატორის წინაშე დასმულ ამოცანათა შორის ერთერთი უმნიშვნელოვანესია საადრიცხვო ჩანაწერების მართვის ადმინისტრირება.

იგი ითვალისწინებს შემდეგს:

- ადმინისტრატორის ამოცანებისა და მოვალეობების გაცნობას;

- საადრიცხოვო ჩანაწერების სახეებისა და ფორმების შესწავლას;
- მომხმარებელთა პაროლების სისტემაში გარკვევას;
- მომხმარებელთა ჯგუფების ორგანიზებას.

ქსელის მართვა

კომპიუტერული ქსელების განვითარების მიმდინარე ეტაპზე, ანუ XXI საუკუნის დასაწყისისათვის, ჯერ კიდევ არ არსებობენ ქსელები, რომელთაც შეუძლიათ მათ წინაშე დასმული ყველა ამოცანის დამოუკიდებლად გადაჭრა. ამიტომ ქსელის ფუნქციონირებას თვალყურს ადევნებს და განაგებს ადმინისტრატორი.

ქსელში არსებული რეზერვების რაციონალური გამოყენება და ახალი რესურსების მოზიდვის საკითხის დასმა, მომხმარებელთა ქსელში შეყვანის განხორციელება და აგრეთვე ქსელიდან მათი მოხსნა, ქსელში მომხმარებელთა სათანადო შედწევის უფლების ორგანიზება და ამ უფლების მოხსნა – ყველა ეს საკითხი ქსელის ადმინისტრატორის პრეროგატივაა.

ადმინისტრატორის წინაშე დასმული ამოცანების გადაწყვეტა ქსელის მართვის პროცესია. მის წარმართვაში ადმინისტრატორს ემსახურება საქსელო პროგრამების სპეციალური ჯგუფები, რომელებიც უტილიტების სახელითაა ცნობილი.

უტილიტა – ეს რომელიმე დიდი პროგრამის ნაწილია, რომელიც განსაზღვრული ამოცანის ამოხსნას ემსახურება.

სიტყვა უტილიტა (ლათ. utilitas-სარგებელი, სარგებლობა), წარმოდგარი ლათინურიდან, ამ შემთხვევაში გულისხმობს იმ სარგებლობას, რაც მოაქვს ქსელის სპეციალურ პროგრამას მართვის ეფექტურობისა და ოპერატიულობის გაზრდის პროცესისათვის.

ადმინისტრირების არეები

მიღებულია რომ ქსელის ადმინისტრირება მოიცავს ხუთ მთავარ არეს, რომლებსაც კარგად უნდა იცნობდეს ადმინისტრატორი:

1. მომხმარებელთა მართვა – საადრიცხოვო ჩანაწერების შექმნა და შემდგომ მათი მხარდაჭერა; მომხმარებელთა ქსელში შედწევის მართვა;
2. საქსელო რესურსების მართვა – მათი დაყენება და შემდგომი მხარდაჭერა;
3. კონფიგურაციის მართვა – ქსელის კონფიგურაციის დაგეგმვა, მისი მართვის შემდგომი გაფართოებისათვის სათანადო წინადადებებისა და დოკუმენტაციის შემოტანა;

4. წარმადობის მართვა – საქსელო ოპერაციების კონტროლი (მონიტორინგი) ქსელის სისტემების წარმადობის გასაუმჯობესებლად და შემდგომი მხარდაჭერისათვის;
5. ქსელის მხარდაჭერა – ქსელის წინაშე წამოჭრილი მოსალოდნელი პრობლემების პროგნოზირება, სუსტი ადგილების გამოვლენა და მათი მოგვარება კომპენტენციის ფარგლებში ან სათანადო საკითხების დასმა.

ადმინისტრატორის მოვალეობები

ქსელის მართვის საკითხთა ერთობლიობის გათვალისწინებით ჩამოყალიბებულია ძირითად ამოცანათა ჩამონათვალი, რომლებზეც პასუხს აგებს ადმინისტრატორი:

- მომხმარებელთა სააღრიცხვო ჩანაწერების შექმნა;
- მონაცემების დაცვა;
- მომხმარებელთა სწავლება და მათი მხარდაჭერა;
- არსებული საპროგრამო უზრუნველყოფის მოდერნიზაცია და ახალის დაყენება;
- აუცილებელი მასალის არქივირება;
- მონაცემების დაკარგვის შესაძლებლობის თავიდან აცილება;
- სერვერში მონაცემების შენახვისათვის თავისუფალი არეების კონტროლი და მონიტორინგი;
- ქსელის გაწეობა მაქსიმალურ წარმადობაზე;
- მონაცემების სარეზერვო კოპირება;
- ქსელის ვირუსებისაგან დაცვის ღონისძიებების გატარება;
- ქსელის მდგრადობის დიაგნოსტიკა;
- ქსელის კომპონენტების მოდერნიზაცია და შეცვლა;
- ქსელის გაფართოების ღონისძიებათა უზრუნველყოფა.

ჩამოთვლილ ამოცანათა ნაწილს უშუალოდ ახორციელებს ადმინისტრატორი (ან საადმინისტრაციო ჯგუფი), ხოლო ნაწილის განხორციელებაში აქტიურად მონაწილეობს სათანადო მასალებისა და წინადადებების მომზადებით.

ადმინისტრატორის მოვალეობაში შემავალი უმეტესი საკითხების არსი განხილულ იქნება ქვემოთ თანმიმდევრობით.

მომხმარებელთა სააღრიცხვო ჩანაწერების შექმნა

ქსელში მომუშავე ნებისმიერი მომხმარებელი უზრუნველყოფილი უნდა იყოს სათანადო სააღრიცხვო ჩანაწერებით, რომლებშიც მითითებული იქნება მომხმარებლის ვინაობა და ქსელში მისი მუშაობის პარამეტრები, აგრეთვე პირობითი

სახელი. ეს საშუალებას მისცემს მომხმარებელს მისთვის დასაშვებ ფარგლებში ეფექტურად გამოიყენოს ქსელის რესურსები.

ინფორმაცია მომხმარებლის ვინაობისა და პარამეტრების შესახებ ადმინისტრატორის მიერ შეტანილ და შენახულ უნდა იქნეს მონაცემთა ბაზაში.

მომხმარებლის ცდის დროს შეაღწიოს ქსელში მისი პირობითი სახელი საშუალებას იძლევა გადაიხედოს მისი საადრიცხვო ჩანაწერები და გააკონტროლდეს მისი მოქმედებების შესაბამისობა ამ ჩანაწერებთან.

მომხმარებლის პირობითი სახელის, ვინაობისა და პარამეტრების თვალყურის დევნების ოპერაციები ხორციელდება სათანადო უტილიტების მეშვეობით. იგივე უტილიტები ადმინისტრატორს საშუალებას აძლევს ოპერატიულად შეიტანოს ქსელის მონაცემთა ბაზაში მომხმარებლებთან დაკავშირებული ცვლილებები.

მონაცემები ქსელის მომხმარებელთა შესახებ

საადრიცხვო ჩანაწერები შეიცავენ ინფორმაციას, რომელიც უზრუნველყოფს მომხმარებლის იდენტიფიკაციას ქსელის უსაფრთხოების სისტემაში.

ამ ჩანაწერებში მოცემულია:

- მომხმარებლის ვინაობა და პაროლი, აგრეთვე პირობითი სახელი;
- საქსელო რესურსებთან შეღწევის უფლებამოსილება;
- ჯგუფი, რომელსაც მიეკუთვნება.

ეს მონაცემები აუცილებელია ადმინისტრატორისათვის საადრიცხვო ჩანაწერების წარმოების პროცესში.

მომხმარებლის პირობითი სახელი უნდა იყოს ინდივიდუალური და ქსელში არ უნდა არსებობდეს მეორე ასეთი სახელი.

ჩანაწერები ვინაობის შესახებ უნდა იძლეოდეს აუცილებელ ინფორმაციას მომხმარებლის შესახებ.

ყოველივე ეს გათვალისწინებული და რეალიზებული უნდა იქნეს ადმინისტრატორის მიერ. ამავე დროს ადმინისტრატორმა უნდა მოახდინოს საადრიცხვო ჩანაწერების კოპირება.

საადრიცხვო ჩანაწერები უნდა წარმოებდეს გარკვეული შაბლონის გამოყენებით.

შაბლონი (გერმანულ-ფრანგული სიტყვა) – ეს არის ნიმუში, რომლის მიხედვიდაც ამზადებენ ერთნაირ ნაკეთობებს.

საადრიცხვო ჩანაწერების საწარმოებლად გარკვეული შაბლონების გამოყენება ადმინისტრატორს საშუალებას აძლევს ეს პროცესი გაართვიოს და გააადვილოს.

მომხმარებლის პარამეტრების დაყენება

ადმინისტრატორის მიერ დაყენებული მომხმარებლის პარამეტრები უნდა ითვალისწინებდეს შემდეგ მოთხოვნებსა და შესაძლებლობებს:

- რეგისტრაციის დრო – რათა დადგენილ იქნეს მომხმარებლის ქსელში მუშაობის პერიოდი;
- საოჯახო კატალოგი – რაც მომხმარებელს საშუალებას აძლევს პირადი ფაილები შეინახოს მისთვის გამოყოფილ ადგილზე;
- სააღრიცხვო ჩანაწერების მოქმედების ვადა – რაც საშუალებას იძლევა შემოსაზღვროს მომხმარებლის ქსელში მუშაობის პერიოდი.

ადმინისტრატორი, როგორც საწყისი სააღრიცხვო ჩანაწერი

ქსელის ოპერაციული სისტემის დაყენებისთანავე იქმნება სააღრიცხვო ჩანაწერი მომხმარებლისათვის, რომელიც „თავის ხელში იღებს მთელ ძალაუფლებას“ ქსელში.

ამ პირველ მომხმარებელს ევალება:

- ქსელის ფორმირება;
- დაცვის საწყისი პარამეტრების დაყენება;
- სხვა მომხმარებლებისათვის სააღრიცხვო ჩანაწერების შექმნა.

Microsoft-ის საქსელო გარემოში ამ პირველი მომხმარებლის სახელია Administrator (ადმინისტრატორი).

Novell-ის გარემოში კი Supervisor (სუპერვიზორი).

ამგვარად, ის ვინც აყენებს საოპერაციო სისტემას და პირველი შედის ქსელში ის არის მისი ადმინისტრატორი და სრულუფლებიანი მმართველი.

სტუმრის სააღრიცხვო ჩანაწერი

მათ, ვინც არ არიან ქსელის სრულფასოვანი მომხმარებლები, მაგრამ ესაჭიროებათ და აქვთ უფლება შეაღწიონ ქსელში, ექმნებათ ე.წ. სტუმრის (Guest) სააღრიცხვო ჩანაწერი. ამ პირის მიერ საქმიანობის დასრულების შემდეგ, მისი სააღრიცხვო ჩანაწერი გამოირთვება. ჩვეულებრივ ის რჩება ქსელში და საჭიროების შემთხვევაში ადმინისტრატორს მისი გააქტიურების საშუალება ეძლევა.

პაროლი

პაროლი (ფრან. Parole – სიტყვა) დათქმული საიდუმლო სიტყვა ან ფრაზაა, რომელსაც იყენებენ რაიმე უფლების მოსაპოვებლად, თავისიანის გამოსაცნობად, პიროვნების უფლებამოსილების დასადგენად და სხვა ანალოგიური დანიშნულებით.

კომპიუტერულ ქსელებში პაროლის არჩევისას ასეთ რეკომენდაციებს იძლევიან:

- არ იქნეს გამოყენებული ცნობილი სახელები და მოვლენები, მაგალითად, საკუთარი დაბადების წელი, მეუღლის ან შვილის სახელი და სხვა.

- ყველაზე უკეთესია პაროლი შენახულ იქნეს მახსოვრობაში და არა ქალაქდზე, თუნდაც საიმედოდ გადამაღულზე;
- არ იქნეს დავიწყებული პაროლის მოქმედების ვადა, რომ მისმა მოულოდნელმა ბლოკირებამ არ წარმოქმნას სირთულეები.

პაროლი (passwords) უზრუნველყოფს ქსელის გარემოს დაცვას არასანქცონირებული ხელყოფისაგან.

ადმინისტრატორის პირველი ამოცანაა პაროლის დადგენა საწყისი სააღრიცხვო ჩანაწერის შექმნის დროს. ამით იგი თავიდან იცილებს უკანონო შეღწევებს.

თითოეულმა მომხმარებელმა უნდა მოიფიქროს პირადი უნიკალური პაროლი და შეინახოს იგი საიდუმლოდ.

პაროლი კომპიუტერულ ტექნოლოგიებში სპეციალური კოდია, რომლის მაქსიმალურ სიგრძედ მიღებულია 14 სიმბოლო.

სხვადასხვა განსაკუთრებული შემთხვევის შემდეგ ადმინისტრატორმა უნდა დაავალდებულოს მომხმარებელი შეცვალოს პაროლი. მრავალი ქსელის საოპერაციო სისტემა თვითონ აიძულებს მომხმარებელს პერიოდულად, ადმინისტრატორთან შეთანხმებით, შეცვალოს პაროლი, წინააღმდეგ შემთხვევაში წყვეტს მის მომსახურებას ძველი პაროლით.

ცალკეულ შემთხვევებში, როდესაც უსაფრთხოება არ არის კრიტიკული საკითხი ან ქსელში შეღწევა ძალიან შეზღუდულია, სააღრიცხვო ჩანაწერმა შეიძლება მიიღოს ისეთი სახე, რომ პაროლის გამოყენება არც იყოს საჭირო.

გარდა ამ შემთხვევებისა ადმინისტრატორმა უნდა გაითვალისწინოს, რომ ქსელის ყოფილმა მომხმარებელმა (ვთქვათ განთავისუფლებულმა თანამშრომელმა) შეიძლება მონდომოს ქსელში შეღწევა, რაღაც პირადი მიზნებით. ამიტომ უნდა მოხდეს ყოფილი მომხმარებლის სააღრიცხვო ჩანაწერის ბლოკირება.

ჯგუფური სააღრიცხვო ჩანაწერები მომხმარებელთათვის

ქსელი შეიძლება მხარს უჭერდეს ათასობით სააღრიცხვო ჩანაწერს. ქსელში ყოველთვის წარმოიშობა სიტუაცია, როდესაც ადმინისტრატორს სჭირდება ერთი და იგივე მოქმედება განახორციელოს მრავალი სააღრიცხვო ჩანაწერის მიმართ. ასევე შესაძლებელია ადმინისტრატორი ერთი და იგივე შეტყობინებას უგზავნიდეს მომხმარებელთა დიდ ჯგუფს, ან აძლევდეს ამ თუ იმ რესურსთან შეღწევის უფლებას მომხმარებელთა მკაცრად განსაზღვრულ კონტიგენტს.

ასეთ და მრავალ სხვა შემთხვევაში აუცილებელი ხდება უამრავ სააღრიცხვო ჩანაწერში შეტანილი იქნეს ცვლილებები. ეს კი პრობლემატური საკითხი ხდება: ადმინისტრატორს ან არ აქვს იმდენი დრო რომ შეიტანოს ეს ცვლილებები, ან მათი

შეტანა მოხდება დაგვიანებით. ამ მდგომარეობიდან გამოსავალს პოულობენ მომხმარებელთა საერთო ჯგუფში (გარკვეული მოთხოვნების გათვალისწინებით) გაერთიანებით.

ჯგუფი (group) – ეს საადრიცხო ჩანაწერების კოლექტიური მომსახურების საშუალებაა, რაც მნიშვნელოვნად უადვილებს საქმიანობას ადმინისტრატორს.

ქსელებს პროგრამებში გათვალისწინებული აქვთ სათანადო უტილიტები, რომლებიც უზრუნველყოფენ ჯგუფების შექმნასა და მომსახურებას.

პრივილეგიების მინიჭება

ქსელში ხშირ შემთხვევაში არიან მომხმარებლები, რომლებიც მომსახურების განსაკუთრებული უფლებებით – პრივილეგიებით სარგებლობენ. საქსელო ადმინისტრატორმა ამ უფლებების განხორციელებისათვის სათანადო ინფორმაცია უნდა შეიტანოს საადრიცხო ჩანაწერებში.

მომხმარებლის საადრიცხო ჩანაწერის ბლოკირება და მოცილება

ზოგიერთ შემთხვევაში ადმინისტრატორს სჭირდება ამა თუ იმ მომხმარებლის ქსელში შეღწევის დროებითი შეზღუდვა ან საერთოდ მომსახურებიდან გამოყვანა. შესაბამისად საჭიროა ამ მომხმარებლის საადრიცხო ჩანაწერში ან სათანადო შესწორების შეტანა ან მისი მოცილება. ადმინისტრატორი ბლოკირებას ახორციელებს მაშინ, როდესაც შემდგომში მოსალოდნელია ამ მომხმარებლის მიმართ მომსახურების აღდგენა, ხოლო თუ ეს ჩაითვლება შეუძლებლად - საადრიცხო ჩანაწერი მოცილდება.

1.3. ქსელის წარმადობის მართვა

ქსელის წარმადობის მართვა ითვალისწინებს შემდეგს:

- ქსელის წარმადობის მონიტორინგის განხორციელებას;
- ქსელში სუსტი ადგილების გამოვლენასა და ღონისძიებების გატარებას მათი ლიკვიდაციის მიზნით;
- ქსელის ეფექტური მართვისათვის მონაცემთა ბაზის შექმნას;
- ქსელის ისტორიის წარმოებას, როგორც მომავალში მისი აღჭურვისა და გაფართოების წინადადებათა წამოყენების დოკუმენტური დადასტურების საშუალებას.

აღნიშნოთ, რომ სიტყვა მონიტორინგი წარმოდგება ლათინურ - ინგლისური monitor-ისაგან, რაც ნიშნავს გამაფრთხილებელს. მონიტორინგი კომპიუტერულ ტექნოლოგიებში დაკვირვების, კონტროლის პროცესებია, რომელთა მიზანს შეადგენს არსებული მდგომარეობის დაფიქსირება-შეფასება და შესაბამისი გამაფრთხილებელი, ყურადსადები ინფორმაციის გამომუშავება. მოცემულ შემთხვევაში მონიტორინგის

შედგები განთავსდება მონაცემთა ბაზაში და მიეწოდება ქსელის ადმინისტრატორს სათანადო რეაგირებისათვის.

მიმოხილვა

ქსელის დაყენებისა და გაშვების შემდეგ ადმინისტრატორი უნდა დარწმუნდეს, რომ იგი (ქსელი) ეფექტურად მუშაობს.

ამ მიზნით საჭიროა განუწყვეტელი თვალყურის დევნება თუ როგორი წარმადობით ფუნქციონირებს ქსელი და იმ ფაქტორების მართვა, რომლებიც გავლენას ახდენენ მის წარმადობაზე.

ქსელის მართვის ამოცანების მასშტაბი დამოკიდებულია:

- ქსელის ზომებზე;
- ქსელის მომსახურე თანამშრომლების რიცხვზე და მათ კვალიფიკაციაზე;
- ქსელის მომსახურებისათვის გამოყოფილი საშუალებების რაოდენობაზე (როგორც ფინანსური, ასევე ტექნიკური მხრივ);
- ქსელის გამოყენებით მიღებულ სარგებელზე.

პატარა ერთრანგიანი ქსელები 8-12 კომპიუტერით შეიძლება გაკონტროლდეს ერთი პიროვნების მიერ ვიზუალურად.

დიდი და, განსაკუთრებით, გლობალური ქსელების მონიტორინგისათვის კი საჭიროა გამოცდილი სპეციალისტების გარკვეული შტატი და სათანადო აღჭურვილობა.

წარმადობის მონიტორინგი

ადმინისტრატორმა უნდა გააკონტროლოს ქსელის წარმადობა, რომ

- მიღწეულ იქნეს მისი წარმადობის უწყვეტი ზრდა არსებული კონფიგურაციის ფარგლებში;
- შესაძლებელი გახდეს მისი განვითარების პროგნოზირება და დაგეგმვა;
- გამოვლინდეს მისი სუსტი ადგილები.

სუსტი ადგილები

დიდი საქსელო ოპერაციები ხორციელდება რამდენიმე მოწყობილობის გაერთიანებული მოქმედებით. თითოეული მათგანი საერთო ოპერაციის შესასრულებლად გარკვეულ დროს მოითხოვს. თუ რომელიმე მათგანი შედარებით მეტ დროს ხარჯავს წარმოიქმნება პრობლემები მთელი ქსელის წარმადობაში.

ასეთ „დამამუხრუჭებელ“ მოწყობილობას ქსელში, ჩვეულებრივ, „სუსტ ადგილს“ (bottleneck) უწოდებენ.

ქსელის მონიტორინგის ერთერთი ძირითადი ფუნქცია სწორედ ამ სუსტი ადგილების გამოვლენაა. ადმინისტრატორმა უნდა გადაწყვიტოს სუსტი ადგილის პრობლემა ან უნდა იპოვოს ის მოწყობილობა, რომელიც აფერხებს ქსელის

მუშაობას, ითხოვს რა მეტ სამუშაო დროს ვიდრე დასაშვებია, და იზრუნვოს მის შეცვლაზე.

სუსტი ადგილი შეიძლება იყოს, მაგალითად, სერვერი და კონკრეტულად მისი რომელიმე კვანძი ან პარამეტრი:

- პროცესორი (სწრაფმოქმედება);
- მეხსიერება (მისი მოცულობა);
- ადაპტერი (სწრაფმოქმედება, მცირე მეხსიერება);
- გადაცემის გარემო (მონაცემების გადაცემის სიჩქარე).

ზოგადად მოწყობილობა მოცემულ ქსელში, მოცემულ კვანძში სუსტ ადგილად შეიძლება გადაიქცეს თუ ის:

- არაეფექტურად გამოიყენება;
- მუშაობს ნელი ტემპით;
- ნაკლები შესაძლებლობისაა, ვიდრე მოითხოვება.

კარგად ორგანიზირებული მონიტორინგი გამოავლენს ნაკლოვანებებს ქსელში და გაადვილებს პრობლემური კომპონენტის პოვნას.

მონიტორინგის საშუალებები

თანამედროვე ქსელების საოპერაციო სისტემებს გააჩნიათ მონიტორინგის უტილიტები. ისინი საშუალებას აძლევენ ადმინისტრატორს გააკონტროლოს ქსელის ფუნქციონირების სხვადასხვა ასპექტი და გამოავლინოს ნაკლოვანებები.

მონიტორინგის უტილიტები საშუალებას აძლევენ ადმინისტრატორს ქსელში მიმდინარე პროცესებს თვალყური ადევნოს, როგორც რეალურ დროში, ასევე ჩანაწერებით.

ასეთი პროცესებია:

- პროცესორის მოქმედება;
- მეხსიერების გამოყენება;
- ქსელის ფუნქციონირება ერთიანად.

მონიტორინგის უტილიტები, ასრულებენ რა თავის ფუნქციებს,

- იწერენ ინფორმაციას ქსელის წარმადობის შესახებ;
- უგზავნიან ადმინისტრატორს გაფრთხილების სიგნალებს;
- მართავენ პროგრამებს, რომელთაც შეუძლიათ ქსელის ფუნქციონირების გაუმჯობესება.

ქსელის ადმინისტრატორი, სარგებლობს რა მონიტორინგის უტილიტების მიერ მიწოდებული ინფორმაციით, აგრეთვე ქსელის ფუნქციონირების სხვა მაჩვენებლებით, იღებს გადაწყვეტილებებს ქსელის წარმადობის გაზრდის უზრუნველსაყოფად.

ქსელის მართვის პროტოკოლი

ქსელის მართვის საპროგრამო უზრუნველყოფა შეესაბამება სტანდარტებს, რომლებიც შემუშავებულია საერთაშორისო ორგანიზაციების მიერ საქსელო მოწყობილობების მწარმოებლებთან ერთად.

ერთერთი ასეთი ფართოდ გამოყენებული სტანდარტია ქსელის მართვის მარტივი პროტოკოლი (Simple Network Management Protocol, SNMP).

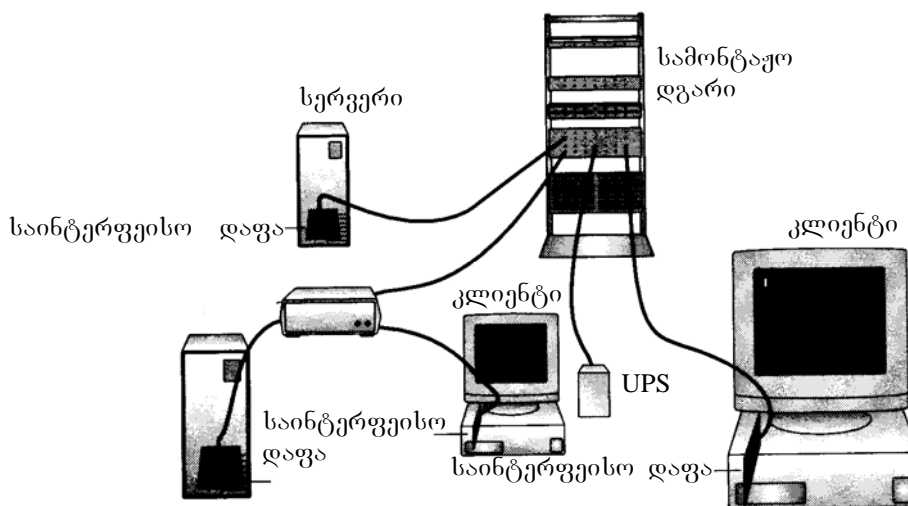
SNMP –ს პროგრამები, რომელთაც აგენტებს უწოდებენ, მათი გამოყენების დროს ჩაიტვირთებიან ნებისმიერ მმართველ მოწყობილობაში. აგენტები აკონტროლებენ ქსელის მუშაობის ტრაფიკსა და კომპონენტთა ფუნქციონირებას, აგროვებენ სტატისტიკურ მონაცემებს. შეგროვილი ინფორმაცია ინახება მართვის მონაცემთა ბაზაში (Management Information Base, MIB).

კომპონენტები, რომლებიც ექვემდებარებიან SNMP–ს პროგრამით გაკონტროლებას, შეადგენენ ქსელის ძირითად ნაწილს.

ასეთ კომპონენტებს მიეკუთვნება:

- სერვერი
- კლიენტი
- კონცენტრატორი
- ადაპტერი
- მარშრუტიზატორი
- ბოგირი
- რაბი

ნახაზზე 1.1 მაგალითის სახით წარმოდგენილია ქსელის ფრაგმენტი SNMP კომპონენტებით, სადაც საინტერფეისო დაფა იგივე საქსელო ადაპტერია.



ნახ. 1.1. ქსელის SNMP კომპონენტები (ფრაგმენტი)

აგენტების მიერ მოპოვებული ინფორმაცია შემდგომ შეიძლება:

- წარდგენილ იქნეს გრაფიკების, სქემებისა და დიაგრამების სახით;
- გადაიგზავნოს მონაცემთა ბაზაში შენახვისათვის და შემდგომი ანალიზისათვის.

ქსელის ამა თუ იმ მაჩვენებლის ადმინისტრატორის მიერ დაშვებული საზღვრებიდან გამოსვლის შემთხვევაში, ეცნობება ადმინისტრატორს მის სამუშაო კომპიუტერზე ან პეიჯერზე.

შემდგომ ქსელის მომსახურე პერსონალმა შეიძლება ან შეიტანოს ცვლილებები ქსელის ფუნქციონირებაში, ან დასვას საკითხი რომელიმე კომპონენტის შეცვლის ან მოდერნიზაციის მიზნით.

სისტემის სრული მართვა

ქსელის ზომების გაზრდამ და გართულებამ მეტისმეტად ძვირი გახადა მისი ყოველმხრივი კონტროლი. ამასთან დაკავშირებით შემუშავებულ იქნა უნივერსალური პროგრამები, რომლებიც ერთდროულად უზრუნველყოფენ როგორც ქსელის მართვას, ასევე მის მონიტორინგს. ასეთი პროგრამის მაგალითია Microsoft Systems Management Server (MSMS) – განაწილებული სისტემების ცენტრალიზებული მართვის პროგრამა.

პროგრამა MSMS-ი უზრუნველყოფს რთულ ქსელებში კომპიუტერების ცენტრალიზებულ ადმინისტრირებას.

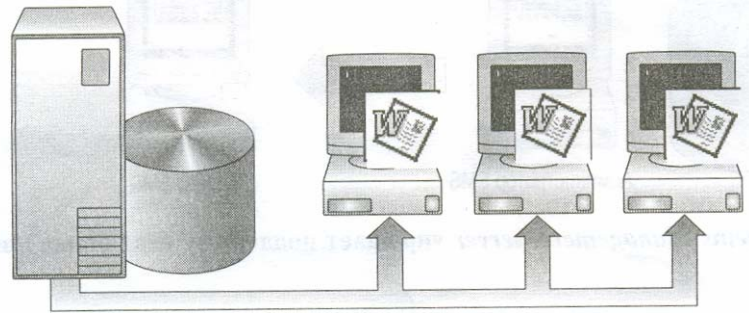
ამ პროგრამით ხორციელდება:

- აპარატურული და პროგრამული უზრუნველყოფის ინვენტარიზაცია;
- პროგრამული უზრუნველყოფის გავრცელება და დაყენება;
- შეფერხების მიზეზების აღმოჩენა აპარატურულ და პროგრამულ უზრუნველყოფაში.

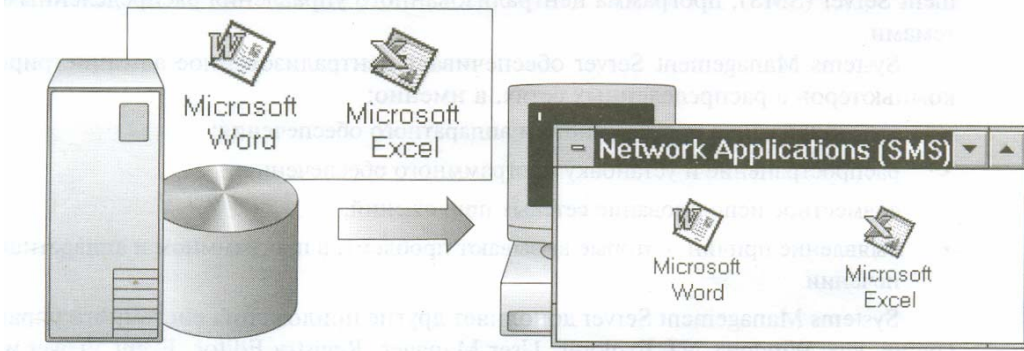
MSMS პროგრამის საფუძველზე მონაცემთა ბაზაში ინახება თითოეული კომპიუტერის აპარატურული აღწერილობისა და მისი პროგრამული უზრუნველყოფის სრული სურათი. ამ დროს ქსელში ჩართულ ნებისმიერ კომპიუტერს საშუალება ეძლევა მიიღოს ყველა ახალი პროგრამა და მოახდინოს მათი კონფიგურაცია; ასევე გამოიყენოს ქსელში ფუნქციონირებადი ნებისმიერი დანართი.

ამგვარად, ქსელი, რომელიც იმართება MSMS პროგრამით, უზრუნველყოფილია:

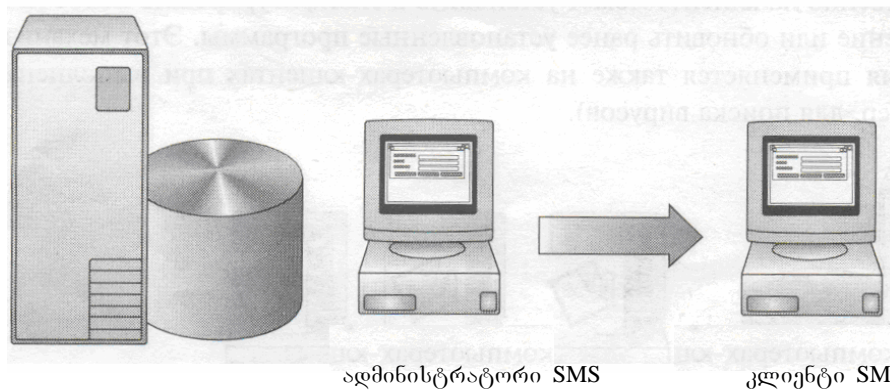
- ა). ახალი პროგრამების ოპერატიული გავრცელებით მთელ ქსელში (ნახ. 1.2),
- ბ). დანართების ერთობლივი გამოყენების გამარტივებული გზებით (ნახ. 1.3),
- გ). შორეული კლიენტების გაადვილებული მომსახურებით (ნახ. 1.4).



ნახ. 12. MSMS-ი ავრცელებს პროგრამულ უზრუნველყოფას



ნახ. 13. MSMS-ი ამარტივებს დანართების გამოყენებას



ნახ. 14. MSMS-ი აადვილებს შორეული კლიენტების მომსახურებას

ყველა ეს ღონისძიება კი, ერთი მხრივ, აიაფებს ქსელის ექსპლუატაციასა და მომსახურებას, მეორე მხრივ, ქსელს ხდის უფრო ოპერატიულსა და საიმედოს მომხმარებლებისათვის.

ქსელის დოკუმენტაცია

ქსელის ნორმალური და საიმედო ფუნქციონირებისათვის დიდი მნიშვნელობა აქვს მასში მიმდინარე თითოეული პროცესის (ზოგჯერ თითქოსდა უმნიშვნელოს) ფიქსაციას, ანუ ქსელის ისტორიის სრული სურათის შექმნას.

ეს ღონისძიება უნდა დაიწყოს ქსელის დაყენების მომენტიდან და გაგრძელდეს მისი არსებობის მთელ მანძილზე.

ასეთი მიდგომა საშუალებას იძლევა გამოვლინდეს პრობლემები დაკავშირებული როგორც უშუალოდ მოწყობილობებთან, ასევე მათ წარმადობასთან;

შეიქმნას მონაცემთა ბაზა შემდგომში ქსელის მოდერნიზაციისა და გაფართოების განხორციელებისათვის.

ქსელის ფუნქციონირების ყველა დეტალი შეტანილ უნდა იქნეს საქსელო ჟურნალში.

თუ ქსელში, მისი დიდი ზომების გამო, რამდენიმე ადმინისტრატორი მუშაობს, მონაცემები მაინც ერთ ჟურნალში უნდა განთავსდეს.

საქსელო ჟურნალში ასახული უნდა იქნეს:

- მოწყობილობათა შექმნისა და დაყენების დრო;
- მოწყობილობათა ძირითადი მაჩვენებლები, სერიული ნომრების მითითებით;
- მომწოდებელთა ვინაობა და დამახასიათებელი მაჩვენებლები;
- მწარმოებელთა საფირმო სახელები, პროდუქციის ნომენკლატურა და საგარანტიო ვადები;
- დაყენების პროცესი და მისი შედეგები;
- ქსელის საწყისი და შემდგომი კონფიგურაცია;
- ყველა საქსელო დანართის სია და შემადგენლობა;
- ქსელის ექსპლუატაციის პირობებში წარმოშობილი პრობლემები და მათი გადაწყვეტა;
- ყველა აპარატურული და პროგრამული ცვლილება.

ასევე მრავალი სხვა მოვლენა თუ პარამეტრი დაკავშირებული ქსელის ფუნქციონირების ნებისმიერ ასპექტთან.

ასეთი ჟურნალი საუკეთესო საშუალება იქნება ქსელის ადმინისტრატორისათვის (ასევე ქსელის ხელმძღვანელობისათვის) შემდგომი ამოცანების გადაწყვეტის დროს.

ასეთი ამოცანები კი შემდგომში შეიძლება იყოს ქსელის გაფართოება და აღჭურვილობის, მომსახურებისა და კონფიგურაციის შეცვლა და სხვა.

ქსელის დოკუმენტაცია (მისი ისტორია) ხელმისაწვდომი და ადვილად გასაგები უნდა იყოს ქსელის ფუნქციონირებით დაინტერესებული ყველა პირისათვის.

საქსელო ჟურნალი შეიძლება წარმოებდეს ელექტრონული ვერსიის სახით ან ქაღალდზე. ასევე მისაღებია ჟურნალის წარმოება ერთდროულად ორივე სახით.

14. ინფორმაციის დაცვა ქსელში

მიმოხილვა

ქსელში ხშირად მუშავდება კონფიდენციალური ინფორმაცია, ინფორმაცია საქმიანი, პირადი და ზოგჯერ საკმაოდ დელიკატურიც.

ქსელში მომუშავე ნებისმიერი მომხმარებელი გარანტირებული უნდა იყოს, რომ მისი ინფორმაცია მისი სურვილის გარეშე არ გასხვისდება და არც დაიკარგება.

ინფორმაცია ქსელში მოითხოვს დაცვას.

ამავე დროს ინფორმაციის დაცვამ არ უნდა მიიღოს ისეთი სახე, რომ თვითონ კანონიერ მომხმარებელს შეუქნას პრობლემები მისთვის საჭირო ინფორმაციის მიღებისა და მოხმარების პროცესში.

ქსელში მომსახურების ეს ამოცანები მნიშვნელოვანწილად ადმინისტრატორის გადასაწყვეტია. მისი გადაწყვეტა კი მოითხოვს დიდ ყურადღებასა და დელიკატურ მიდგომას. აუცილებელია მომხმარებლისათვის ქსელი იყოს მოხერხებული, საიმედო და უსაფრთხო ინსტრუმენტი მისი საქმიანობისათვის, იქნება ეს სამსახურებრივი თუ სრულიად პირადი.

ქსელის დაცვის დაგეგმვა

ქსელის ფუნქციონირების პროცესში აუცილებელია როგორც უშუალოდ ინფორმაციის, ასევე თვითონ ქსელის დაცვა. ამიტომ უნდა დაიგეგმოს და გატარდეს უსაფრთხოების ღონისძიებები, რომ გამოირიცხოს ქსელის დაზიანება და ინფორმაციის ხელყოფა.

ქსელის უსაფრთხოებისათვის განსაკუთრებით საშიშია და ამიტომ თავიდან უნდა იქნეს აცილებული:

- არასანქცონირებული შეღწევა;
- ელექტრონული მიყურადება;
- ქურდობა;
- წინასწარგანზრახული ან შემთხვევითი დაზიანება.

დაცვის ღონე

ქსელის დაცვის ღონე დამოკიდებულია მის დანიშნულებაზე. ცხადია, ქსელი, რომელიც ემსახურება მსხვილ კორპორაციას, ბანკს ან რომელიმე პატარა ორგანიზაციას განსხვავებულ დაცვას მოითხოვს.

დაცვის პოლიტიკის შემუშავება

ქსელის დაცვისათვის შემუშავებული უნდა იქნეს გარკვეული პოლიტიკა.

უსაფრთხოების პოლიტიკის შემუშავება ის პირველი ნაბიჯია, რომელიც უნდა გადაიდგას ნებისმიერ ორგანიზაციაში ინფორმაციის დაცვის გზაზე.

დაცვის პოლიტიკა თავდაპირველად აყალიბებს ე.წ. გენერალურ ხაზს, რომელსაც შემდგომ ეყრდნობა როგორც ადმინისტრატორი, ასევე მომხმარებელი. ამ პოლიტიკაში სიტუაციის მიხედვით შეტანილი უნდა იქნეს ცვლილებები, რომ გამოინახოს გამოსავალი ყველა შექმნილი მდგომარეობიდან.

ამგვარად, უსაფრთხოების პოლიტიკის შემუშავება და მიღება მნიშვნელოვანი პირობაა ქსელის ეფექტურად გამოყენებისათვის.

პრევენციული დაცვა

დაცვის საუკეთესო საშუალებაა მისი პრევენცია. თუ თავიდან აცილებული იქნება ქსელში არასანქცონირებული შეღწევა ან შეღწევის მცდელობა, ეს ნიშნავს, რომ ინფორმაცია საიმედოდაა დაცული.

დაცვის შესაფერისი ღონისძიებები ადმინისტრატორის მოსაფიქრებელი და გასატარებელია, ამიტომ იგი სრულად უნდა ფლობდეს სიტუაციას.

იდენტიფიკაცია

მომხმარებელმა ქსელში რომ შეაღწიოს საჭიროა მან სწორად შეიყვანოს პირობითი სახელი და პაროლი. ეს მონაცემები საადრიცხვო ჩანაწერების ელემენტებია და მათი იდენტიფიკაცია დაცვის პირველი საფეხურია.

სწავლება

ადმინისტრატორის ერთერთი მთავარი მოვალეობაა გაარკვიოს მომხმარებელი უსაფრთხოების ღონისძიებებში და ასწავლოს მათი გამოყენება.

ადმინისტრატორმა შეიძლება შექმნას სათანადო სახელმძღვანელო და პირადადაც აწარმოოს სწავლება, განსაკუთრებით გამოუცდელი მომხმარებლებისათვის.

ნაკლებად მოსალოდნელია ნასწავლმა მომხმარებელმა არამიზანდასახულად შემთხვევით დააზიანოს ქსელი და მონაცემები.

მოწყობილობების ფიზიკური დაცვა.

მონაცემების დაცვა საქსელო მოწყობილობების ფიზიკური დაცვით უნდა დაიწყოს.

ფიზიკური დაცვის ორგანიზების დროს გასათვალისწინებელია:

- კომპანიის ზომები;
- ინფორმაციის ხასიათი;
- ხელმისაწვდომი რესურსების რაოდენობა.

ერთრანგიან ქსელებში ფიზიკური დაცვის ორგანიზების პოლიტიკა არ არსებობს. მომხმარებელი თვითონ აგებს პასუხს მისი კომპიუტერის უსაფრთხოებაზე.

სერვერის დაცვა

დიდ ცენტრალიზებულ სისტემებში, სადაც მომხმარებელთა რიცხვი მაღალია, ხოლო კომპანიის მონაცემები მნიშვნელოვანი, სერვერები დაცული უნდა იქნენ შემთხვევითი და წინასწარგანზრახული ხელყოფისაგან.

სერვერების ფიზიკური დაცვის ორგანიზების მარტივი ვარიანტია მათი განთავსება სპეციალურ სათავსოში, სადაც შესვლა შეზღუდული იქნება. თუ ამის საშუალება არ არის მინიმუმ შესაძლებელია მათი დაყენება რომელიმე საკეტებიან კარადაში.

კაბელების დაცვა

კაბელი, სპილენძის გამტარით, გარკვეულ მანძილზე ასხივებს მასში გამავალ სიგნალებს. სპეციალური მოწყობილობების საშუალებით შესაძლებელია მათი დაჭერა. ასევე შესაძლებელია კაბელთან უშუალო მიერთება და ინფორმაციის მითვისება პირდაპირ საქსელო კაბელიდან.

აქედან გამომდინარე, საკაბელო ტრაქტებში შედწევა მკაცრად შეზღუდული უნდა იყოს და იქ დაიშვას მხოლოდ უშუალოდ მომსახურე პერსონალი. კარგი შედეგების მომგანია, დაცვის თვალსაზრისით, კაბელების გატარება სპეციალურ შეზღუდული გაბარიტების მქონე ჭრილებში და სპეციალურ მილებში საამშენებლო კონსტრუქციების შიგნით.

როგორც სერვერების, ასევე საკაბელო მეურნეობის დაცვის საკითხები ადმინისტრატორის განუწყვეტელი ყურადღების საგანი უნდა იყოს.

დაცვის მოდელები

ქსელის კომპონენტების დაცვასთან ერთად უდიდესი მნიშვნელობა აქვს აგრეთვე ქსელის რესურსების დაცვას.

მომხმარებლისათვის რესურსების დაცვა და რაციონალური განაწილება ქსელით სარგებლობის უმნიშველოვანესი საკითხებია, ხოლო ადმინისტრატორისათვის კი ძირითადი ამოცანებია.

ამ მიზნების განსახორციელებლად სადღეისოდ ორი მოდელი გამოიყენება. ისინი გარკვეულწილად უზრუნველყოფენ ქსელის საინფორმაციო და სააპარატო უსაფრთხოებას. ეს მოდელებია:

- დაცვა პაროლის მიხედვით;
- დაცვა შედწევის ნებართვით.

ამ მოდელებს ასევე უწოდებენ:

- დაცვა საერთო რესურსების დონეზე (resource level – დაცვა პაროლით);
- დაცვა მომხმარებლის დონეზე (user level – დაცვა ნებართვით).

რესურსებთან შედწევის პაროლი.

საერთო რესურსების დაცვის ერთერთი მთავარი მეთოდია თითოეული რესურსისათვის საკუთარი პაროლის მიკუთვნება. მომხმარებელს მხოლოდ მაშინ შეეძლება ამ რესურსით სარგებლობა თუ ის შეიყვანს სათანადო პაროლს.

ბევრ სისტემაში საერთო რესურსების გამოყენება ხორციელდება ქსელში სხვადასხვა დონის შეღწევით. შეღწევის დონეს კი განსაზღვრავს პაროლის ტიპი.

ინფორმაციის გარკვეული კატალოგისათვის (ჩამონათვალისათვის) შეღწევის დონე სხვადასხვა მომხმარებლისათვის შეიძლება არაერთსახოვანი იყოს.

მიღებულია ასეთი დონეები:

- შეღწევა მხოლოდ კითხვის ნებართვით (read only);

ამ დონის შეღწევის უფლების მქონე მომხმარებლები კატალოგში მოცემულ მასალას წაიკითხავენ ე.ი. კატალოგში მათ შეუძლიათ მხოლოდ გადაათვალიერონ მასალა. ამავე დროს შეუძლიათ მოახდინონ მისი კოპირება საკუთარ კომპიუტერზე, ამობეჭდონ იგი, მაგრამ არ აქვთ უფლება რაიმე ცვლილება შეიტანონ დედანში (ანუ ქსელში განთავსებულ მასალაში).

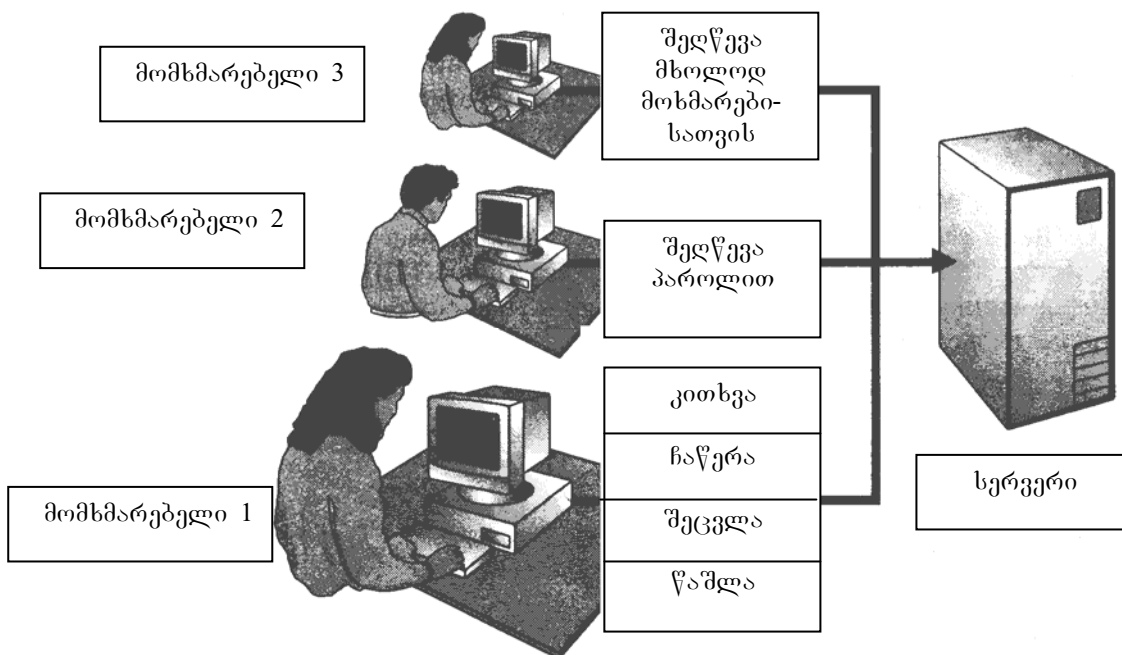
- შეღწევის დონე პაროლის მიხედვით (depending on password);

ამ შემთხვევაში საერთო გამოყენების კატალოგს პაროლის ორი დონე მიეკუთვნება: ერთ შემთხვევაში შეღწევის დონე ნებას აძლევს მომხმარებელს მხოლოდ წაიკითხოს მასალა, მეორე შემთხვევაში შეღწევის დონე სრულია.

- სრული შეღწევა (full access).

ამ დონის შეღწევის უფლების მქონე მომხმარებელს კატალოგში მოცემულ მასალაში შეუძლია ცვლილებებისა და გარდაქმნების შეტანა საკუთარი შესხედულებების მიხედვით.

ნახაზზე 1.5 წარმოდგენილია საერთო რესურსში სხვადასხვა შეღწევის დონის გამოყენების მაგალითი.



ნახ. 1.5. რესურსთან შეღწევის დონეთა სურათი

შედწევის ნებართვა

მომხმარებელი ქსელში შეადწევს პირობითი სახელისა და პაროლის გამოყენებით. ქსელის კონკრეტული საერთო რესურსის გამოყენებისათვის მას სჭირდება ამ რესურსთან შედწევის განსაკუთრებული ნებართვა.

თითოეულ მომხმარებელს შეიძლება ჰქონდეს ნებართვების მთელი დასტა საერთო მომხმარებლის რესურსების გარკვეული ნაწილის ან სრული შემადგენლობით სარგებლობის უფლებით.

ასეთი ღონისძიება უფრო მაღალი საფეხურის დაცვას განახორციელებს და მას ეწოდება დაცვა მომხმარებლის დონეზე.

დაცვა მომხმარებლის დონეზე უფრო ეფექტურია და ქსელისა და რესურსების უსაფრთხოების უფრო მაღალ საფეხურს უზრუნველყოფს.

ქსელში რესურსებთან შედწევის ნებართვები კონტროლირდება ადმინისტრატორის მიერ.

ჯგუფური ნებართვა

ადმინისტრატორმა თითოეულ მომხმარებელს უნდა მიანიჭოს საერთო რესურსებთან შედწევის ნებართვა. მომხმარებელთა დიდი რიცხვის დროს ეს რთული ამოცანაა, ამიტომ ნებართვის მინიჭება ხორციელდება მთელი ჯგუფისათვის.

ჯგუფისათვის მიჭებული ნებართვა ვრცელდება მის თითოეულ წევრზე.

დაცვის დამატებითი საშუალებები.

არსებობს ქსელის უსაფრთხოების გაზრდის სხვადასხვა მეთოდი.

ასეთი მეთოდებია:

- აუდიტი;
- უდისკო კომპიუტერები;
- მონაცემების დაშიფვრა.

აუდიტი

აუდიტი (auditing) – ეს სერვერის უსაფრთხოების ჟურნალში წარმოებული ჩანაწერებია.

ეს ჩანაწერები ქსელში მომხმარებელთა მოქმედების თვალყურის დევნების საშუალებას იძლევიან. ჩანაწერები ქსელის დაცვის ელემენტს წარმოადგენს, ვინაიდან ჟურნალში ასახულია ყველა იმ მომხმარებლის მონაცემები, რომელიც მუშაობდა კონკრეტულ რესურსთან ან მცდელობა ქონდა შეედწეა მასთან.

აუდიტი აფიქსირებს:

- ქსელში შედწევის მცდელობებს;
- მოცემულ რესურსთან მიერთებას და მისგან გათიშვას;

- საადრიცხვო ჩანაწერების ბლოკირებას;
- ფაილების გახსნასა და დახურვას;
- ფაილების მოდიფიკაციას;
- პაროლების შეცვლას;
- რეგისტრაციის პარამეტრების შეცვლას და მრავალ სხვას.

საერთოდ აუდიტი გვიჩვენებს თუ როგორ ფუნქციონირებს ქსელი.

ადმინისტრატორმა აუდიტის ჟურნალი შეიძლება გამოიყენოს ქსელის ფუნქციონირების ანგარიშის წარდგენის დროს, ასევე რაიმე სიტუაციის ანალიზის აუცილებლობის შემთხვევაში. განსაკუთრებით მაშინ, როდესაც ფიქსირდება ქსელში შედარებით არასაკმარისი მცდელობები და თანაც არაჩვეულებრივ დროს. ასეთი შემთხვევების ანალიზმა შეიძლება გამოავლინოს ის მომხმარებლები, რომლებიც ცდილობენ ქსელში არასანქცონირებულად შეაღწიონ.

უდისკო კომპიუტერები.

უდისკო კომპიუტერები თავის შემადგენლობაში არ შეიცავენ მუდმივი მასსოვრობის კომპონენტებს. მათ შეუძლიათ შეასრულონ დავალება, მაგრამ მიღებული შედეგები არ იქნება შენახული მათ კომპონენტებში. ისინი ყველაფერს მუშაობის პროცესშივე გადასცემენ სერვერს და ფაქტიურად ფუნქციონირებენ სერვერის კომპონენტებით. უდისკო კომპიუტერებს არ გააჩნიათ ჩატვირთვის დისკები და ქსელში მათი ჩართვა სორციელდება სპეციალური მასსოვრობის მიკროსქემების საშუალებით, რომლებიც განთავსებულნი არიან საქსელო ადაპტერების დაფებზე. უდისკო კომპიუტერის ჩართვისთანავე მისი მიკროსქემა სერვერს აცნობებს, რომ კომპიუტერი აპირებს ფუნქციონირების დაწყებას. სერვერი მოახდენს რეაგირებას ამ სიგნალზე, გადასცემს რა მის ოპერატიულ მასსოვრობას ჩატვირთვის პროგრამას და უხსნის მას ქსელში ჩართვის გზას. ამის შემდეგ კომპიუტერი მუშაობს სერვერთან ერთად.

ასეთი კომპიუტერები უსაფრთხოების თვალსაზრისით სამაგალითონი არიან. მომხმარებელს არა აქვს საშუალება გადმოიწეროს და გამოიტანოს სამუშაო ადგილიდან რაიმე ინფორმაცია, რომელიც მისთვის ხელმისაწვდომია მუშაობის პროცესში.

მონაცემების დაშიფვრა

კონფიდენციალური ინფორმაციის უსაფრთხო გადაცემის აუცილებლობის შემთხვევაში სპეციალური უტილიტა ახდენს მის დაშიფვრას და იგი მხოლოდ ასეთი სახით გაიგზავნება ქსელში.

ეს ინფორმაცია, მიღებული შესაბამის კომპიუტერზე, გაივლის გაშიფვრის პროცესს და აღდგება საწყისი სახით.

დაშიფრული სახით გაგზავნილ შეტყობინებაში ჩადებული ინფორმაციის ამოცნობა კი მათთვის, ვინც მას არასანქციონირებულად ჩაიგდებს ხელში (მიუერთდება კაბელს, დაიჭერს გამოსხივებულ ელექტრომაგნიტურ ტალღას და ა.შ.) მეტად გართულებულია. ყოველ შემთხვევაში ძნელია ოპერატიული რეაგირება შესაბამის ინფორმაციაზე.

ინფორმაციის დაშიფვრისათვის იქმნება სპეციალური ავტომატური აპარატურა. იგი სპეციალური სტანდარტებით ახორციელებს როგორც დაშიფვრის, ასევე გამოშიფვრის პროცესებს. ინფორმაციის დაშიფვრისა და გამოშიფვრის მიზნებისათვის სახელმწიფო დონეზე, კორპორაციებისა და მსხვილი ფირმების დონეზე იქმნება სპეციალური კოდები, რომლებიც მხოლოდ მომხმარებელთა შეზღუდული წრისათვის არის ცნობილი. ამით ინფორმაციული უსაფრთხოების დონე უფრო მაღალ საფეხურზეა აყვანილი.

ვირუსებისაგან დაცვა

კომპიუტერულ ქსელებში ინფორმაციის უსაფრთხო დამუშავების ერთერთი მნიშვნელოვანესი ხელშემშლელი პირობაა ვირუსების არსებობა.

ვირუსი (< virus ლათ. საწამლავი) კომპიუტერულ ტექნოლოგიებში სპეციალური პროგრამაა, რომელიც იმგვარადაა შექმნილი, რომ შეუძლია თავად ჩაერთოს საოპერაციო სისტემაში და მოახდინოს ზემოქმედება (ყველა სახის: გააქროს, შეცვალოს, დაამახინჯოს და ა.შ.) მასში არსებულ, როგორც მომხმარებლის, ასევე კომპიუტერის შიდა სამომსახურეო ფაილებზე.

ქსელის დაცვის ღონისძიებების გატარების დროს მხედველობაში უნდა იქნეს მიღებული ვირუსების მავნე ზემოქმედება. სადღეისოდ არ არსებობს მათგან თავდაცვის უნივერსალური საშუალება, თუმცა სპეციალური პროგრამებისა და ღონისძიებების საშუალებით შესაძლებელია მათი მავნე გავლენის მასშტაბების მნიშვნელოვნად შემცირება.

ასეთი ღონისძიებებია:

- ვირუსების მოცილება;
- ვირუსების აქტივიზაციის შეფერხება;
- ანტივირუსული პროგრამების დაყენება და სხვა.

ვირუსების საწინააღმდეგოდ მიმართულ ღონისძიებად ასევე უნდა ჩაითვალოს ქსელში არასანქციონირებული შეღწევის გამორიცხვა, ვინაიდან სწორედ ეს იქცევა ხოლმე ვირუსების შეტანის წყაროდ.

ადმინისტრატორმა უნდა განახორციელოს ვირუსებისაგან დაცვის პროგრამული და ორგანიზაციული ღონისძიებები, რათა უზრუნველყოს ქსელის ფუნქციონირება ინფორმაციული უსაფრთხოების მაღალი დონით.

1.5. მონაცემების დაკარგვის თავიდან აცილება

მიმოხილვა

მომხმარებლისათვის ქსელი, რომ იყოს მოხერხებული, საიმედო და უსაფრთხო ინსტრუმენტი უდიდესი მნიშვნელობა აქვს მასში მონაცემების დაკარგვის შესაძლებლობის გამორიცხვას.

ქსელში მონაცემების დაკარგვის მრავალი მიზეზი არსებობს და თითოეული მათგანი განხილვისა და შესწავლის საგანს უნდა წარმოადგენდეს. ეს საშუალებას იძლევა დაისახოს პროგრამული, აპარატურული და სხვა სახის ღონისძიებები ამ მიზეზების გამოვლენათა ლიკვიდაციის მიზნით.

მონაცემების ფიზიკური დაცვა

მონაცემების ფიზიკური დაცვის ორგანიზება აუცილებელია იმ მრავალრიცხოვანი მიზეზების გამო, რომლებმაც შეიძლება გამოიწვიონ მათი ფიზიკური განადგურება. ამ მიზეზებს უბედურებებს უწოდებენ. ასეთი უბედურებები კი შეიძლება გამოიწვიოს ბევრმა რამემ: ადამიანის მოქმედებიდან - ბუნებრივ კატაკლიზმებამდე.

ამ მიზეზებიდან აღსანიშნავია:

- ქურდობა და ვანდალიზმი;
- ხანძარი;
- ბუნებრივ მოვლენები (ელვა, მიწისძვრა, ქარიშხალი, წყალდიდობა);
- ელექტროკვების მტყუნება და ძაბვის მნიშვნელოვანი ნახტომები;
- კომპონენტთა მტყუნება.

ქსელის გაჩერება, გამოწვეული განსაკუთრებული მიზეზების გამო, ყოველთვის უბედურებაა და დაკავშირებულია მნიშვნელოვან ფინანსურ და ტექნიკურ დანაკარგებთან.

ქსელის სიცოცხლისუნარიანობის აღსადგენად საჭიროა მონაცემების მობილიზირება სარეზერვო სისტემებიდან (სწორედ მათი არსებობის აუცილებლობის საკითხს განვიხილავთ ამ პარაგრაფში). ასეთი რეზერვებისა და სხვა პრევენციული ღონისძიებების გარეშე ქსელების, განსაკუთრებით დიდი და გლობალურის, მტყუნება ინფორმაციის უზარმაზარი ნაკადების განადგურების მიზეზი ხდება და შედეგები კი

კატასტროფულია არამართო ცალკეული კონცერნისა თუ ფირმისთვის, არამედ საერთოდ საზოგადოებისათვის.

მონაცემთა კატასტროფული განადგურების გამორიცხვა შესაძლებელია წინმსწრები ღონისძიებების გატარებით.

ასეთი ღონისძიებებია:

- მონაცემთა სარეზერვო ასლების გადაღება;
- გარანტირებული კვების წყაროების გამოყენება;
- მტყუნებამდგრადი სისტემების ორგანიზება.

მონაცემთა ასლების გადაღება

მონაცემების კატასტროფული დაკარგვისაგან დაცვა შესაძლებელია შედარებით უბრალო და არც თუ ძალიან ძვირად ღირებული გზით – პერიოდულად სარეზერვო ასლის გადაღების გზით. შემდგომ კი მიღებული მასალის განსხვავებულ და საიმედო ადგილზე შენახვით.

რეზერვირების საიმედო სტრატეგია მინიმუმამდე ამცირებს მონაცემების დაკარგვის რისკს. ამ სტრატეგიის განხორციელებისათვის კი საჭიროა:

- მოწყობილობა, რომელიც ამ მიზანს ემსახურება;
- ასლების გადაღების სათანადო მექანიზმის ორგანიზება;
- თანამშრომლები, რომლებიც ამ საქმეს ემსახურებიან.

მოწყობილობა, უმეტეს შემთხვევაში, ეს მაგნიტური დისკები, ფირები, კომპაქტდისკები და ფლეშ-კარტებია.

ამ ღონისძიებების გატარებისათვის გაწეული ხარჯები წარმოუდგენლად მცირეა იმ სავალალო შედეგებთან შედარებით, რაც შეიძლება გამოიწვიოს მონაცემების დაკარგვამ.

სარეზერვო ასლების გადაღების სისტემა

რეზერვირების ზოგადი პრინციპი ასეთია: თუ არ შეგიძლია იარსებო რაიმეს გარეშე (იგულისხმება ინფორმაციასთან დაკავშირებით), დაამზადე მისი ასლი.

ასლების გადაღების ობიექტები შეიძლება იყვნენ კატალოგები და ფაილები, სხვადასხვა დანიშნულების მონაცემების წყაროები, რომლებიც ინფორმაციის მთელ მასივებს შეიცავენ.

მონაცემების რეზერვირებისათვის შემუშავებულ უნდა იქნეს მთელი სისტემა. მონაცემების ასლების გადაღება შეიძლება განხორციელდეს მაგალითად, ყოველდღიურ, ყოველკვირეულ და ყოველთვიურ რეჟიმში, იმისდა მიხედვით თუ რამდენად მნიშვნელოვანია ესა თუ ის ინფორმაცია და რა სიხშირით ხდება მისი განახლება.

რეზერვირების პროცესმა რომ არ შეაფერხოს ქსელის ნორმალური ფუნქციონირება ასლის გადაღების დრო სათანადოდ უნდა იქნეს შერჩეული – როდესაც ქსელი ყველაზე ნაკლებადაა დატვირთული. ასევე მიზანშეწონილია მომხმარებელთა წინასწარი ინფორმირება ქსელში მიმდინარე რეზერვირების პროცესებთან დაკავშირებით. ეს კი გაუგებრობების თავიდან აცილების საიმედო საშუალებაა.

ტესტირება და შენახვა

სარეზერვო ასლის გადაღების იდეალური ვარიანტია ორი სარეზერვო ასლის გადაღება, რომელთაგან ერთი იქვე იქნება შენახული, ხოლო მეორე სხვა საიმედო ადგილზე.

ასლების გადაღების ორგანიზებას კონტროლს ადმინისტრატორი უწევს. მან რეგულარულად უნდა აწარმოოს სარეზერვო ასლების გადაღების პროცედურების ტესტირება, რათა დარწმუნებული იყოს, რომ რისი რეზერვირებაც უნდა მოხდეს, მართლაც რეზერვირდება. ეს კი გარანტია იქნება იმის, რომ საჭიროების შემთხვევაში ქსელი დიდი დანაკარგების გარეშე აღადგენს ნორმალურ ფუნქციონირებას.

სარეზერვო ასლების გადაღების ჟურნალი

სარეზერვო ასლების გადაღების ჟურნალის არსებობა დიდ დახმარებას უწევს ადმინისტრატორს დაკარგული და დამახინჯებული ფაილების აღდგენის პროცესში. ამიტომ აუცილებელია ასეთი ჟურნალის არსებობა და იგი უნდა ინახებოდეს იქვე, სადაც სარეზერვო ასლების გადაღების მასალებია განთავსებული.

სარეზერვო ასლების გადაღების ჟურნალში შეიტანება შემდეგი სახის ინფორმაცია:

- სარეზერვო ასლის განთავსების ადგილი;
- სარეზერვო ასლების გადაღების განხორციელების დრო;
- ინფორმაციის მატარებლის საიდენტიფიკაციო მარკერები;
- ინფორმაციის მომწოდებლის მონაცემები;
- შენახული ფაილების სახელები და პარამეტრები;
- ასლების გადაღები პირის მონაცემები.

სარეზერვო ასლების გადაღების ორგანიზება

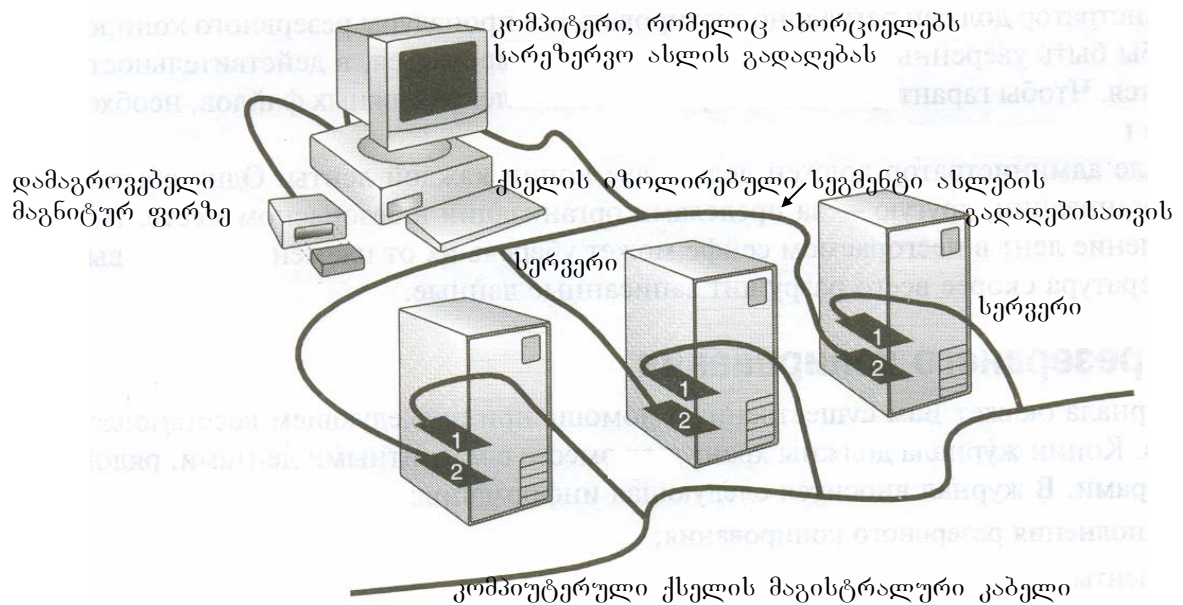
ასლების გადაღების მიზნით მაგნიტურ დამაგროვებელზე ინფორმაციის ჩაწერა სორციელდება ან უშუალოდ სერვერთან მიერთებით ან რომელიმე კომპიუტერის გამოყენებით.

პირველ შემთხვევაში, როგორც რეზერვირების, ასევე აღდგენის ოპერაციები სწრაფად მიმდინარეობს, ვინაიდან ამ დროს ქსელი არ გამოიყენება.

სარეზერვო ასლების გადაღება ქსელის გამოყენებით, ერთი მხრივ მოხერხებული მეთოდია, მეორე მხრივ იგი წარმოქმნის მნიშვნელოვან საქსელო ტრაფიკს და, შესაბამისად, ზრდის ქსელის რეაგირების დროს მომხმარებელთა მოთხოვნებზე. ეს კი ქსელის წარმადობის შემცირების ხარჯზე ხდება. აქედან გამომდინარე, უმჯობესია რეზერვირებისათვის შეირჩეს პერიოდი, როდესაც სერვერი ნაკლებადაა დატვირთული

თუ ქსელში რამდენიმე სერვერი კომპაქტურადაა განთავსებული, მაშინ რეზერვირებით გამოწვეული ტრაფიკის შემცირება შესაძლებელია იმ კომპიუტერის იზოლირებულ სეგმენტზე მიერთებით, რომლის გავლითაც ხორციელდება ასლების გადაღება.

ამ შემთხვევაში, ასლების გადაღებისათვის დანიშნული კომპიუტერი უერთდება სერვერის ასლის გადაღების საქსელო დაფას, როგორც ეს ნაჩვენებია ნახაზზე 1.6.



- 1 – დაფა სერვერის ქსელთან მუშაობისათვის
- 2 – დაფა სერვერისა და ასლის გადაღების კომპიუტერის ურთიერთქმედებისათვის

ნახ. 1.6. სარეზერვო ასლის გადაღება იზოლირებული სეგმენტის გამოყენებით

გარანტირებული კვების წყარო

გარანტირებული კვების წყარო – ეს კვების გარე წყაროა, რომელიც უზრუნველყოფს მასთან მიერთებული ქსელის კომპონენტის უწყვეტ ელექტროკვებას.

გარანტირებული კვების პირობებში ქსელის კომპონენტებმა მუშაობა შეიძლება გააგრძელონ ძირითადი წყაროს მწყობრიდან გამოსვლის შემთხვევაში. ეს პროცესი შეიძლება გაგრძელდეს საკმაოდ დროის განმავლობაში (ათეული წუთიდან რამდენიმე საათამდე და ზოგჯერ კიდევ უფრო მეტ ხანს) ან სულ რამდენიმე წუთს, სანამ ძირითადი წყარო არ დაუბრუნდება მუშა მდგომარეობას.

გარანტირებული კვების წყარო შეიძლება თვითონ ენერგიას იღებდეს აკუმულატორისაგან, სპეციალური გარდამსახისაგან, მაგალითად, ძრავი – გენერატორი, ან რომელიმე არატრადიციული ენერჯის (მაგალითად, მზის ენერჯის გარდამსახი) წყაროსაგან.

ძირითადი წყაროს შეფერხების შემთხვევაში გარანტირებული კვების წყარო გამაფრთხილებელ სიგნალს აწვდის ადმინისტრატორს და მომხმარებელს, თვითონ კი ირთვება მუშაობაში.

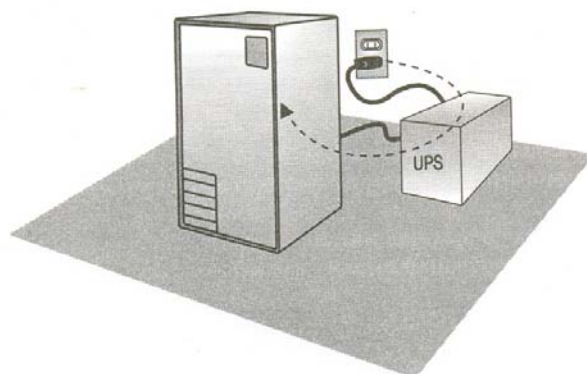
თუ ძირითადი წყაროს მუშა მდგომარეობის აღდგენა მოხდება გარანტირებული კვების წყაროს შესაძლო ფუნქციონირების ვადებში, ქსელის მოცემული კომპონენტი გააგრძელებს ნორმალურ ფუნქციონირებას. თუ შეფერხება უფრო ხანგრძლივია იგი გამოყვანილი უნდა იქნეს ექსპლატაციიდან.

ეს პროცესი მიმდინარეობს ადმინისტრატორის მეთვალყურეობის ქვეშ და იგი ატარებს ყველა ღონისძიებას, მისი კომპენტენციის ფარგლებში, შექმნილი მდგომარეობის მოსაწესრიგებლად.

გარანტირებული კვების ორგანიზების ორი ძირითადი მეთოდი არსებობს.

ერთ შემთხვევაში გარანტირებული კვების წყარო მუდმივ მუშაობაშია. იგი იღებს ენერგიას ძირითადი წყაროსაგან (რომელიც ჩვეულებრივად ცვლადი დენის წყაროა), გარდაქმნის მას მუდმივ დენად და მუხტავს აკუმულატორს. აკუმულატორი ენერგიას აწვდის გარდამსახს, რომელიც მას კვლავ გარდაქმნის ცვლადი დენის ენერჯიად და ასე აწვდის სათანადო მოწყობილობას, როგორც ეს ნაჩვენებია ნახაზზე 1.7.

გარანტირებული კვების ასეთი სისტემებისათვის დამკვიდრებული სახელია- უწყვეტი კვების წყარო UPS- Uninterrupted power supply.



ნახ. 1.7. გარანტირებული კვების ორგანიზების სურათი

ასეთი სახით კვების ორგანიზება არ გამოირჩევა მაღალი მარგი მოქმედების კოეფიციენტით, ვინაიდან ენერჯის ორჯერადი გარდაქმნა ხორციელდება:

ცვლადიდან მუდმივისაკენ და მუდმივიდან ცვლადისაკენ. სამაგიეროდ ეს სისტემა უზრუნველყოფს მოწყობილობების უწყვეტ ელექტროკვებას.

მეორე შემთხვევაში გარანტირებული კვების წყარო მხოლოდ ძირითადის გათიშვის შემდეგ ირთვება და თავისთავზე იღებს მოწყობილობების კვებას. ამ სახით კი უწყვეტი კვების ორგანიზება პრინციპულად შეუძლებელია, თუმცა წყვეტა შეიძლება მეტად ხანმოკლე იყოს.

ყოველ კონკრეტულ შემთხვევაში ადმინისტრატორის გადასაწყვეტია, თუ გარანტირებული კვების რომელი გზა იქნეს არჩეული.

მტყუნებამდგრადი სისტემები

მიმოხილვა

კომპიუტერულ ტექნოლოგიებში ინფორმაციის შენახვისათვის ფართოდ გამოიყენებენ მყარ დისკებს. მყარი დისკი – ეს ერთი ან რამდენიმე მყარი ფირფიტაა, რომელზეც დატანილია ინფორმაციის მატარებელი ფენა. ფირფიტებზე დატანილი ფენა შეიძლება იყოს ფერომაგნიტური, ოპტიკური და მაგნიტოოპტიკური.

სადღეისოდ სარეზერვო ასლების გადაღების სისტემებში ძირითადად ინფორმაციის ფერომაგნიტური მატარებლები გამოიყენება და მათ მაგნიტურ დისკებს უწოდებენ.

ფუნქციონირების დროს მაგნიტური დისკი დიდი სიჩქარით ბრუნავს (3600-დან 10 000-მდე ბრუნი წამში). ჩაწერისა და ამოკითხვის მაგნიტური თავები საჰაერო ბალიშზე ლივლივებენ 0,2 – 0,5 მიკრონის მანძილზე და უკონტაქტო მეთოდით აწარმოებენ ინფორმაციის ჩაწერასა და ამოკითხვას. ვინაიდან ისინი უშუალოდ არ ეხებიან ფერომაგნიტურ დისკებს გამოირიცხება მაგნიტომატარებლის მექანიკური დაზიანება.

ამგვარად, მყარი დისკი - ეს მეტად რთული მექანიკურ – ელექტრონული მოწყობილობაა. მისი დამზადებისათვის გამოიყენება უახლესი ტექნოლოგიები და შედეგებიც საუკეთესოა: მიღწეულია მათი საიმედოობის მაღალი დონე.

მაგნიტური დისკის ფირფიტები შეფუთულნი არიან სპეციალურ ჰერმეტიულ გარემოში და ქმნიან ბლოკს, რომელსაც კასეტას უწოდებენ. ასეთი კასეტები მოხერხებულია გადასატანად და უსაფრთხო ადგილზე დასაბინავებლად, მაგალითად, საბანკო სეიფებში.

მიუხედავად ყველაფერი ამისა, მყარი დისკი, ისევე როგორც ნებისმიერი სხვა რამ, მუდმივი არ არის და ყოველთვის შესაძლებელია მისი დაზიანება და მოწყობრიდან გამოსვლა. ყველა სახის მოწყობილობას, მექანიკური იქნება ის, თუ ელექტრონული, მტყუნებამდე მუშაობის გარკვეული დრო გააჩნია. ამავე დროს თუ გავიხსენებთ ცნობილ თეზისს, რომელიც ამბობს: „ყველაფერი ცუდი, რაც უნდა

მოხდეს, ის ადრე თუ გვიან, აუცილებლად მოხდება“- დისკების მწყობრიდან გამოსვლაც მოსალოდნელია და ბუნებრივი.

ასეთ პირობებში მტყუნებამდგრადი, კარგად მოფიქრებული და რეალიზებული სისტემების არსებობას უდიდესი მნიშვნელობა აქვს მონაცემების დაკარგვისა და განადგურებისაგან დაცვის საქმეში.

მტყუნებამდგრადი სისტემების შექმნის მეთოდები

მტყუნებამდგრადი სისტემები უზრუნველყოფენ ინფორმაციის დაკარგვისაგან დაზღვევას ადგილზე, უშუალოდ კომპიუტერულ ტექნოლოგიებში მიმდინარე პროცესების დროს წარმოშობილი ხელშემშლებისა და დაბრკოლებების გამო. მართალია, ისინი ვერ დაიცავენ ინფორმაციას ადგილზე მომხდარი სტიქიური უბედურებებისაგან, ხანძრისაგან, წყალდიდობისაგან და სხვა მსგავსი მოვლენებისაგან, მაგრამ უდიდეს როლს თამაშობენ კომპიუტერული მომსახურების პროცესის ნორმალურ მსვლელობაში.

მტყუნებამდგრადი სისტემების მოქმედების ძირითადი იდეა ინფორმაციის შენახვის მეთოდებში სიჭარბის შეტანა და მისი (ინფორმაციის) განთავსება სხვადასხვა ფიზიკურ მატარებელზე.

მტყუნებამდგრადი სისტემების შექმნის მეთოდებია:

- დისკების მორიგეობა;
- დისკების სარკისებური ასლის შექმნა;
- დისკების სარკისებური დუბლირება;
- დისკების მორიგეობა შემოწმებით ლუწობაზე;
- დისკების მასივის სარკისებური ასლის შექმნა;
- სექტორების გადანაცვლება;
- კლასტერული სისტემის ორგანიზება.

არაძვირადღირებული დისკების სიჭარბის მასივები

მტყუნებამდგრადი სისტემების ტიპების სტანდარტიზაცია და კლასიფიკაცია დონეების მიხედვით ხორციელდება. ეს დონეები გამოიხატება ე.წ. არაძვირადღირებული დისკების (Redundant Arrays of Inexpensive Disks – RAID) გამოყენების სახით.

RAID – ეს არის მყარი დისკების ერთობლიობა, რომელიც ფუნქციონირებს, როგორც ერთი მოწყობილობა. ამ დისკების მოქმედება და გამოყენება განსხვავებულია RAID – ის დონეების მიხედვით. საერთო პრინციპი კი ის არის, რომ ერთი მათგანის მტყუნების შემთხვევაში სხვები აგრძელებენ ფუნქციონირებას და

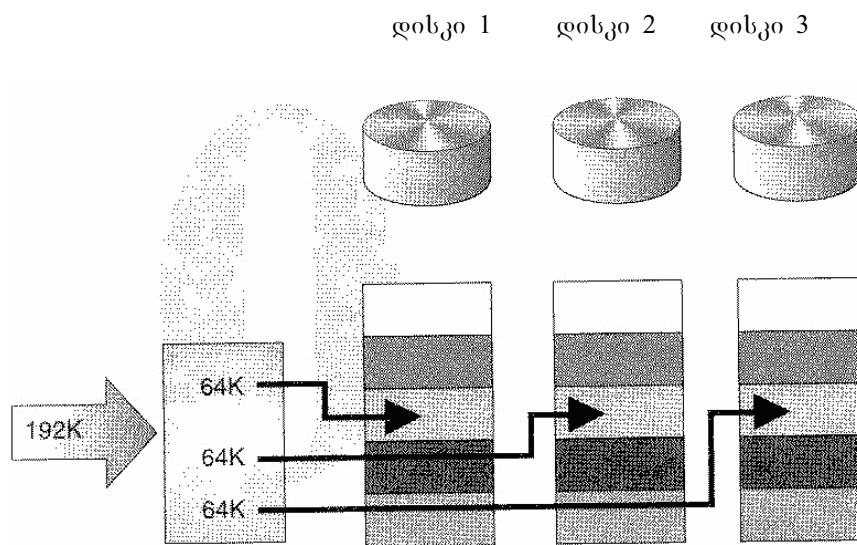
უზრუნველყოფენ ინფორმაციის დამუშავების ერთიანი სისტემის მაღალ სიციცხლისუნარიანობას.

RAID-ის ფუნქციონირება რამდენიმე დონედ იყოფა.

განვიხილოთ მათ შორის ყველაზე გავრცელებული: RAID - 0; RAID - 1; RAID - 5.

დონე RAID – 0.

ეს დონე ემყარება დისკების მორიგეობის მეთოდს. ამ დროს მონაცემები იყოფა 64 კბაიტის ბლოკებად და თანაბრად ნაწილდება დისკების მასივზე. მასივში შემავალ დისკთა საერთო რაოდენობა 2-დან 32-მდეა.



ნახ. 1.8. დისკების მორიგეობის სურათი

ნახაზზე 1.8 ნახვენებია სამი დისკის მორიგეობის სურათი. ამ შემთხვევაში მონაცემების საერთო მოცულობა შეადგენს 192კბაიტს. ერთი ნაწილი, 64კბაიტი ჩაწერილია დისკზე 1, მეორე – ასევე 64კბაიტი დისკზე 2 და მესამე – ასევე 64კბაიტი დისკზე 3.

ამგვარად, იქმნება ერთიანი ლოგიკური დისკი, თუმცა იგი ვერ უზრუნველყოფს საიმედოობის გაზრდას, რადგან არ წარმოქმნის ამისთვის აუცილებელ მონაცემთა სიჭარბეს.

ამ სახით დისკების მორიგეობა ზრდის მათ წარმადობას, ვინაიდან რამდენიმე მათგანზე ინფორმაციის პარალელურად ჩაწერისა და ამოკითხვის საშუალებას იძლევა.

დისკების მორიგეობის ამ მეთოდის მიკუთვნება მტყუნებამდგრადი სისტემებისთვის პირობითია და განპირობებულია იმით, რომ იგი აუმჯობესებს საერთო საექსპლუატაციო მაჩვენებლებს.

დონე RAID –1.

ეს დონე ემყარება დისკების სარკისებური ასლის შექმნის მეთოდს. ამ დროს მონაცემები ჩაიწერება პარალელურად ორ დისკზე, ე. ი. უწყვეტად მიმდინარეობს სარეზერვო ასლის გადაღება. ინფორმაციის ნებისმიერი ნაწილი ორ დისკზეა განთავსებული და იგი დაცულია რომელიმე მათგანის მტყუნების დროს.

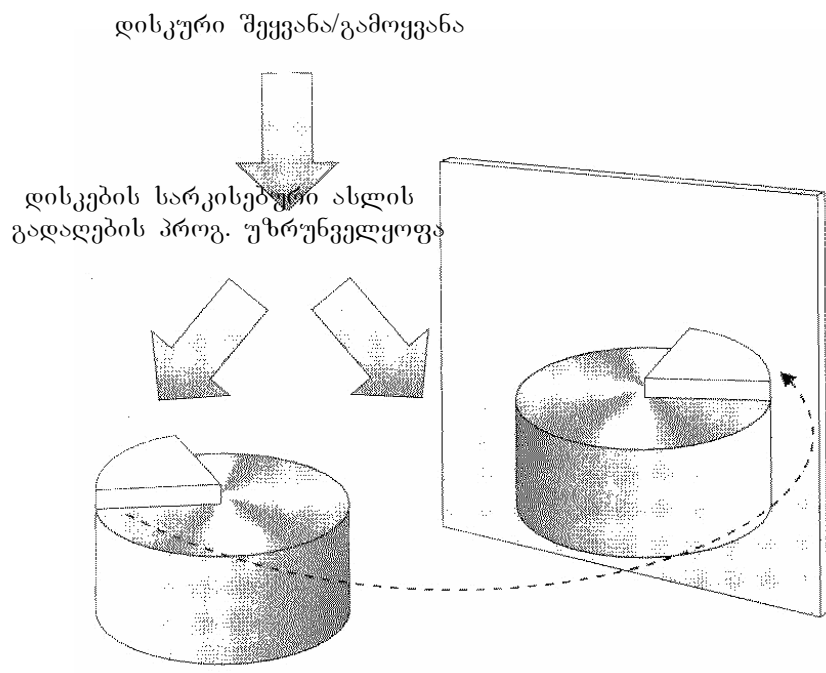
ამ შემთხვევაში ორივე დისკთან ერთი კონტროლერი მუშაობს.

კონტროლერი (controller) – ეს ელექტრონული მოწყობილობაა, რომელიც ახორციელებს მართვის პროცესს.

არსებობს დისკების სარკისებური ასლის შექმნის მეთოდის მეორე ვარიანტი, რომელიც დისკების სარკისებური დუბლირების სახელით მოიხსენიება.

ამ შემთხვევაში თითოეულ დისკს თავისი კონტროლერი მართავს. ასე რომ კონტროლერის დუბლირებაც ხდება და ეს კიდევ უფრო ზრდის სისტემის საიმედოობას.

ნახაზზე 19 წარმოდგენილია შეტყობინების დაცვის მაგალითი დისკების სარკისებური ასლის შექმნის გზით.



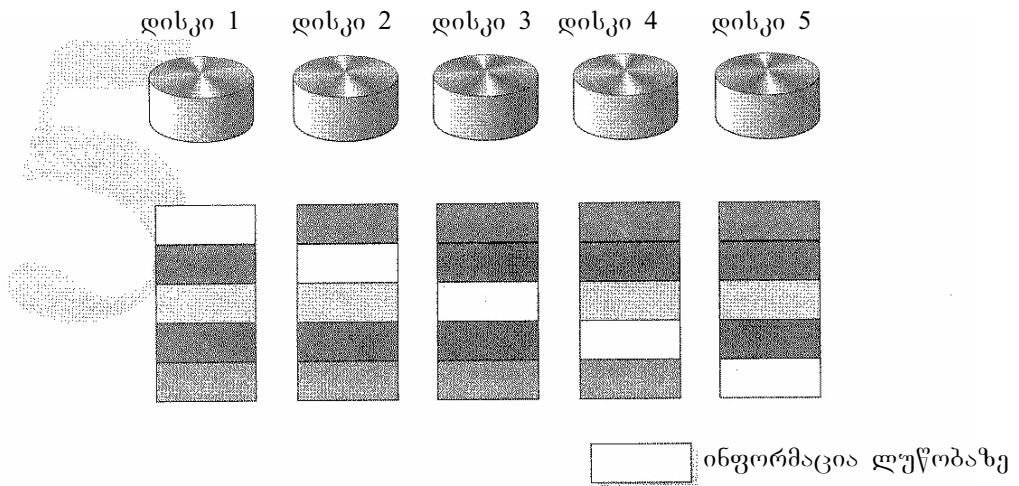
ნახ. 19. დისკების სარკისებური ასლის შექმნის სურათი

დონე RAID –5.

ეს დონე ემყარება ლუწობაზე შემოწმებითი დისკების მორიგეობის მეთოდს.

შემოწმება ლუწობაზე – ეს შეტყობინების სწორად გადაცემის ერთერთი მეთოდია, რომელიც მასში (შეტყობინებაში) სიჭარბის შეტანით ხორციელდება.

ნახაზზე 1.10 წარმოდგენილია ხუთ დისკზე ძირითადი ინფორმაციისა და შესაბამისი ლუწობის ინფორმაციის განაწილების სურათი.



ნახ. 1.10. ლუწობაზე შემოწმებითი დისკების მორიგეობის მეთოდი

ამ დროს სასიგნალო ელემენტების - ბიტების გარკვეულ რაოდენობაში ყოველთვის ბიტების ლუწი რაოდენობა უნდა იყოს. თუ რეალურ სიგნალში ის თავისთავად ლუწია, მას ემატება ელემენტი ნული, ხოლო თუ კენტია - ერთიანი.

ლუწობაზე შემოწმებითი დისკების მორიგეობის მეთოდის გამოყენების დროს თითოეულ დისკზე განთავსდება, როგორც უშუალოდ ინფორმაცია, ასევე მისი ლუწობაზე შემოწმების მონაცემები. ეს გარემოება კი მნიშვნელოვნად ზრდის იმ ინფორმაციის აღდგენის შესაძლებლობას, რომელიც განთავსებულია მტყუნებად დისკზე.

შემოწმება ლუწობაზე ფართოდ გამოიყენება ცალკეული კომპიუტერის შიგნით შეტყობინების გადაადგილების დროს ან ერთობლივად მომუშავე კომპიუტერულ სისტემებში ერთმანეთს შორის შეტყობინებების გაცვლის პროცესებში.

ლუწობაზე შემოწმებითი დისკების მორიგეობის მეთოდი სადღეისოდ ყველაზე პოპულარული მტყუნებამდგრადი სისტემაა, მასში შეიძლება შედიოდეს დისკების ერთობლიობა 3-დან 32-მდე.

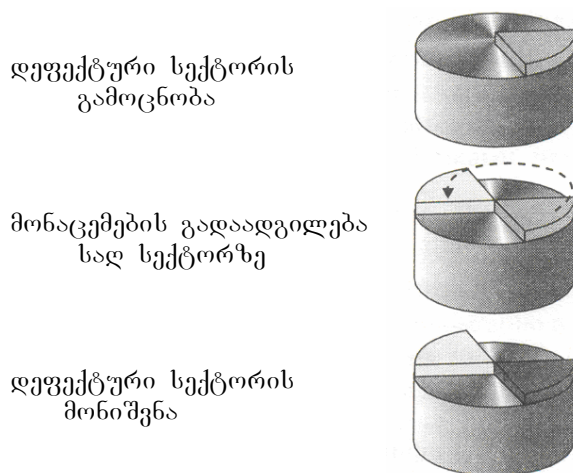
სექტორების გადანაცვლება

მტყუნებამდგრადობის გაზრდის ერთერთი მეთოდია სექტორების გადანაცვლება.

თუ დისკზე ინფორმაციის შეყვანა/გამოყვანის პროცესში აღმოჩენილ იქნება დაზიანებული სექტორი, შესაბამისი დრაივერი ამ ინფორმაციას გადაიტანს კარგ სექტორზე, ხოლო დაზიანებულ სექტორს მონიშნავს. ამ პროცესს „ცხელ შეცვლას“ უწოდებენ (ნახ. 1.11).

სპეციალური უტილიტები, განთავსებული საოპერაციო სისტემებში, ადმინისტრატორს ატყობინებენ სექტორებში მიმდინარე გადაადგილებებისა და საერთოდ სექტორების ყველა მტყუნების შესახებ.

ამ ღონისძიების მიზნია შეტყობინების დაცვა დაკარგვისაგან.



ნახ. 1.11. სექტორების განაცხადების სურათი

კლასტერული სისტემის ორგანიზება

კლასტერი - ეს დამოუკიდებელ სისტემათა გარკვეული ჯგუფია, რომელიც მოქმედებს, როგორც მთლიანი ერთობლიობაა. ამ ერთობლიობაში როგორც კი ერთი სისტემა გამოდის მწყობრიდან ყველა დანარჩენი ინაწილებს მის ფუნქციებს და მთელი კომპლექსი აგრძელებს მუშაობას შეუფერხებლად.

კლასტერული სისტემის ორგანიზება, ცხადია, არ ცვლის სარეზერვო ასლების გადაღების სისტემას, მაგრამ ეს ტექნოლოგია მტყუნებამდგრადობის გაზრდის ერთერთი მნიშვნელოვანი მეთოდია.

კლასტერულ სისტემაში მიმდინარე ყველა პროცესის შესახებ ეცნობება ადმინისტრატორს სათანადო ღონისძიებების გასატარებლად.

დასკვნა:

ადმინისტრატორის ძირითადი მოვალეობაა მართოს ქსელის ფუნქციონირება. ამისათვის მან უნდა გამოიმუშაოს სათანადო წესები და შემდგომ მკაცრად შეასრულოს ისინი. ადმინისტრირების სწორად წარმართვამ უნდა უზრუნველყოს ქსელში მონაცემების მაღალ დონეზე უსაფრთხო დამუშავებასაც და თვითონ ქსელის მოწყობილობათა დაცვაც.

ამ ფუნქციების შესასრულებლად ადმინისტრატორის ხელში მძლავრი იარაღია ქსელის მონიტორინგის უფლებითა და მასში მიმდინარე ნებისმიერი პროცესის კონტროლის სახით. და რაც მთავარია, ამ პროცესებზე ზემოქმედების დიდი უფლებამოსილებითა და შესაძლებლობებით.

თავი 2

მარშრუტიზაცია გლობალურ ქსელებში

2.1. ქსელი დაგროვებითი კომუტაციის მეთოდით

გლობალური კომპიუტერული ქსელი (Wide Area Network - WAN) ტელეკომუნიკაციური საშუალებებით ერთმანეთს აკავშირებს დიდ ტერიტორიაზე განაწილებულ კომპიუტერებსა და ლოკალურ კომპიუტერულ ქსელებს. ამგვარად იგი შეიძლება წარმოვიდგინოთ, როგორც ორი ძირითადი სტრუქტურის, მაგისტრალურისა და გამანაწილებლი, ანუ სამომხმარებლო ქსელების, შემცველი სისტემა.

მაგისტრალური ნაწილის შემადგენელი კომპონენტებია ტელეკომუნიკაციის ის საშუალებები, რომლებიც ემსახურებიან შეტყობინების გადაცემას დედამიწის ნებისმიერი წერტილიდან ნებისმიერ წერტილამდე. ასეთ საშუალებებს კი წარმოქმნიან ლითონის გამტარიანი და ოპტიკურ-ბოჭკოვანი კაბელებით ორგანიზებული სისშირული და დროითი შემჭიდროების მოწყობილობები, ტელეკომუნიკაციის რადიოსარელეო ხაზები, თანამგზავრული სისტემები და საკომუტაციო ცენტრები.

გამანაწილებელი ნაწილის ძირითადი შემადგენელი კომპონენტებია მომხმარებელთა სააბონენტო პუნქტები (Subscriber point SP), აღჭურვილი სხვადასხვა კლასის კომპიუტერებით და ლოკალური კომპიუტერული ქსელები (Lokal Area Network-LAN).

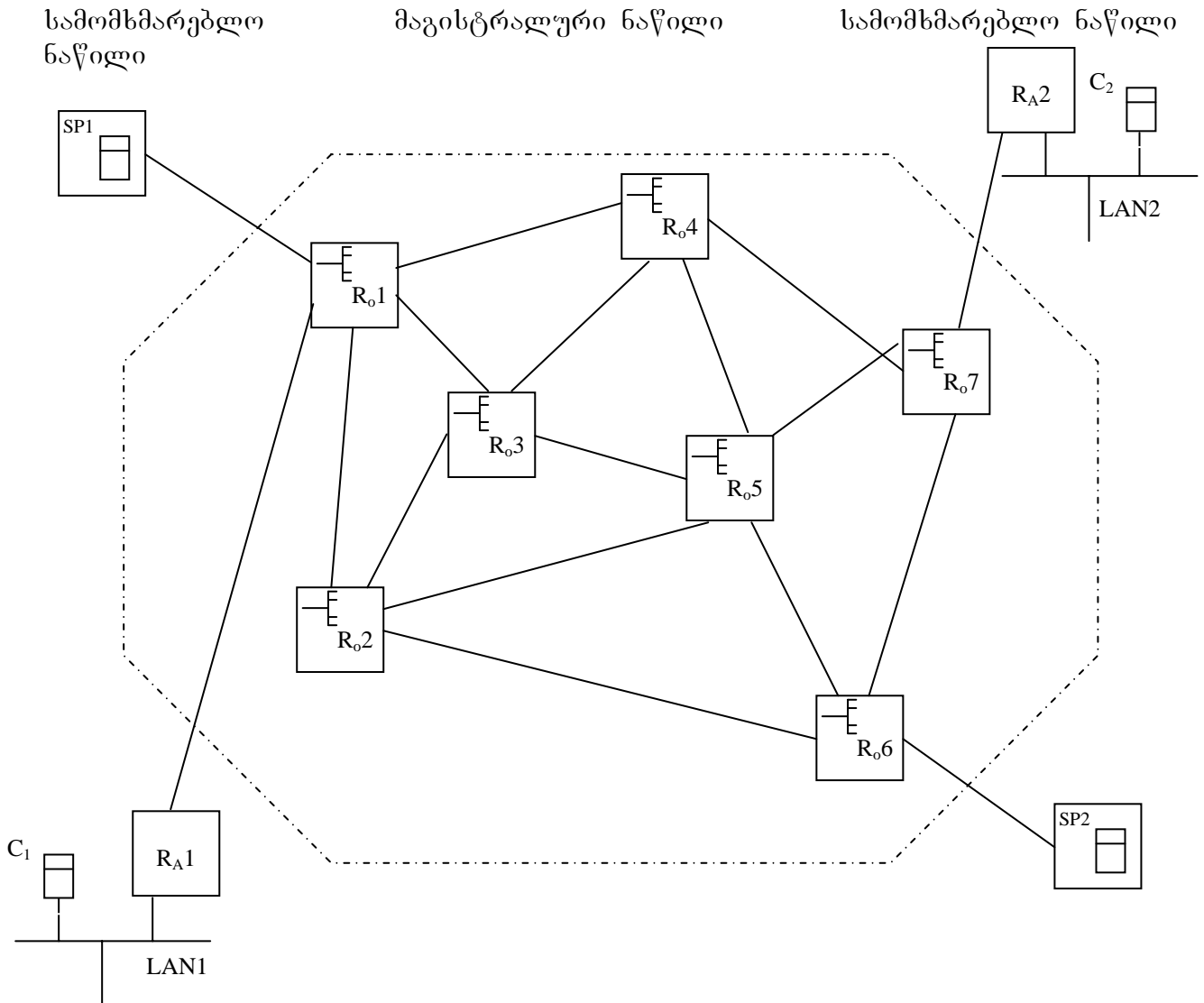
მომხმარებელთა მომსახურებისათვის იქმნება სპეციალიზირებული დწესებულება, რომელსაც ტელეკომუნიკაციის ოპერატორი (telekommunikation carrier) ეწოდება.

ოპერატორი (ლათ. operator – მოქმედი) ტრადიციული სემანტიკით აღნიშნავს იმას, ვინც თვალყურს ადევნებს ამა თუ იმ მოვლენას და მასზე სათანადო რეაგირებას ახდენს. ამჟამად სიტყვის „ოპერატორის“ განმარტებაში გარდა ტრადიციული სემანტიკისა იგულისხმება იმ ტექნიკური საშუალებებისა და მომსახურების ერთობლიობა, რომელიც უზრუნველყოფს შეტყობინების გადაცემას გარკვეულ ტერიტორიაზე ნებისმიერი წერტილიდან ნებისმიერ წერტილამდე.

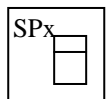
ნახაზზე 2.1 მოცემულია გლობალური კომპიუტერული ქსელის ფრაგმენტული სტრუქტურა.


გლობალური ქსელის უმნიშვნელოვანესი კომპონენტებია საკომუტაციო ცენტრები თავიანთი მრავალფეროვანი, სხვადასხვა დანიშნულების აპარატურით. მათ უნდა უზრუნველყონ ცენტრში შემოსული შეტყობინების სათანადო მიმართულებით გაგზავნა. ამ მიზნის მისაღწევად საკომუტაციო ცენტრები აღჭურვილნი არიან

სპეციალური მოწყობილობებით, მარშრუტიზატორებით (Router - R), რომლებიც ქსელში ადგენენ შეტყობინების გადასაცემ მარშრუტებს და შემდგომ ამ მარშრუტების გამოყენებით გადასცემენ მათ.



 საკომუტაციო ცენტრი ოპერატორის მარშრუტიზატორით R₀X
Router (R)

 სააბონენტო პუნქტი
Subscriber point (SP)

 ლოკალური ქსელის მარშრუტიზატორი
R_AY აბონენტის მარშრუტიზატორი Router (R_AY)

 კომპიუტერი Computer (C)

ნახ. 2.1. გლობალური კომპიუტერული ქსელი (ფრაგმენტული)

კომპიუტერული ქსელის ფრაგმენტზე (ნახ. 2.1) წარმოდგენილია ტოპოლოგია K – შეერთება, ვინაიდან მაგისტრალურ ნაწილში საკომუტაციო ცენტრებს შორის არ არის რეალიზებული სრული შეერთება. ასევე ნაჩვენებია ქსელის მაგისტრალურ ნაწილთან გამანაწილებელი, ანუ სამომხმარებლო ქსელების კომპონენტების-სააბონენტო პუნქტებისა (SP) და ლოკალური ქსელების (LAN), კავშირების სურათი.

სადღეისოდ შეტყობინების გადასაცემად ძირითადად გამოყენებულია დაგროვებითი კომუტაციის მეთოდები.

დაგროვებითი კომუტაციის არსი მდგომარეობს იმაში, რომ შემოსული შეტყობინება ჯერ ჩაიწერება სათანადო მასსოვრობის მოწყობილობაში (ე.ი. დაგროვდება), შემდეგ კი ხორციელდება მისი დამუშავება და შემდგომი გადაცემა.

რადიოტექნიკის, მიკროელექტრონიკის, ნანოტექნოლოგიების განვითარების მაღალმა დონემ შესაძლებელი გახადა შეტყობინების გადაცემის სიზუსტისა და სიჩქარის მკვეთრი გაზრდა. ამან კი განაპირობა ყველა სახის ინფორმაციის დაგროვებითი მეთოდების გამოყენებით გადაცემის შესაძლებლობა.

გლობალურ კომპიუტერულ ქსელებში შეტყობინების გადაცემა ძირითადად მისი შემადგენელ ნაწილებად, პაკეტებად, დაშლის გზით მიმდინარეობს.

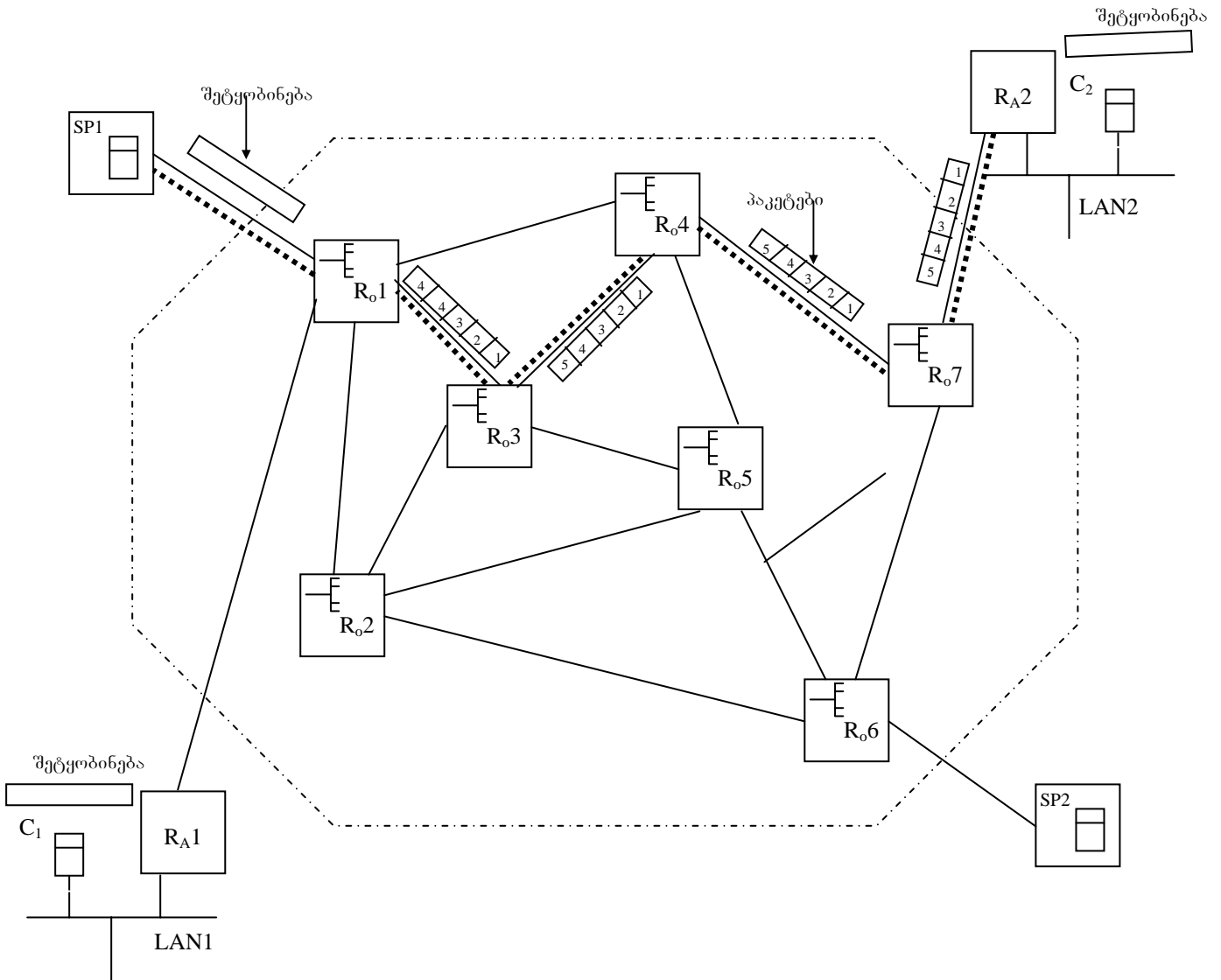
შეტყობინების შემადგენელი პაკეტების გადაცემა კომუტაციის ორი მეთოდით ხორციელდება: ვირტუალური არხებით და დატაგრამებით.

თუ მოცემულ ქსელში პაკეტების გადაცემისათვის შეირჩეა ერთი გარკვეული გზა, როგორც ეს ნაჩვენებია ნახაზზე 2.2, და ერთი შეტყობინების ყველა პაკეტი ამ გზით გადაიცემა გვექნება პაკეტების კომუტაციის ქსელი *ვირტუალური არხებით*.

ნახაზზე წარმოდგენილი სურათის მიხედვით შეტყობინება სრული სახით შემოდის სააბონენტო პუნქტიდან SP1 საკომუტაციო ცენტრში, რომელიც აღჭურვილია მარშრუტიზატორით R₀₁. ამ ცენტრში შეტყობინება იშლება, მაგალითად 5 პაკეტად (პაკეტების რიცხვი დამოკიდებულია საწყისი შეტყობინების მოცულობაზე და მოცემულ ქსელში პაკეტების მიღებულ ზომაზე). შემდეგ მარშრუტიზატორის მიერ არჩეულია მაგისტრალურ ნაწილში პაკეტების გადაცემის გზა: R₀₃ - R₀₄ - R₀₇. მარშრუტიზატორი R₀₇ ადგენს, რომ მიმდები აბონენტი ლოკალურ ქსელშია ჩართული და რომ ამ ქსელს გააჩნია სააბონენტო მარშრუტიზატორი R_{A2} და მას გადასცემს შემოსულ პაკეტებს. მარშრუტიზატორი R_{A2} ადადგენს ამ პაკეტებიდან საწყის შეტყობინებას და გადასცემს ადრესატს, კომპიუტერ C2. ამით შეტყობინების გადაცემის პროცესი სრულდება.

ქსელის მოცემული ფრაგმენტით შეტყობინების გადაცემის პროცესების ანალიზის დროს ყურადღება უნდა მიექცეს სააბონენტო მარშრუტიზატორ R_{A2}-ს. მისი

როლი და მნიშვნელობა იგივეა, რაც გააჩნიათ ოპერატორის მარშრუტიზატორებს R_oX , მხოლოდ ეკუთვნიან პერიფერიულ ნაწილს.

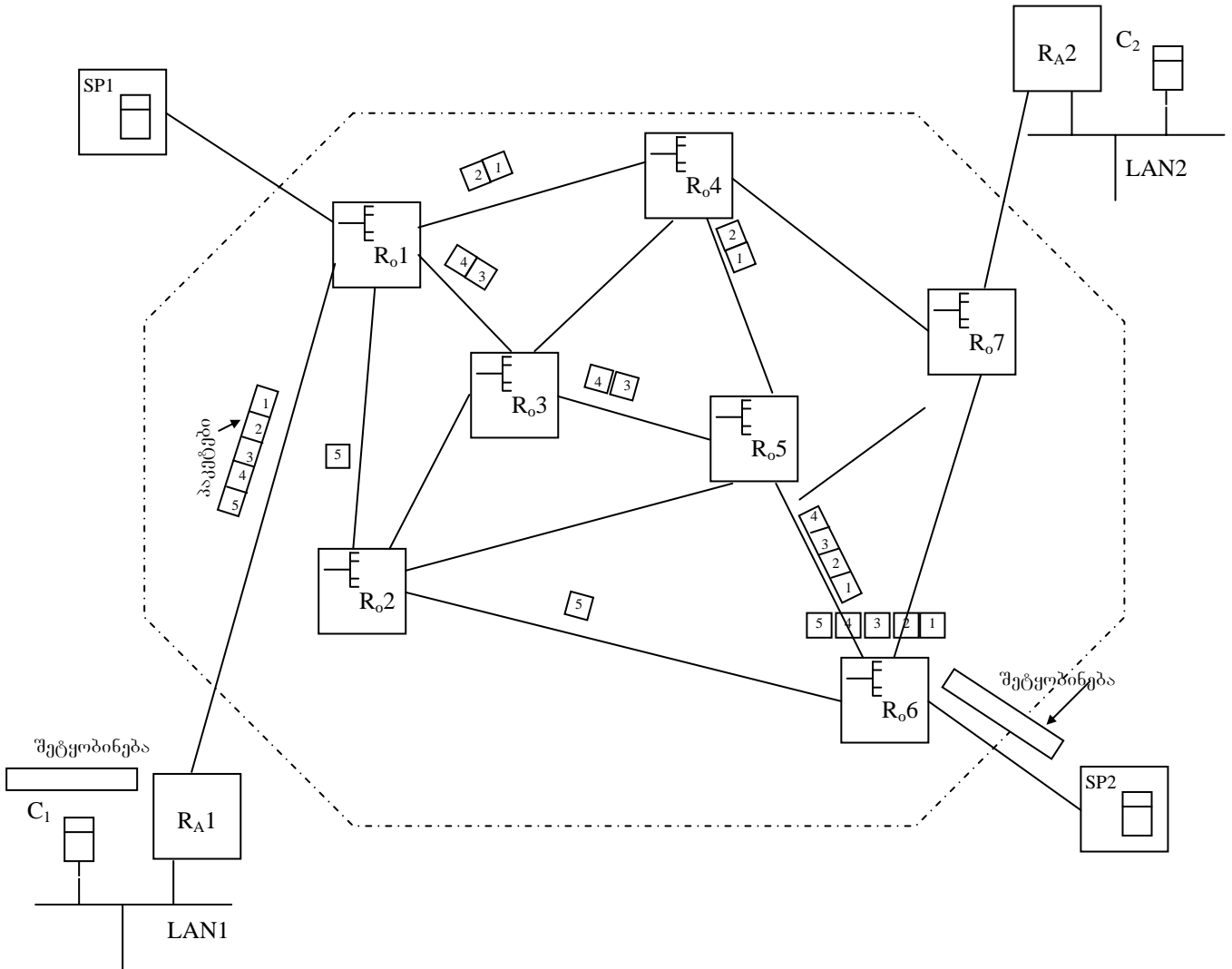


ნახ. 2.2. პაკეტების კომუტაციის ქსელი ვირტუალური არხებით

თუ მოცემულ ქსელში პაკეტების გადაცემა სხვადასხვა გზით მიმდინარეობს, როგორც ეს ნაჩვენებია ნახაზზე 2.3, გვეჩვენება პაკეტების კომუტაციის ქსელი დატავრამებით.

ნახაზზე წარმოდგენილი სურათის მიხედვით შეტყობინებას გადასცემს ლოკალურ ქსელში ჩართული კომპიუტერი C₁. შეტყობინებას, პირველ რიგში, იღებს ამ ლოკალურ ქსელში ჩართული სააბონენტო მარშრუტიზატორი R_{A1}, რომელიც ამ შეტყობინებას დაშლის, მაგალითად, 5 პაკეტად (პაკეტების რიცხვი დამოკიდებულია საწყისი შეტყობინების მოცულობაზე და მოცემულ ქსელში პაკეტების მიღებულ ზომაზე). ეს პაკეტები სრული შემადგენლობით შემოდის საკომუტაციო ცენტრში, რომელიც აღჭურვილია მარშრუტიზატორით R_{o1}. ეს მარშრუტიზატორი პაკეტების

გადაცემისათვის აღგენს გზებსა და თითოეული მათგანით გადასაცემა პაკეტების რიცხვს. მოცემულ მაგალითში ორი პაკეტი გადაეცემა მარშრუტიზატორს R_04 , ორი - R_03 -ს და ერთი R_02 . პაკეტები გადაადგილდებიან არჩეული გზებით და თავს მოიყრიან მარშრუტიზატორ R_06 , რომელთანაც დაკავშირებულია მიმღები სააბონენტო პუნქტი $SP2$. მარშრუტიზატორი R_06 განსაზღვრავს, რომ ადრესატი უშუალოდ აბონენტია, ამიტომ თვითონ დაუბრუნებს შეტყობინებას საწყის სახეს, ე.ი. განახორციელებს შემოსული პაკეტების მიხედვით შეტყობინების აღგენას და გადასცემს მას სააბონენტო პუნქტ $SP2$ -ს. ამით შეტყობინების გადაცემის პროცესი სრულდება.



ნახ. 2.3. პაკეტების კომუტაციის ქსელი დატვირთვებით

ამგვარად, პაკეტების გადაცემა ქსელში შეიძლება მიმდინარეობდეს ვირტუალური არხებით ან დატვირთვებით.

გადაცემის ორივე მეთოდს აქვს თავისი დადებითი და უარყოფითი მხარეები.

შევადართ ერთმანეთს ამ ორი მეთოდის ზოგიერთი მახვენებელი:

დამისამართება	<i>ვირტუალური არხებით დატაგრამებით</i>	თითოეულ პაკეტს ესაჭიროება ვირტუალური არხის მოკლე მისამართი თითოეულ პაკეტს ესაჭიროება, როგორც ადრესატის, ასევე ადრესანტის, სრული მისამართი
მარშრუტიზაცია	<i>ვირტუალური არხებით დატაგრამებით</i>	გადაცემის არხი დგინდება ერთხელ ყველა პაკეტისათვის თითოეული პაკეტისათვის გადაცემის არხი დგინდება ინდივიდუალურად
მარშრუტიზატორის გამოსვლა მწყობრიდან	<i>ვირტუალური არხებით დატაგრამებით</i>	ყველა არხი, რომელიც ამ დროს მოცემული მარშრუტიზატორის გავლით მუშაობს, წყვეტს ფუნქციონირებას იკარგება რამდენიმე პაკეტი, რომელიც ამ დროს გადაიცემოდა მოცემული მარშრუტიზატორის გავლით

ამ მაჩვენებლებს გარდა მხედველობაში მისაღებია ის გარემოება, რომ:

1. ვირტუალური არხებით გადაცემა არხების შეერთების განსახორციელებლად და შესაბამისი მისამართის დასამუშავებლად გარკვეულ დროს მოითხოვს. ამის შემდეგ კი პაკეტების გადაცემა უფრო სწრაფად მიმდინარეობს ვიდრე დატაგრამების მეთოდის გამოყენების დროს;

2. თუ სამომხმარებლო პაკეტები მცირე ზომებისაა, მაშინ დამისამართების წილი პაკეტში დატაგრამების მეთოდის გამოყენების დროს მნიშვნელოვანია და ამით მთელი არხის გამტარუნარიანობა მცირდება.

დასკვნის სახით უნდა აღვნიშნოთ, რომ ზოგადად უპირატესობის მინიჭება არც ვირტუალური არხებით გადაცემისათვის და არც დატაგრამებით გადაცემისათვის არ შეიძლება. კონკრეტული ქსელის რეალიზების პროცესში განხილულ უნდა იქნეს შეტყობინებათა გადაცემის ყველა ასპექტი და შესაბამისად შეირჩეს გადაცემის მისაღები მეთოდი.

2.2. მარშრუტიზაციის ალგორითმები

2.2.1. ზოგადი მიმოხილვა

გლობალურ კომპიუტერულ ქსელებში შეტყობინების გადაცემა ერთი სააბონენტო პუნქტიდან მეორე სააბონენტო პუნქტამდე, მაშინ როდესაც ეს პუნქტები დიდი მანძილით არიან ერთმანეთისაგან დაშორებული, მოითხოვს ქსელის რესურსების მნიშვნელოვანი ნაწილის გამოყენებას. ეს პროცესი რაციონალური გზით უნდა წარიმართოს, რათა ეფექტურად იქნეს გამოყენებული ქსელის შესაძლებლობები. ქსელში შეტყობინების გადაცემა გულისხმობს მარშრუტიზატორების გარკვეული მწკრივით მათი გადაადგილების პროცესს.

ამ მიზნის მისაღწევად ქსელში განთავსებულია მარშრუტიზატორების ერთობლიობა, შექმნილია მათი სრული ტოპოლოგიური სურათი და არსებობს იმის შესაძლებლობა, რომ შეირჩეს შეტყობინების გადაცემის ოპტიმალური გზა. ამიტომ დამუშავებულია ქსელში მარშრუტიზაციის მრავალი ალგორითმი.

ალგორითმი (ფრანგულ-არაბულ-ბერძნული) რაიმე ამოცანის ამოსახსნელად საჭირო მათემატიკურ მოქმედებათა ერთობლიობაა.

ალგორითმი ტელეკომუნიკაციური ქსელით ინფორმაციის გადაცემასთან დაკავშირებით იმ პროცესებისა და პროცედურების ერთობლიობაა, რომელიც უზრუნველყოფს შეტყობინების ეფექტურ გადაცემას ქსელის აბონენტებს შორის.

პროცესი (ლათ) - რაიმე მოვლენათა თანამიმდევრობითი მონაცვლეობაა;

პროცედურა (ფრანგ) – რისამე შესასრულებლად საჭირო მოქმედებათა, ღონისძიებათა თანამიმდევრობაა.

ნებისმიერი გლობალური ქსელისათვის უნდა შეირჩეს სათანადო ალგორითმი ან ალგორითმთა ერთობლიობა, რომელთა მკაცრი დაცვით წარიმართება მარშრუტიზატორების ფუნქციონირება.

მარშრუტიზაციის პროცესი ორი ეტაპისაგან შედგება: ერთი გადაცემის გარკვეული მარშრუტის დადგენაა, მეორე კი უშუალოდ პაკეტების გადაცემაა, რომელსაც *გადაგზავნას* უწოდებენ.

ამგვარად, ქსელის ფუნქციონირება შეიძლება განხილულ იქნეს როგორც ორი პროცესის ერთობლიობა: პირველი, როცა ხორციელდება მარშრუტიზაციის ცხრილების შედგენა და შემდგომი განახლება და მეორე, როცა ამ ცხრილების მონაცემებზე დაფუძნებით, მარშრუტიზატორები ახორციელებენ შეტყობინების გადაცემას. სწორედ ამ დროს იწყებენ თავის როლის თამაშს მარშრუტიზაციის ალგორითმები.

აქ ხაზი უნდა გაესვას ერთ გარემოებას, როდესაც განიხილება მარშრუტიზაციის ალგორითმები, არ აქვს მნიშვნელობა, იძებნება მარშრუტი ცაკეული პაკეტისათვის (ე.ი. გამოყენებულია დატაგრამების მეთოდი), თუ ერთი

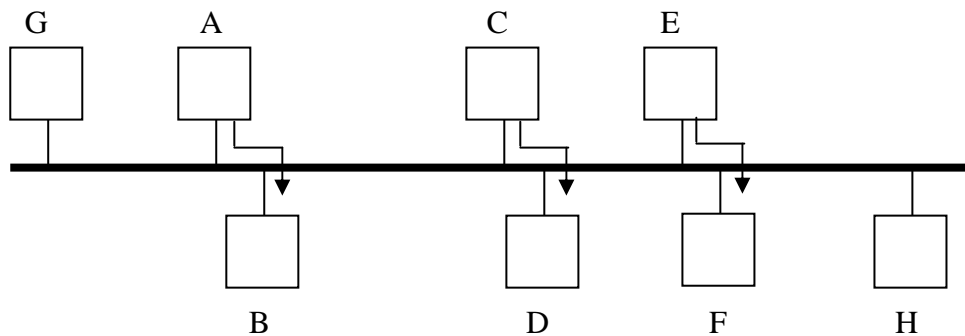
საერთო შეერთებისათვის (ე.ი. გამოყენებულია ვირტუალური არხების მეთოდი) იგი უნდა წარიმართოს ერთგვარი პირობების დაცვით.

მარშრუტის არჩევის ალგორითმი უნდა ხასიათდებოდეს გარკვეული თვისებებით: კორექტულობით, ანუ სისწორით, სიმარტივით, საიმედოობით და სამართლიანობით.

მოთხოვნა კორექტულობისა და სიმარტივის შესახებ ახსნას არ მოითხოვს.

საიმედოობასთან დაკავშირებით უნდა აღინიშნოს, რომ დიდი ქსელების ფუნქციონირების დროს განუწყვეტლივ აქვს ადგილი ამა თუ იმ აპარატურის მტყუნებას და ამასთან დაკავშირებით ქსელის ტოპოლოგიისა და ქსელში ტრაფიკის ცვლილებას. მარშრუტიზაციის ალგორითმმა უნდა შეძლოს შეტყობინებათა გადაცემის პროცესის მორგება ცვალებად ტოპოლოგიასთან და ტრაფიკთან, ისე რომ არ მოითხოვოს გადაცემის პროცესების დაწყება ყოველგვარი შეფერხებების დროს.

მოთხოვნა სამართლიანობის შესახებ განვიხილოთ კონკრეტულ მაგალითზე. ნახაზზე 2.4 წარმოდგენილია ქსელის სათანადო ფრაგმენტი.



ნახ. 2.4. სამართლიანობის საილუსტრაციო ქსელის ფრაგმენტი

დაუშვათ აქ მოცემულ A და B, C და D, E და F სადგურებს შორის ტრაფიკი იმდენად ინტენსიურია, სალტე ყოველთვის გაჯერებულია და ვერ ხერხდება G და H სადგურების ურთიერთდაკავშირება. ასეთ შემთხვევაში მარშრუტიზაციის ალგორითმისაგან მოითხოვება ტრაფიკის სამართლიანი გადანაწილება სადგურებს შორის ისე, რომ G და H სადგურებსაც მიეცეთ ურთიერთდაკავშირების საშუალება.

მარშრუტიზაციის ალგორითმის დამუშავების თუ შერჩევის დროს წინასწარ გადასაწყვეტია ქსელის რომელი პარამეტრის მიმართ განხორციელდეს ოპტიმიზაცია. ასეთი პარამეტრები კი შეიძლება იყოს ქსელში შეტყობინების დაყოვნების დროის მინიმიზაცია, ქსელის საერთო გამტარუნარიანობის გაზრდა და სხვა.

მარშრუტის არჩევის ალგორითმები ორ ძირითად კლასად იყოფა: *ადაპტური* და *არაადაპტური*.

არაადაპტური ალგორითმები მარშრუტის არჩევის დროს არ ითვალისწინებენ ქსელის მიმდინარე მდგომარეობას, ე.ი. რეალურ ტოპოლოგიას და ტრაფიკის

მახასიათებლებს მოცემული მომენტისათვის. ამ შემთხვევაში წინასწარ საერთო ტოპოლოგიური სურათით დგინდება მარშრუტი ქსელის ნებისმიერ ორ აბონენტს შორის. ეს მაჩვენებლები შეიტანება მარშრუტიზატორის მარშრუტთა სიაში და შემდეგ ხორციელდება მკაცრად ამ სახით მისი რეალიზება.

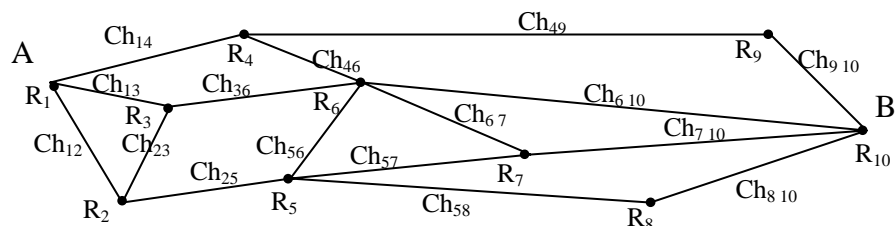
მარშრუტიზაციის ასეთ პროცედურას *სტატიკურ მარშრუტიზაციას* უწოდებენ.

ადაპტური ალგორითმები მარშრუტის არჩევის დროს ითვალისწინებენ ქსელის მიმდინარე მდგომარეობას, ე.ი. რეალურ ტოპოლოგიას და ტრაფიკის მახასიათებლებს მოცემული მომენტისათვის. ამის მიღწევა ხორციელდება ქსელის მდგომარეობის შესახებ ინფორმაციის უწყვეტ რეჟიმში მიღებით და ამ ინფორმაციაზე მყისიერი რეაგირებით. ეს პროცესები რთულია და რეალიზებისათვის ქსელის მნიშვნელოვან რესურსებს მოითხოვს, მაგრამ მისი წარმატებით ორგანიზება ქსელის ეფექტური ფუნქციონირების გარანტიაა.

მარშრუტიზაციის ასეთ პროცედურას *დინამიურ მარშრუტიზაციას* უწოდებენ.

2.2.2. მარშრუტიზაცია და გრაფთა თეორია

გრაფთა თეორია დისკრეტული მათემატიკის დარგია, რომელიც ობიექტებს შეისწავლის გეომეტრიული მიდგომით. თეორიის ძირითადი ცნებებია გრაფი, რომელიც წვეროების და წიბოების სიმრავლით წარმოდგება (ნახ. 2.5).



ნახ. 2.5. გრაფი

ეს სახელწოდება მიღებულია ბერძნული სიტყვისაგან „გრაფა“ (graphe ხაზი) – მანძილი, შუალედი ორ ხაზს შორის.

გრაფთა თეორია საშუალებას იძლევა მოიძებნოს წვეროების დამაკავშირებელი წიბოების ოპტიმალური რიგი. მაგალითად, უმოკლესი გზა A და B წვეროებს შორის.

კომპიუტერულ ქსელებში გრაფთა თეორიის საფუძველზე შეიძლება დადგინდეს საკომუტაციო ცენტრებს შორის უმოკლესი გზა, ანუ გადაწყდეს ქსელში ოპტიმალური მარშრუტიზაციის ამოცანა. იგი ასე შეიძლება წარმოვადგინოთ:

გვაქვს გრაფი $T(R,Ch)$, სადაც:

T - გრაფია, ტელეკომუნიკაციის ამოცანაში ქსელის ტოპოლოგია (Topos);

R - წვეროებია, ტელეკომუნიკაციის ამოცანაში მარშრუტიზატორები (Router);

Ch-წიბოებია, ტელეკომუნიკაციის ამოცანაში კავშირის არხები (Chenel).

გრაფისათვის (T) უნდა გადაწყდეს მარშრუტიზატორების (R) დაკავშირების უმოკლესი გზების მოძებნის ამოცანა არსებული წიბოების (Ch) პირობებში.

ამ მიზნით კომპიუტერული ქსელებისათვის შემუშავებულია რამდენიმე ალგორითმი, რომლებიც ცნობილი არიან მარშრუტიზაციის ალგორითმების სახელით. ასეთია, მაგალითად ედვინ დეიქსტრას (Edwin Dijkstra) ალგორითმი.

2.3. სტატიკური მარშრუტიზაციის ალგორითმები

2.3.1. უმოკლესი გზების მოძებნა ე. დეიქსტრას ალგორითმით

ქსელში აბონენტებს შორის უმოკლესი, ოპტიმალური გზების მოძებნის რამდენიმე ალგორითმია ცნობილი, მათ შორის ედვინ დეიქსტრას (Edwin Dijkstra) ალგორითმი, რომელსაც აქ განვიხილავთ.

სანამ უშუალოდ ამ ალგორითმის განხილვას შეუდგებოდეთ, ავლნიშნოთ, რომ ოპტიმალური გზა მრავალი მაჩვენებლის მიხედვით შეიძლება განისაზღვროს. ასეთი მაჩვენებელი შეიძლება იყოს უშუალოდ ფიზიკური მანძილი, სატრანზიტო კვანძების რიცხვი, შეტყობინების გადაგზავნის დრო, გადაგზავნის ტარიფი და სხვა. თითოეული ეს მაჩვენებელი და მათი კომბინაცია შეიძლება წარმოადგენდეს ოპტიმიზაციის კრიტერიუმს.

აქ განხილულ იქნება ე. დეიქსტრას ალგორითმი ქსელის მარშრუტიზატორებს შორის ფიზიკური მანძილის ოპტიმიზაციის კრიტერიუმით. ასეთი არჩევა არ არღვევს მეთოდის ზოგად სახეს და მარტივად შეიძლება ყველა სხვა კრიტერიუმზე გადასვლა. ფიზიკური მანძილის ოპტიმიზაციის კრიტერიუმად არჩევა მოხერხებულია მისი სიმარტივისა და თვალსაჩინოების გამო.

ე. დეიქსტრას ალგორითმის განხილვის დროს ამოცანა ზოგადად ასე დგება: გვაქვს გრაფი $T(R,Ch)$ და ნაპოვნი უნდა იქნეს მინიმალური მანძილები ნებისმიერი წვეროდან ყველა სხვა წვერომდე. ამ ამოცანის გადაწყვეტა მიმდინარეობს თანმიმდევრობით, ნაბიჯ-ნაბიჯ გრაფის წვეროების მოვლით.

ტელეკომუნიკაციის ამოცანების გადაწყვეტის პირობებში ამ პროცესს ძებნის საფეხურები ვუწოდოთ. ძებნის პირველ საფეხურზე დგინდება მანძილები საწყისი წვეროს მეზობელ წვეროებამდე. ნებისმიერი წვეროსათვის მეზობლად ითვლება წვერო, რომელთანაც ის დაკავშირებულია წიბოთი. წვეროების მოვლის დროს ხდება მათი მონიშვნა მანძილის მიხედვით ძებნის საწყისი წვეროს მიმართ. ძებნის ყველა საფეხურზე დგინდება წვერო, რომელიც ამ საფეხურისათვის უმოკლესი მანძილითაა დაშორებული საწყისი წვეროდან. შემდეგ დგინდება უკვე ამ წვეროს მეზობელი წვეროები და ა. შ. ძებნის ყველა საფეხურზე ერთმანეთს ედარება განსახილველი

წვეროს არსებული მონიშვნა, ე.ი. მანძილის მაჩვენებელი თუ ის მას გააჩნია, და ძებნის ამ საფეხურზე მიღებული მანძილის მაჩვენებელი. თუ წვეროს არსებული მონიშვნა უფრო მცირეა, ვიდრე ახალი შედეგი, მაშინ რჩება არსებული მონიშვნა; თუ კი წვეროს არსებული მონიშვნა უფრო მეტია, ვიდრე ახალი შედეგი, მაშინ წვეროს ეცვლება არსებული მონიშვნა და ხელახლა მონიშნება. ეს იმის მაჩვენებელია, რომ ნაპოვნია საწყისი წვეროდან მოცემულ წვერომდე უფრო მოკლე გზა.

ეს პროცესი გრძელდება მანამ, სანამ ძებნის საფეხურებით მოვლილი არ იქნება გრაფის ყველა წვერო, ანუ არ დადგინდება მინიმალური მანძილები საწყისი წვეროდან ყველა სხვა წვერომდე, არ განისაზღვრება უმოკლესი, ოპტიმალური გზები.

განვიხილოთ კონკრეტულ მაგალითზე ე. დეიქსტრას ალგორითმის რეალიზების პროცესი. ამ მიზნით ავიღოთ მაგალითად ქსელის ნახაზ 2.1 წარმოდგენილი ფრაგმენტი გამარტივებული სახით (ნახ. 2.6).

მოცემულ ფრაგმენტზე მოცემულია ქსელი K-შეერთების ტოპოლოგიით. საკომპუტაციო ცენტრები ნახაზზე წარმოდგენილია მარშრუტიზატორების სახით, როგორც ძირითადი კომპონენტები ოპტიმალური გზების დადგენის პროცესში.

ქსელის ეს ფრაგმენტი შეიძლება განხილულ იქნეს, როგორც გრაფი $T(7,13)$, ე.ი. გრაფი 7 წვეროთი და 13 წიბოთი.

უმოკლესი, ოპტიმალური გზების ძებნის პირველი ნაბიჯია დადგინდეს თუ რომელი წვეროს მიმართ უნდა განისაზღვროს მანძილები, ანუ მოხდეს საწყისი წვეროს სახელდება. აქედან გამომდინარე, საწყისად მივიღოთ R1 წვერო.

ძებნის დაწყების წინ მიღებულია გრაფი ასე მონიშნოს: საწყისი წვერო „0“, ხოლო ყველა სხვა წვერო „X“. ეს მიუთითებს, რომ ჯერ ძებნა არ დაწყებულა.

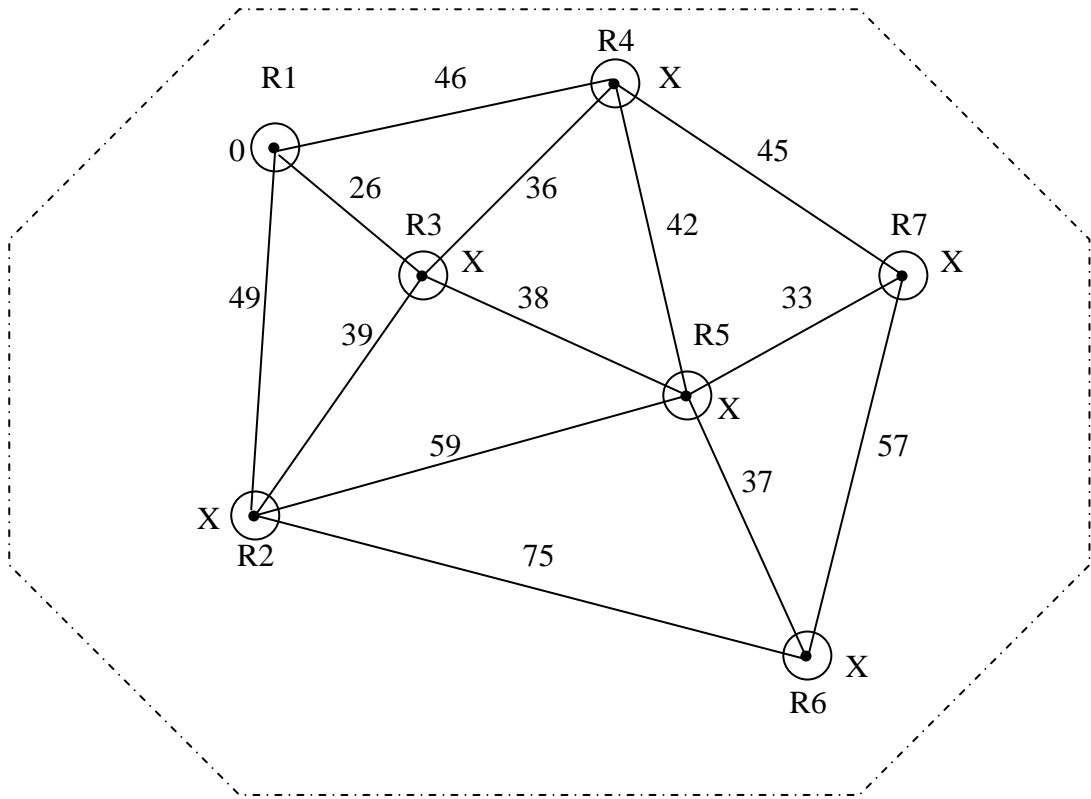
შემდგომ ძებნის საფეხურების შედეგების მიხედვით იცვლება წვეროების მონიშვნები და ეს პროცესი სრულდება, როდესაც ძებნის საფეხურები შეეხება ყველა წვეროს.

მანამ, სანამ ნაჩვენები იქნება დეიქსტრას ალგორითმის შესრულების პროცესი უნდა დადგინდეს მანძილები წვეროებს შორის, ანუ წიბოთა სიგრძეები. პირობითად მივიღოთ, რომ წიბოებისათვის მასშტაბია 1 მმ – 1 კმ.

ეს მონაცემები წარმოდგენილია ნახაზზე 2.6.

ძებნის I საფეხური

წვერო R1 მონიშნულია „0“, ე.ი. იგი წარმოადგენს წვეროს, რომლის მიმართაც უნდა დადგინდეს უმოკლესი მანძილები. ამიტომ წვერო R1 –ის მონიშვნა შევცვალოთ ახლით - r_0 .



ნახ. 2.6. ქსელის ფრაგმენტი $T(7,13)$ გრაფის სახით
საწყისი მდგომარეობა

ვიპოვოთ $r_0(R1)$ -ის მეზობელი წვეროები და დავალაგოთ დაშორების მიხედვით. ასეთებია R3, R4, R2.

წვეროდან $r_0(R1)$ მეზობელ წვეროებამდე ასეთი მანძილებია (კმ):

R3-მდე 26;

R4-მდე 46;

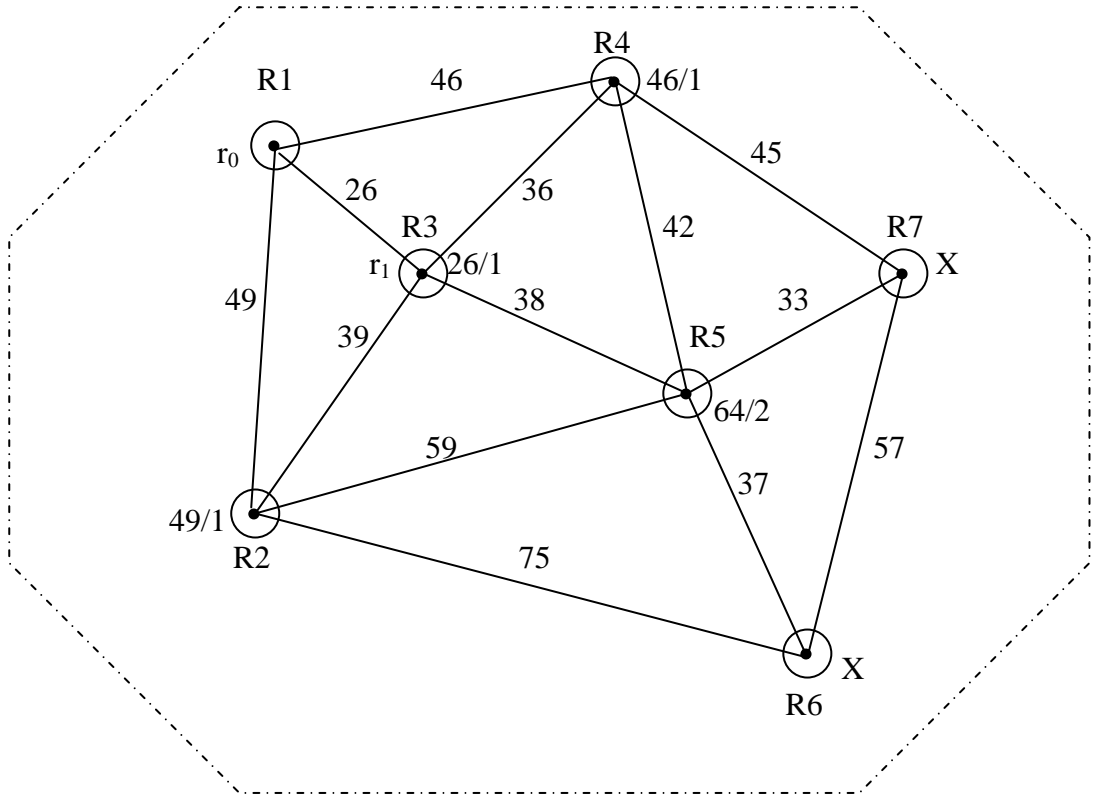
R2-მდე 49.

ძეზნის I საფეხურის შედეგები დაეიტანოთ ნახაზზე, ანუ ნიშნულები X შეეცვალოთ შესაბამისი სიდიდეებით. ნახაზზე 8.5/1 ისინი ნაჩვენებია, როგორც ახალი ნიშნულები. (ნიშნული, მაგალითად, 46/1 გეიჩვენებს, რომ 46კმ-ია საწყისი, $r_0(R1)$ წვეროდან და რომ იგი დადგენილია ძეზნის I საფეხურზე).

ძეზნის I საფეხურზე ვადგენთ, რომ წვეროდან $r_0(R1)$ უახლოესია R3 წვერო. იგი მოვნიშნოთ, როგორც $r_1(R3)$.

ძეზნის II საფეხური

ვიპოვოთ $r_1(R3)$ -ის მეზობელი წვეროები და დავალაგოთ დაშორების მიხედვით. ასეთებია R1 (თვით საწყისი წვერო, რომელიც აქ აღარ განიხილება), R4, R5, R2.



ნახ. 2.6/1. ქსელის ფრაგმენტი $T(7,13)$ გრაფის სახით
 მდგომარეობა ძებნის I და II საფეხურის შემდეგ

$r_0(R1)$ წვეროდან $r_1(R3)$ -ის მეზობელი წვეროებამდე ასეთი მანძილებია (კმ):

R4-მდე $26 + 36 = 62$;

R5-მდე $26 + 38 = 64$;

R2-მდე $26 + 39 = 65$.

მიღებული შედეგები უნდა შეფასდეს:

წვერო R4 მონიშნულია, როგორც 46/1, ახალი შედეგი 62-ია. ეს ნიშნავს, რომ წვერო R4-მდე უფრო მოკლე მანძილი ნაპოვნი არ არის და უნდა დარჩეს არსებული ნიშნული;

ასევე, წვერო R2 მონიშნულია, როგორც 49/1, ახალი შედეგი 65-ია. ეს ნიშნავს, რომ წვერო R2-მდე უფრო მოკლე მანძილი ნაპოვნი არ არის და უნდა დარჩეს არსებული ნიშნული;

წვერო R5 მონიშნულია, როგორც X, ამიტომ ვსვამთ მიღებულ შედეგს 64/2.

ნახაზზე 8.5/1 ნაჩვენებია მდგომარეობა ძებნის I და II საფეხურის შემდეგ.

ძებნის III საფეხური

ძებნის III საფეხურის წინ უნდა შეირჩეს მორიგი წვერო. ამ მიზნით ერთმანეთს უნდა შეედაროს ყველა ნიშანდებული წვერო, რომლის მოვლაც არ შემდგარა.

მოცემული მომენტისათვის, ანუ ძეხვის III საფეხურის წინ, ასეთი წვეროებია: R4 ნიშნულით 46/1, R2 ნიშნულით 49/1 და R5 ნიშნულით 64/2,

ამ წვეროებიდან უმცირესი ნიშნული გააჩნია წვეროს R4 - 46/1, ამიტომ მივიღოთ R4 ძეხვის III საფეხურის მორიგ წვეროდ და მოვნიშნოთ, როგორც r_2 .

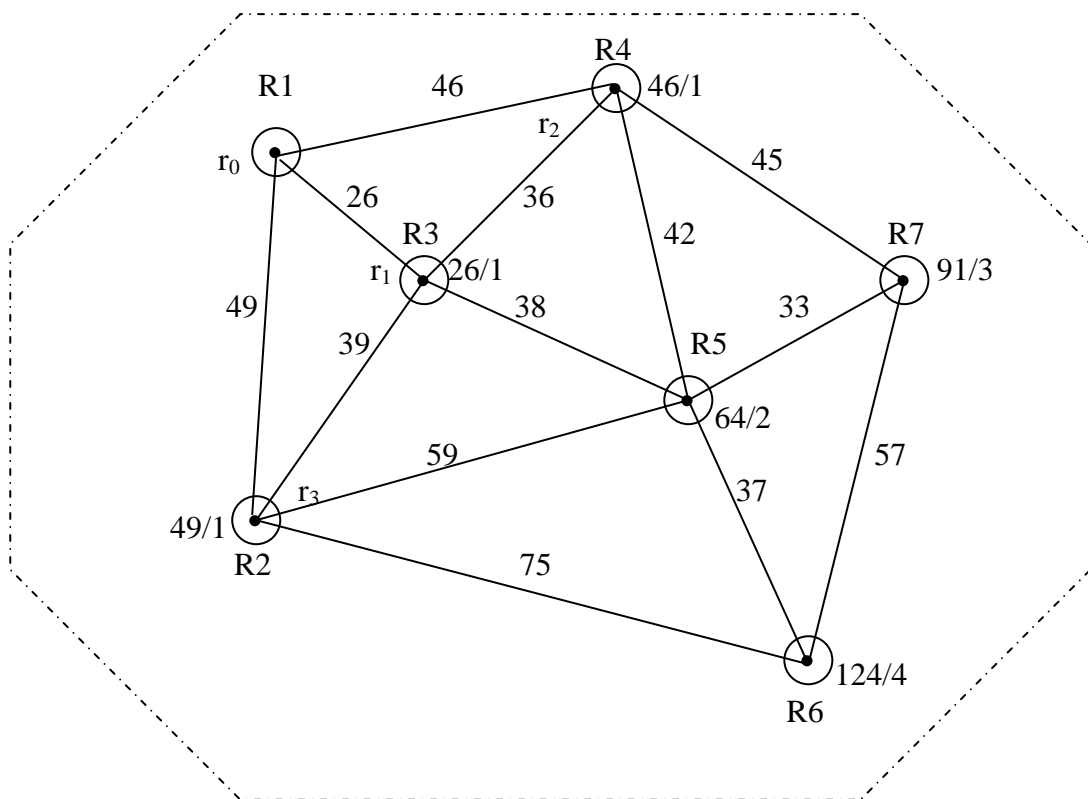
ვიპოვოთ $r_2(R4)$ -ის მეზობელი წვეროები და დავაღაგოთ დაშორების მისედვით. ასეთებია R1 (თვით საწყისი წვერო, რომელიც აქ აღარ განიხილება), R3, R5, R7.

$r_0(R1)$ წვეროდან $r_2(R4)$ -ის მეზობელ წვეროებამდე ასეთი მანძილებია (კმ):

R3-მდე დადგენილია, 26/1;

R5-მდე $46 + 42 = 88$;

R7-მდე $46 + 45 = 91$.



ნახ. 2.6/2. ქსელის ფრაგმენტი $T(7,13)$ გრაფის სახით მდგომარეობა ძეხვის III და IV საფეხურის შემდეგ

მიღებული შედეგები უნდა შეფასდეს:

წვერო R5 მონიშნულია, როგორც 64/2, ახალი შედეგია 88. ეს ნიშნავს, რომ წვერო R5-მდე უფრო მოკლე მანძილი ნაპოვნი არ არის და უნდა დარჩეს არსებული ნიშნული;

წვერო R7 მონიშნულია, როგორც X, ამიტომ ვსვამთ მიღებულ შედეგს 91/3. ძეხვის IV საფეხური

ქების IV საფეხურის წინ უნდა შეირჩეს მორიგი წვერო. ამ მიზნით ერთმანეთს უნდა შეედაროს ყველა ნიშანდებული წვერო, რომლის მოვლაც არ შემდგარა.

მოცემული მომენტისათვის, ანუ ქების IV საფეხურის წინ, ასეთი წვეროებია: R2 ნიშნულით 49/1, R5 ნიშნულით 64/2 და R7 ნიშნულით 91/3.

ამ წვეროებიდან უმცირესი ნიშნული გააჩნია წვეროს R2 - 49/1, ამიტომ მივიღოთ R2 ქების IV საფეხურის მორიგ წვეროდ და მოვნიშნოთ, როგორც r_3 .

ვიპოვოთ $r_3(R2)$ -ის მეზობელი წვეროები და დავაღაგოთ დაშორების მიხედვით. ასეთებია R1 (თვით საწყისი წვერო, რომელიც აქ აღარ განიხილება), R3, R5, R6.

$r_0(R1)$ წვეროდან $r_3(R2)$ -ის მეზობელ წვეროებამდე ასეთი მანძილებია (კმ):

R3-მდე დადგენილია, 26/1;

R5-მდე $49 + 59 = 108$;

R6-მდე $49 + 75 = 124$.

მიღებული შედეგები უნდა შეფასდეს:

წვერო R5 მონიშნულია, როგორც 64/2, ახალი შედეგია 108. ეს ნიშნავს, რომ წვერო R5-მდე უფრო მოკლე მანძილი ნაპოვნი არ არის და უნდა დარჩეს არსებული ნიშნული;

წვერო R6 მონიშნულია, როგორც X, ამიტომ ვსვამთ მიღებულ შედეგს 124/4.

ნახაზზე 8.5/2 ნაჩვენებია მდგომარეობა ქების III და IV საფეხურის შემდეგ.

ქების V საფეხური

ქების V საფეხურის წინ უნდა შეირჩეს მორიგი წვერო. ამ მიზნით ერთმანეთს უნდა შეედაროს ყველა ნიშანდებული წვერო, რომლის მოვლაც არ შემდგარა.

მოცემული მომენტისათვის, ანუ ქების V საფეხურის წინ, ასეთი წვეროებია: R5 ნიშნულით 64/2, R7 ნიშნულით 91/3 და R6 ნიშნულით 124/4.

ამ წვეროებიდან უმცირესი ნიშნული გააჩნია წვეროს R5 - 64/2, ამიტომ მივიღოთ R5 ქების V საფეხურის მორიგ წვეროდ და მოვნიშნოთ, როგორც r_4 .

ვიპოვოთ $r_4(R5)$ -ის მეზობელი წვეროები და დავაღაგოთ დაშორების მიხედვით. ასეთებია R7, R6, R3, R4, R2.

$r_0(R1)$ წვეროდან $r_4(R5)$ -ის მეზობელ წვეროებამდე ასეთი მანძილებია (კმ):

R7-მდე $64 + 33 = 97$;

R6-მდე $64 + 37 = 101$;

R3-მდე დადგენილია, 26/1;

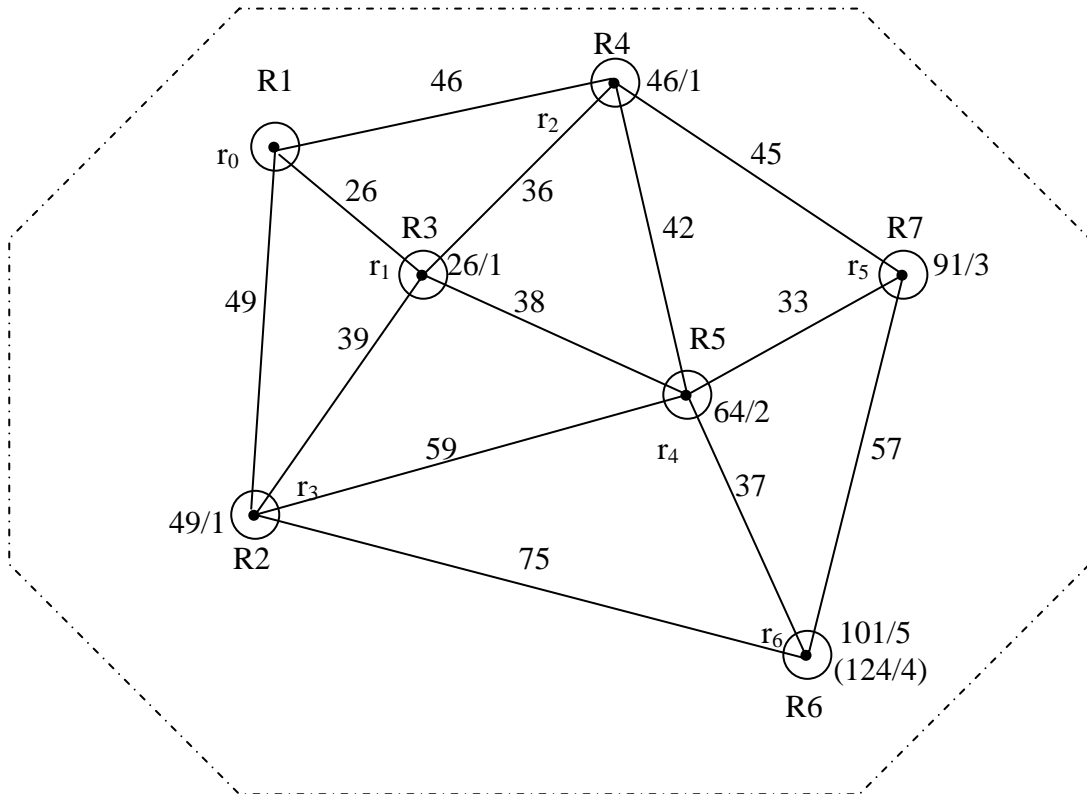
R4-მდე დადგენილია, 46/1;

R2-მდე დადგენილია, 49/1.

მიღებული შედეგები უნდა შეფასდეს:

წვერო R7 მონიშნულია, როგორც 91/3, ახალი შედეგია 97. ეს ნიშნავს, რომ წვერო R7-მდე უფრო მოკლე მანძილი ნაპოვნი არ არის და უნდა დარჩეს არსებული ნიშნული;

წვერო R6 მონიშნულია, როგორც 124/4, ახალი შედეგია 101. ეს ნიშნავს, რომ წვერო R6-მდე ნაპოვნია უფრო მოკლე მანძილი და უნდა შეიცვალოს არსებული ნიშნული 124/4, ახალით 101/5.



ნახ. 2.6/3. ქსელის ფრაგმენტი $T(7,13)$ გრაფის სახით მდგომარეობა ძეგნის V, VI და VII საფეხურის შემდეგ

ძეგნის VI საფეხური

ძეგნის VI საფეხურის წინ უნდა შეირჩეს მორიგი წვერო. ამ მიზნით ერთმანეთს უნდა შეედაროს ყველა ნიშანდებული წვერო, რომლის მოვლაც არ შემდგარა. მოცემული მომენტისათვის, ანუ ძეგნის VI საფეხურის წინ, ასეთი წვეროებია: R7 ნიშნულით 91/3 და R6 ნიშნულით 101/5.

ამ წვეროებიდან უმცირესი ნიშნული გააჩნია წვეროს R7 - 91/3, ამიტომ მივიღოთ R7 ძეგნის VI საფეხურის მორიგ წვეროდ და მოვნიშნოთ, როგორც r_5 .

ვიპოვოთ $r_5(R7)$ -ის მეზობელი წვეროები და დავაღვათ დაშორების მიხედვით. ასეთებია R5, R4, R6.

$r_0(R1)$ წვეროდან $r_5(R7)$ -ის მეზობელ წვეროებამდე ასეთი მანძილებია (კმ):

R5-მდე დადგენილია, 64/2;

R4-მდე დადგენილია, 46/1;

R6-მდე დადგენილია, 101/5.

მიღებული შედეგები უნდა შეფასდეს:

$r_0(R1)$ წვეროდან $r_5(R7)$ -ის მეზობელ წვეროებამდე ყველა მანძილია დადგენილი არავითარ ცვლილებას არ ექნება ადგილი.

დარჩენილია მოუვლელი წვერო R6, მივიღოთ იგი ძეხვის VII საფეხურის მორიგ წვეროდ და მოვნიშნოთ, როგორც r_6 .

ვიპოვოთ $r_6(R6)$ -ის მეზობელი წვეროები და დავაღაგოთ დაშორების მიხედვით. ასეთებია R5, R7, R2.

$r_0(R1)$ წვეროდან $r_6(R6)$ -ის მეზობელ წვეროებამდე ასეთი მანძილებია (კმ):

R5-მდე დადგენილია, 64/2;

R7-მდე დადგენილია, 91/3;

R2-მდე დადგენილია, 49/1.

მიღებული შედეგები უნდა შეფასდეს:

$r_0(R1)$ წვეროდან $r_6(R6)$ -ის მეზობელ წვეროებამდე ყველა მანძილია დადგენილი არავითარ ცვლილებას არ ექნება ადგილი.

ვინაიდან მოუვლელი არ არის დარჩენილი არც ერთი წვერო, ძეხვა დასრულებულია.

ნახაზზე 2.6/3 ნაჩვენებია მდგომარეობა ძეხვის V, VI და VII საფეხურის, ანუ ძეხვის დასრულების შემდეგ.

მიღებული შედეგების მიხედვით დგინდება მარშრუტიზატორ R1-ის სამარშრუტო გზები, რომლებიც მოცემულია ცხრილში 2.1.

ცხრილი 2.1.

დანიშნულების მარშრუტიზატორი	უმოკლესი გზის მარშრუტი	მანძილი (კმ)
R2	უშუალოდ R1 – R2	49
R3	უშუალოდ R1 – R3	26
R4	უშუალოდ R1 – R4	46
R5	R1 – R3 – R5	64
R6	R1 – R3 – R5 – R6	101
R7	R1 – R4 – R7	91

ანალოგიური ცხრილები იქმნება ქსელის ნებისმიერი მარშრუტიზატორისათვის.

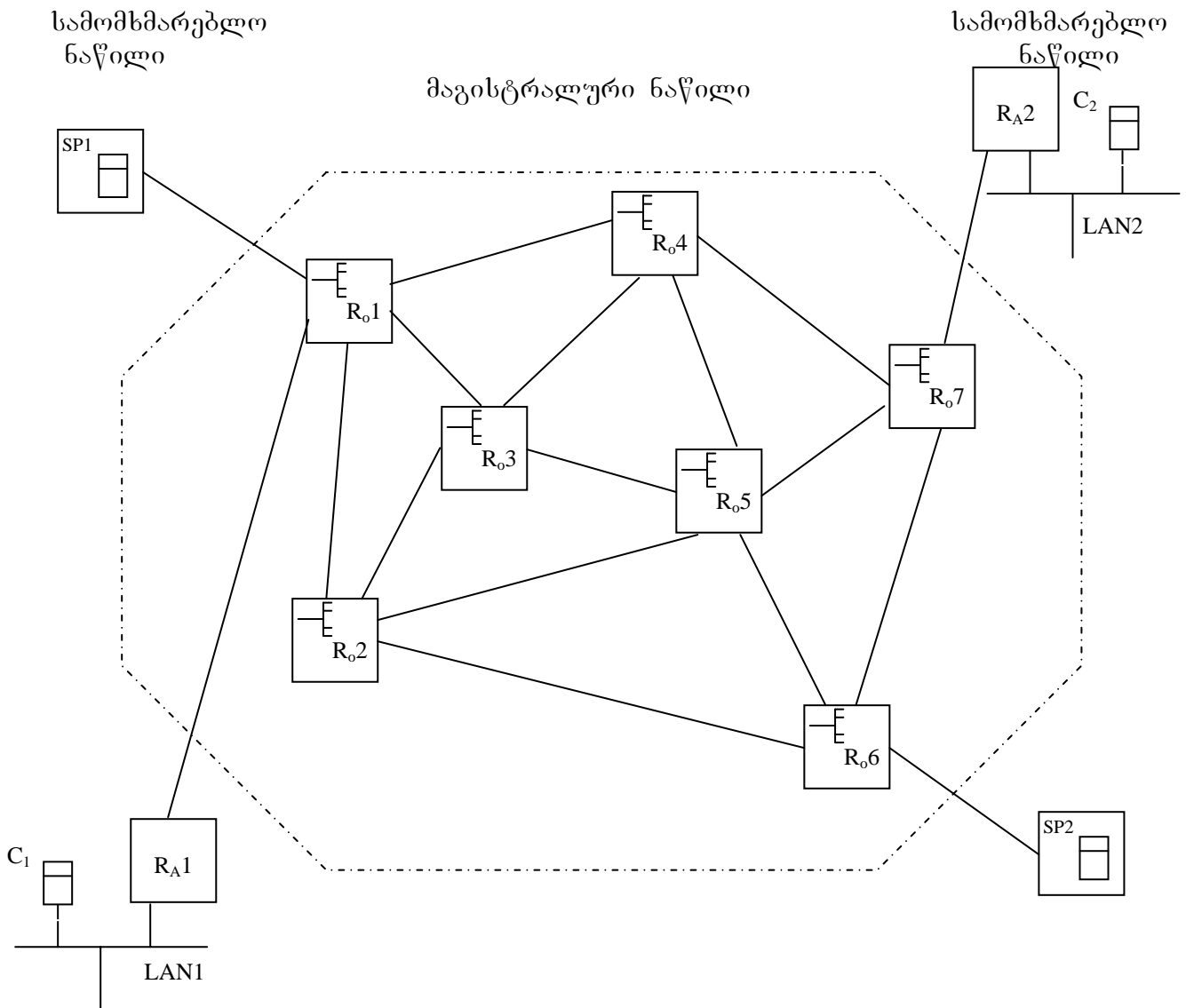
ქსელში კონკრეტული შეტყობინების შემოსვლის დროს სამისამართო ნაწილის მიხედვით განისაზღვრება უმოკლესი გზა გადამცემ და მიმღებ მარშრუტიზატორებს შორის და შეტყობინებაც ამ გზით გადაიცემა.

2.3.2. ავსება (flood)

ალგორითმის „ავსება“ ფუნქციონირება შეტყობინებათა გადაცემის ძალზე მარტივ სქემას ეფუძნება: თითოეული შემოსული პაკეტი ეგზავნება ყველა მეზობელ მარშრუტიზატორს, გარდა იმისა, ვისგანაც იგი იყო მიღებული.

ამ ალგორითმის რეალიზება ქსელში წარმოშობს პაკეტების დიდ რაოდენობას, ხოლო თუ ქსელი რთულია და შეკრული კონტურების მქონე, მათი რიცხვი უსასრულოდაც კი შეიძლება გაიზარდოს.

მაგალითისათვის ავიღოთ ნახაზ 2.1 წარმოდგენილი ქსელის ფრაგმენტი, ოდნავ სახე შეცვლილი და ვნახოთ პაკეტების გავრცელების როგორ სურათს მივიღებთ (ნახ. 2.7).



ნახ. 2.7. ტელეკომუნიკაციური ქსელის ფრაგმენტული ალგორითმ „ავსების“ ილუსტრაციისათვის

დაუშვათ, რომ ქსელში შეტყობინების წყაროა მარშრუტიზატორი R₁. ალგორითმ ავსების თანახმად იგი შესაბამის პაკეტს გაუგზავნის

მარშრუტიზატორებს R2, R3 და R4. თავის მხრივ, R2 გაუგზავნის R3, R5 და R6; R3 კი R2, R4 და R5; R4 კი R3, R5 და R7.

ამგვარად, მარშრუტიზატორი R5 ამ ალგორითმის საფუძველზე მოცემულ პაკეტს მიიღებს R2, R3 და R4 მარშრუტიზატორებისაგან.

ეხლა უკვე მარშრუტიზატორი R5 იწყებს ყველა მიმართულებით ამ პაკეტის დაგზავნას და იგი აღმოჩნდება დაბრუნებული მარშრუტიზატორებთან R2, R3 და R4. ეს მარშრუტიზატორები იწყებენ კვლავ გადაცემის ციკლს, ხოლო მარშრუტიზატორები R6 და R7 კი ებმებიან გადაცემათა ახალ ციკლში და ასე, პრაქტიკულად, დაუსრულებლად.

ამ მიზეზით, ალგორითმ „ავსების“ პრაქტიკულად რეალიზების დროს ატარებენ სპეციალურ ღონისძიებებს ქსელში მოძრავი პაკეტების რაოდენობის შესამცირებლად.

ასეთი დანიშნულების ღონისძიებების რამდენიმე ვარიანტი არსებობს.

ერთი მათგანია, მარშრუტიზატორში მოცემული პაკეტის გავლის აღრიცხვა სათანადო ნიშნის დასმით. როდესაც ამ ნიშნის მქონე პაკეტი კვლავ შემოვა მარშრუტიზატორში, იგი მის გავრცელებას შეწყვეტს, როგორც უკვე გადაცემულის და მას ამოკვეთს (წაშლის თავისთან).

ასევე შესაძლებელია პაკეტს თავიდან მიეკუთვნოს გარკვეული ნომერი (სპეციალური ამ დანიშნულებისათვის). მოცემულ მარშრუტიზატორში თუ განმეორებით შემოვიდა ადრე დაფიქსირებულ ნომრიანი პაკეტი, იგი მას აღარ გაავრცელებს და ამოკვეთს.

ეს და მსგავსი ღონისძიებები, მნიშვნელოვნად ზღუდავენ პაკეტების ტირაჟირების პროცესს ქსელში.

გარდა უშუალოდ ალგორითმ „ავსებისა“ არსებობს მისი ვარიანტი, რომელსაც *შერჩევითი ავსება* ეწოდება.

ამ შემთხვევაში მარშრუტიზატორები წინასწარ, პაკეტის მიღებისთანავე, საზღვრავენ (მისამართის მიხედვით) მისი გადაადგილების მიმართულებას. ამის შემდეგ მხოლოდ ამ მიმართულებით მდებარე მარშრუტიზატორებს გადასცემენ მას და არა ყველა მეზობელ მარშრუტიზატორს.

ასე მაგალითად, იგივე ფრაგმენტზე (ნახ. 2.1) მოყვანილი ქსელის პირობებში, მარშრუტიზატორი R5, მარშრუტიზატორ R3-დან შემოსილ პაკეტს აღარ გაავზავნის R2 და R4 მარშრუტიზატორებისაკენ.

აქ უნდა ავღნიშნოთ, რომ მოყვანილი ფრაგმენტი მარტივია და ამიტომ ალგორითმ „შერჩევით ავსების“ ეფექტი ნაკლებად თვალსაჩინოა, რთული სტრუქტურის ქსელებში კი მისი გამოყენებით მნიშვნელოვანი შედეგები მიიღება.

რეალურ გლობალურ ქსელებში სწორედ შერჩევით ავსების ალგორითმი პრაქტიკულად უფრო მეტადაა გამოყენებული.

ვეცნობით რა, ალგორითმ „ავსებას“ და მის ვარიანტს - „შერჩევით ავსებას“, ჩნდება მოსაზრება, საერთოდ რამდენად მიზანშეწონილია ასეთი ალგორითმის გამოყენება. ალგორითმის, რომელიც დაკავშირებულია პაკეტების გადაცემის პროცესების ასეთ გართულებებთან და ამდენ შეზღუდვებთან?

საქმე ის არის, რომ ალგორითმ „ავსებას“ დიდი საიმედოობა ახასიათებს და საბოლოო ვარიანტში, შეტყობინების მიტანა მომხმარებელამდე დიდი ალბათობითაა გარანტირებული.

შეტყობინების საიმედო მიტანას მომხმარებელამდე კი ზოგიერთ შემთხვევაში უდიდესი მნიშვნელობა ენიჭება, მაგალითად სამხედრო საქმეში. ეს მაშინ, როდესაც ნებისმიერ დროს მოსალოდნელია შეტყობინების გაგრძელების გზის განადგურება და, როგორც შედეგი, თუ ეს გზა ერთადერთია, შეტყობინების დაკარგვა.

ამას გარდა, ალგორითმი „ავსება“ მეტად მოხერხებულია მონაცემთა ბაზების შექმნისა და შევსების პროცესებში. ამ დროს შეტყობინებები მონაცემთა ბაზებისათვის ვრცელდება სწრაფად და იღებს ყველა, ვისთვისაც ისინი არიან დანიშნული.

არის კიდევ მესამე შემთხვევა, როდესაც ალგორითმ „ავსების“ გამოყენებაა მიზანშეწონილი. ეს არის ოპტიმალური გზების შერჩევის სხვადასხვა ალგორითმის ეტალონური ტესტირების პროცესი.

ალგორითმი „ავსება“ შეტყობინებას გადასცემს ყველა გზით და, ცხადია, მათ შორის ოპტიმალურითაც. პაკეტების სახით წარმოდგენილი შეტყობინების გადაცემის პროცესში გამოყენებული გზების შედარებითი ანალიზი აადვილებს მათ შორის ოპტიმალურის გამოვლენას.

ამგვარად, ალგორითმი „ავსება“ ყველა მისთვის დამახასიათებელი დადებითი და უარყოფითი მახვენებლების გათვალისწინებით პოულობს თავის გამოყენების სივრცეს კომპიუტერულ ქსელებში.

2.4. დინამიური მარშრუტიზაციის ალგორითმები

2.4.1. მარშრუტიზაცია მანძილის ვექტორის მიხედვით

მარშრუტიზაცია მანძილის ვექტორის მიხედვით წარმოადგენს დინამიური მარშრუტიზაციის ალგორითმების ერთერთ სახეს. ალგორითმები მანძილის ვექტორის მიხედვით მუშაობენ სპეციალური ცხრილების საფუძველზე. ამ ცხრილებს ვექტორებს უწოდებენ. ეს ცხრილები, ანუ ვექტორები, შეიცავენ ყველა ცნობილ გზას მოცემული მარშრუტიზატორიდან ნებისმიერ შესაძლო ადრესატამდე (მიმღებამდე).

ამ ცხრილების ორგანიზებასა და მის შემდგომ შევსებას ახორციელებს (მხარსუჭერს) ქსელის ყველა მარშრუტიზატორი. ქსელის ფუნქციონირების პროცესში მარშრუტიზატორები მუდმივად ცვლიან ერთმანეთს შორის სათანადო ინფორმაციას და უზრუნველყოფენ ცხრილების მონაცემების მუდმივ განახლებას.

ალგორითმებს, მანძილის ვექტორის მიხედვით, ხშირად მოიხსენიებენ ავტორების, ბელმან – ფორდ – ფულკერსონის (Bellman – Ford - Fulkerson) სახელითაც.

ალგორითმის, მარშრუტიზაცია მანძილის ვექტორის მიხედვით, კრიტერიუმად შეიძლება მიღებულ იქნეს უშუალოდ მანძილი, ვთქვათ, კილომეტრებში, პაკეტების გადაგზავნის დრო ქსელის ამა თუ იმ მონაკვეთზე, შეტყობინებათა მიერ გავლილ შუალედურ მარშრუტიზატორთა რიცხვი და სხვა.

თუ კრიტერიუმად მანძილია მიღებული, მაშინ მარშრუტიზატორებს გააჩნიათ სრული ინფორმაცია მანძილების შესახებ მეზობელ მარშრუტიზატორებს შორის. ამ მონაცემებზე დაყრდნობით ხორციელდება ოპტიმალური გზების შერჩევა.

თუ კრიტერიუმად პაკეტების გადაგზავნის დროა მიღებული, მაშინ ნებისმიერი მარშრუტიზატორი თავის მეზობლებთან აგზავნის სპეციალურ პაკეტს, რომელსაც ECHO (ეჰო)-ს უწოდებენ. ეს პაკეტი, მივა რა დანიშნულების ადგილზე, მოინიშნება გადაგზავნისთვის დახარჯული დროითი მაჩვენებლით და სასწრაფოდ უბრუნდება გამგზავნს (თითქოს და სრულდება ეჰოს პროცესი).

ქსელში სხვა კრიტერიუმების გამოყენების შემთხვევებში ასევეა გათვალისწინებული მათი რეალიზების გზები.

ალგორითმის, მარშრუტიზაცია მანძილის ვექტორის მიხედვით, მოქმედების თვალსაჩინოებისათვის წარმოვადგინოთ ქსელის ფრაგმენტი (ნახ. 2.8).

ალგორითმის, მარშრუტიზაცია მანძილის ვექტორის მიხედვით, გამოყენებისას ძირითადად კრიტერიუმი - პაკეტების გადაგზავნის დრო – გამოიყენება.

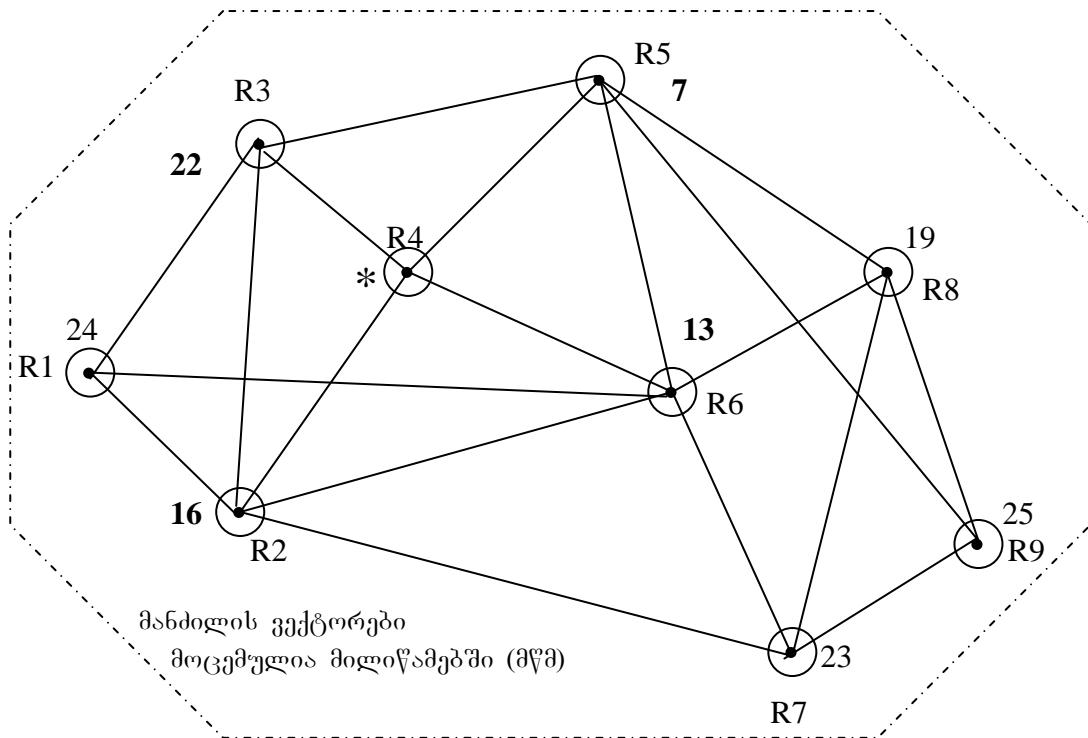
ამ შემთხვევაში მარშრუტიზატორები გარკვეული, წინასწარ დადგენილი, T პერიოდით, უგზავნიან მეზობლებს ECHO (ეჰო) პაკეტებს, თვითონაც იღებენ მეზობლებისაგან მათ და ქმნიან წინა პირობას სათანადო ცხრილების შესაქმნელად ან გასახლებლად.

ალგორითმის, მარშრუტიზაცია მანძილის ვექტორის მიხედვით, რეალიზებისას გადაგზავნის დროით ერთეულად, ჩვეულებრივად, მიღებულია მილიწამი (მწმ).

მოცემული ფრაგმენტის მიმართ უუჩვენოთ ქსელში მიმდინარე პროცესები.

ალგორითმის მოქმედება განვიხილოთ მარშრუტიზატორ R4-ის მიმართ და იგი მოვნიშნოთ ნიშნაკით *. მარშრუტიზატორ R4-ის მეზობელი მარშრუტიზატორებია R2, R3, R5 და R6.

მოცემული მარშრუტიზატორისათვის მეზობელია ყველა ის მარშრუტიზატორი, რომელთანაც მას უშუალო კავშირი აქვს.



ნახ. 2.8. ალგორითმის, მარშრუტიზაცია მანძილის ვექტორის მიხედვით, ილუსტრაციისათვის

დაუშვათ მოცემულ მომენტში მარშრუტიზატორმა R4 ECHO (ეჭო) პაკეტების საშუალებით დაადგინა შეტყობინების გადაგზავნის დრო ყველა მეზობელ მარშრუტიზატორამდე და ასეთი შედეგები მიიღო:

R2-მდე – 16 მწმ, R3-მდე – 22 მწმ, R5-მდე – 7 მწმ და R6-მდე – 13 მწმ.

ამავე დროს მარშრუტიზატორმა R4 მეზობლებისაგან მიიღო ინფორმაცია თუ როგორია მათთვის გადაგზავნის დრო ქსელის ყველა სხვა მარშრუტიზატორამდე.

მოცემული მარშრუტიზატორის მიერ მეზობელი მარშრუტიზატორისაგან მიღებულ მონაცემებს, დაკავშირებულს შეტყობინების გადაგზავნის დროსთან, პირობითად მანძილის ვექტორი ეწოდება.

მარშრუტიზატორი R4 მეზობლებისაგან მიღებულ ინფორმაციას შეიტანს თავის სამოქმედო ცხრილში (ცხრილი 2.2).

ცხრილი 2.2

მეზობ მარშ ქს მარშ	R2	R3	R5	R6	R4	სატრანზიტო მარშრუტიზატორი
R1	8	10	21	12	24	R2
R2	0	9	27	11	16	-
R3	11	0	8	14	22	-
R4	15	20	7	15	0	0
R5	25	17	0	6	7	-
R6	18	23	9	0	13	-
R7	22	38	22	10	23	R6
R8	32	32	12	8	19	R5
R9	34	42	18	22	25	R5

ცხრილში მოცემული შედეგების ანალიზის დროს ყურადღება უნდა მიექცეს ერთ ფაქტს: შეტყობინების გადაგზავნის დრო, ვთქვათ, A პუნქტიდან B პუნქტში და, პირიქით, B პუნქტიდან A პუნქტში ძირითადად ერთმანეთისაგან განსხვავებულია, რაც შეესაბამება რეალურ სიტუაციებს.

ამავე ცხრილში (მეორე ნაწილი) მარშრუტიზატორ R4-ის მიერ შეტანილ იქნება მის მიერ ECHO პაკეტით დადგენილი გადაგზავნების დრო მეზობლებამდე (ნაჩვენებია მსხვილად) და მის მიერ ნაანგარიშები გადაგზავნების ოპტიმალური დროის მაჩვენებლები დანარჩენ მარშრუტიზატორებამდე. აქვეა მოცემული იმ სატრანზიტო მარშრუტიზატორების ნომრები, რომელთა გავლითაც ხდება გადაგზავნების ოპტიმალური დროის რეალიზება.

I. გადაგზავნის ოპტიმალური დროის დადგენა მარშრუტიზატორ R1-მდე.

მარშრუტიზატორ R1-მდე შეტყობინების გადაგზავნის შესაძლო გზებია:

1. R4 – R2 – R1 შეტყობინების გადაგზავნის დროით (მწმ) $16 + 8 = 24$
2. R4 – R3 – R1 შეტყობინების გადაგზავნის დროით (მწმ) $22 + 10 = 32$
3. R4 – R5 – R1 შეტყობინების გადაგზავნის დროით (მწმ) $7 + 21 = 28$
4. R4 – R6 – R1 შეტყობინების გადაგზავნის დროით (მწმ) $13 + 12 = 25$

მიღებული შედეგების მიხედვით მარშრუტიზატორ R4-დან მარშრუტიზატორ R1-მდე შეტყობინების გადაგზავნის ოპტიმალური გზა დროის მიხედვით გადის მარშრუტიზატორ R2-ზე და იგი შეადგენს 24მწმ. ეს შედეგი შეტანილია ცხრილში.

II. გადაგზავნის ოპტიმალური დროის დადგენა მარშრუტიზატორ R7-მდე.

მარშრუტიზატორ R7-მდე შეტყობინების გადაგზავნის შესაძლო გზებია:

1. R4 – R2 – R7 შეტყობინების გადაგზავნის დროით (მწმ) $16 + 22 = 38$
2. R4 – R3 – R7 შეტყობინების გადაგზავნის დროით (მწმ) $22 + 38 = 60$

3. R4 – R5 – R7 შეტყობინების გადაგზავნის დროით (მწმ) $7 + 22 = 29$

4. R4 – R6 – R7 შეტყობინების გადაგზავნის დროით (მწმ) $13 + 10 = 23$

მიღებული შედეგების მიხედვით მარშრუტიზატორ R4-დან მარშრუტიზატორ R7-მდე შეტყობინების გადაგზავნის ოპტიმალური გზა დროის მიხედვით გადის მარშრუტიზატორ R6-ზე და იგი შეადგენს 23მწმ. ეს შედეგი შეტანილია ცხრილში.

III. გადაგზავნის ოპტიმალური დროის დადგენა მარშრუტიზატორ R8-მდე.

მარშრუტიზატორ R8-მდე შეტყობინების გადაგზავნის შესაძლო გზებია:

1. R4 – R2 – R8 შეტყობინების გადაგზავნის დროით (მწმ) $16 + 32 = 52$

2. R4 – R3 – R8 შეტყობინების გადაგზავნის დროით (მწმ) $22 + 32 = 54$

3. R4 – R5 – R8 შეტყობინების გადაგზავნის დროით (მწმ) $7 + 12 = 19$

4. R4 – R6 – R8 შეტყობინების გადაგზავნის დროით (მწმ) $13 + 8 = 21$

მიღებული შედეგების მიხედვით მარშრუტიზატორ R4-დან მარშრუტიზატორ R8-მდე შეტყობინების გადაგზავნის ოპტიმალური გზა დროის მიხედვით გადის მარშრუტიზატორ R5-ზე და იგი შეადგენს 19მწმ. ეს შედეგი შეტანილია ცხრილში.

IV. გადაგზავნის ოპტიმალური დროის დადგენა მარშრუტიზატორ R9-მდე.

მარშრუტიზატორ R9-მდე შეტყობინების გადაგზავნის შესაძლო გზებია:

1. R4 – R2 – R9 შეტყობინების გადაგზავნის დროით (მწმ) $16 + 34 = 50$

2. R4 – R3 – R9 შეტყობინების გადაგზავნის დროით (მწმ) $22 + 42 = 64$

3. R4 – R5 – R9 შეტყობინების გადაგზავნის დროით (მწმ) $7 + 8 = 25$

4. R4 – R6 – R9 შეტყობინების გადაგზავნის დროით (მწმ) $13 + 22 = 35$

მიღებული შედეგების მიხედვით მარშრუტიზატორ R4-დან მარშრუტიზატორ R9-მდე შეტყობინების გადაგზავნის ოპტიმალური გზა დროის მიხედვით გადის მარშრუტიზატორ R5-ზე და იგი შეადგენს 25მწმ. ეს შედეგი შეტანილია ცხრილში.

ყველა მიღებული შედეგი დატანილია ნახაზზე 2.8.

მარშრუტიზატორი R4 გარკვეული დროის განმავლობაში სარგებლობს შედგენილი ცხრილით და მის შესაბამისად ახორციელებს შეტყობინებათა გადაგზავნას ქსელში.

ამ დროის გასვლის შემდეგ ცხრილის შედგენის პროცესი მეორდება, საჭიროების შემთხვევებში შედის მასში ცვლილებები და მარშრუტიზატორი უკვე განახლებული ცხრილის მაჩვენებლების შესაბამისად ახორციელებს შეტყობინებათა გადაგზავნას ქსელში.

მარშრუტიზაციის ცხრილების განახლების პროცედურების დროდადრო გამეორება განპირობებულია ქსელში მიმდინარე პროცესების დიდი დინამიურობით. რასაც განაპირობებს მოწყობილობათა დაზიანება და ცვლა, შეტყობინებათა

ნაკადების მნიშვნელოვანი განსხვავებულობა, (გამოწვეული მრავალი მიზეზის გამო - საზეიმო დღეები, სპორტული შეჯიბრებები, სტიქიური მოვლენები) და სხვა ფაქტორები.

2.4.2. მარშრუტიზაცია არხების მდგომარეობის გათვალისწინებით

ალგორითმი მარშრუტიზაცია არხების მდგომარეობის გათვალისწინებით დაფუძნებულია ხუთ მოთხოვნაზე, რომელთა შესრულებაც აუცილებელია განახორციელოს ყველა მარშრუტიზატორმა.

მარშრუტიზატორმა უნდა

1. დაადგინოს მისი მეზობლები და დააფიქსიროს მათი საქსელო მისამართები;
2. გაზომოს მეზობლებთან გადაგზავნის დრო ან გადაგზავნის ღირებულება (ან შეფასების რომელიმე სხვა კრიტერიუმი, რომელიც მიღებულია მოცემულ ქსელში შეტყობინების გადაცემის მთავარ მაჩვენებლად);
3. შექმნას სპეციალური პაკეტი, რომელიც შეიცავს 1 და 2 პუნქტების მიხედვით დაგროვილ სრულ ინფორმაციას, რაც პრაქტიკულად წარმოადგენს ალგორითმის, მარშრუტიზაცია არხების მდგომარეობის გათვალისწინებით, ასახვას;
4. გადაუგზავნოს შემუშავებული სპეციალური პაკეტი ქსელის ყველა მარშრუტიზატორს;
5. დაადგინოს მიღებული სპეციალური პაკეტების საფუძველზე უმოკლესი გზა ყველა მარშრუტიზატორამდე.

მარშრუტიზატორების მიერ ამ მოთხოვნათა რელიზების შემდეგ თითოეულ მათგანს ექნება ქსელის სრული ტოპოლოგიური სურათი მიღებული კრიტერიუმის ყველა მაჩვენებლით.

განვიხილოთ ხუთივე მოთხოვნა.

1. პირველ მოთხოვნას შეიძლება *მეზობლების გაცნობა* ვუწოდოთ.

მარშრუტიზატორი, რომლის ინიციალიზაციაც ხდება ქსელში, წყვეტს თავის უპირველეს ამოცანას: გაეცნოს და გაიცნოს მეზობლები. ამ მიზნით იგი აგზავნის მასთან შეერთებული ხაზების მიმართულებით (ფაქტიურად ყველა მეზობლისაკენ) პაკეტს სახელწოდებით HELLO (სალამი!). ნებისმიერი ხაზის მეორე ბოლოში მყოფი მარშრუტიზატორი ვალდებულია პაკეტ HELLO-ს მიღებისთანავე უპასუხოს მის გამომგზავნს და გადასცეს ინფორმაცია თავის შესახებ.

აქ ხაზი უნდა გაეხვას ერთ გარემოებას: ქსელში თითოეული მარშრუტიზატორის მისამართი აუცილებლად უნდა იყოს უნიკალური (ერთადერთი), რათა აბსოლუტურად გამოირიცხოს არევის ნებისმიერი შესაძლებლობა

მარშრუტიზატორების ვინაობის დადგენის დროს. ეს კი უზრუნველყოფს შეტყობინების აღრევით მიწოდების შესაძლებლობის გამორიცხვას.

2. მეზობლებთან შეტყობინების გადაგზავნის მაჩვენებლის გაზომვა.

როგორც აღნიშნული იყო, შეტყობინების გადაგზავნა რამდენიმე კრიტერიუმის მიხედვით შეიძლება შეფასდეს; ასევე შესაძლებელია ერთი ან რამდენიმე კრიტერიუმის ერთდროული გათვალისწინება. ნებისმიერი კრიტერიუმის, თუნდაც მათი ერთობლიობის, ძირითად მაჩვენებლად მაინც გადაგზავნის დრო რჩება. ამიტომ, შეეჩერდეთ ამ კრიტერიუმზე.

შეტყობინების გადაგზავნის დროის დადგენა.

შეტყობინების გადაგზავნის დროის დადგენის ფართოდ გავრცელებული მეთოდია პაკეტი ECHO (ეჰო) გაგზავნა. ეს მეთოდი ორი ვარიანტით შეიძლება განხორციელდეს. ერთ შემთხვევაში, გაიგზავნოს პაკეტი ECHO და უწყვეტ რეჟიმში დაუბრუნდეს გამგზავნს. ამ პროცესისათვის დახარჯული დრო კი ორად გაიყოს.

აქ უნდა ავლნიშნოთ, რომ უმეტეს შემთხვევაში გადაგზავნის დრო სხვადასხვაა. ამიტომ უკეთ შეფასების მიზნით პროცესს რამდენჯერმე იმეორებენ და საშუალო მაჩვენებლით აკეთებენ დასკვნას.

უფრო ზუსტი შედეგის მომცემია ამ მეთოდის მეორე ვარიანტი: შეტყობინების უშუალოდ გადაგზავნის დაწყების წინ (და არა მისი რიგში დგომის დროს) ტაიმერი გადამცემის მხარეს აფიქსირებს ამ მომენტს, ხოლო ტაიმერი მიმღების მხარეს კი მისი შემოსვლის მომენტს. ამ ინფორმაციით შევსებული პაკეტი ECHO უბრუნდება გამგზავნს. ამით კი უზრუნველყოფილია შეტყობინების გადაგზავნის რეალური მაჩვენებლების ობიექტური შეფასება.

3. არხების მდგომარეობის ამსახველი სპეციალური პაკეტის შექმნა.

მას შემდეგ, რაც რელიზებულ იქნება პირველი და მეორე პუნქტების მოთხოვნები, მიღებული მონაცემების საფუძველზე იქმნება სპეციალური საინფორმაციო პაკეტი. იგი იწყება გამგზავნის იდენტიფიკაციით, შემდეგ მოდის რიგითი ნომერი და მახასიათებელი კრიტერიუმის (მოცემულ შემთხვევაში გადაგზავნის დრო) მაჩვენებლით.

ასეთი პაკეტის შექმნა არ ითვლება რთულ პროცესად; უფრო პრობლემატურია თუ როდის, რა პერიოდულობით უნდა განხორციელდეს მათი შექმნის პროცესი.

თუ ქსელის ფუნქციონირება სტაბილურ რეჟიმში მიმდინარეობს (არ იცვლება აპარატურა, არ აქვს ადგილი სერიოზულ დაზიანებებს) პაკეტების განახლება პერიოდულად, გარკვეული ინტერვალებით ხორციელდება.

თუ ქსელის ფუნქციონირება მკვეთრად იცვლება რაიმე მნიშვნელოვანი მოვლენის, მაგალითად შემაერთებელი ხაზის ან მარშრუტიზატორის მწყობრიდან

გამოსვლის ან, პირიქით, დაზიანების შემდეგ მწყობრში ჩადგომის გამო, პაკეტების განახლების პროცესი სწრაფად უნდა განხორციელდეს.

4. არხების მდგომარეობის ამსახველი *სპეციალური პაკეტების გადავზავნა*.

მოთხოვნათა ეს პუნქტი, ერთი შეხედვით, ნაკლებ რთულ და საპასუხისმგებლო პროცესად გამოიყურება. რეალურად კი სწორედ ის არის ყველაზე რთული.

ვინაიდან ქსელში მიმდინარე პროცესები დიდი დინამიურობით ხასიათდებიან, ხოლო მდგომარეობის მახვენებელი პაკეტები უშუალოდ და უწყვეტ რეჟიმში მონაწილეობენ ამ პროცესებში, იქმნება სიტუაცია, როდესაც მარშრუტიზატორების ნაწილი უკვე მოქმედებს განახლებული პაკეტების გამოყენებით, ხოლო ნაწილი ისევ უკვე დაძველებული პაკეტის მონაცემებს ეყრდნობა, ვინაიდან ახალი ჯერ მათთან არ შემოსულა.

ეს კი იწვევს ქსელის ნორმალური ფუნქციონირების შეფერხებას.

ამ მიზეზის გამო, გარდა ასეთი პაკეტების უსწრაფესად გადაცემის ღონისძიებებისა, მიმართავენ ალგორითმ აგებას, როგორც ქსელის ნებისმიერ პუნქტამდე შეტყობინების საიმედო და გარანტირებული მიტანის საშუალებას.

5. *უმოკლესი გზის დადგენა* ქსელის მარშრუტუზატორებამდე.

მოცემული მარშრუტუზატორი მოაგროვებს რა ყველა პაკეტს არხების მდგომარეობის შესახებ, ქმნის ქსელის სრულ გრაფს. მიღებული გრაფის მიმართ კი იყენებს უმოკლესი გზების დადგენის დეიქსტრას ალგორითმს.

დეიქსტრას ალგორითმის გამოყენებით მიღებული შედეგები განთავსდება მარშრუტუზატორის სამარშრუტო ცხრილებში და ამის შემდეგ ქსელი გააგრძელებს ნორმალურ ფუნქციონირებას.

ალგორითმი, მარშრუტიზაცია არხების მდგომარეობის გათვალისწინებით, ფართოდ გამოყენებული ალგორითმია თანამედროვე კომპიუტერულ ქსელებში.

ამ ალგორითმის ინტერნეტში წარმატებით გამოყენების მიზნით ინტერნეტის პროექტირების ჯგუფის მიერ შემუშავებული და დანერგილია სპეციალური პროტოკოლი OSPF (Open Shortest Path First – უმოკლესი გზის არხების დია ალგორითმი). სტანდარტების საერთაშორისო ორგანიზაციის (ISO) მიერ კი მიღებულია ამ ალგორითმის გამოყენებისათვის ასევე მეტად მნიშვნელოვანი პროტოკოლი IS-IS (Intermediate System to Intermediate System – შუალედური სისტემა - შუალედური სისტემა).

თავი 3

ქსელის მომსახურება

3.1. შესავალი

კომპიუტერული ქსელი აგებისა და ექსპლუატაციაში გაშვებისთანავე აუცილებლად მოითხოვს მისი მომსახურების ორგანიზებას. ქსელის მომსახურება, როდესაც ლაპარაკია დიდ მასშტაბურ ქსელებზე, მოიცავს რთულ ღონისძიებათა მთელ კომპლექსს.

ქსელის მომსახურების ორგანიზების დროს, პირველ რიგში, აქცენტი უნდა გაკეთდეს პრობლემების არდაშვების მიმართულებით და, რა თქმა უნდა, პრობლემების წარმოშობის შემთხვევაში კი მათი უსწრაფესი აღმოფხვრის საშუალებებზე. ყოველივე ეს მომსახურე პერსონალისაგან მოითხოვს ქსელის ოპტიმალურ რეჟიმში ფუნქციონირების დაგეგმვასა და მართვის უზრუნველყოფას.

ქსელის მომსახურების პროცესში კი პრობლემატური თუ არა მტკივნეული მრავალი საკითხია. ასეთი საკითხების წარმოშობის ერთი მხარეა უშუალოდ ქსელის შემადგენელი მოწყობილობა-დანადგარების, როგორებიცაა უშუალოდ კომპიუტერები, მარშრუტიზატორები, ბოგირები და სხვა, საკაბელო მეურნეობა, არხწარმომქნელი აპარატურა, კვების სისტემები და ა.შ., შეფერხებით მუშაობა და მწყობრიდან გამოსვლა, მეორე მხარეა ქსელის რეალიზებული პარამეტრების შეთანხმება-შერწყმა მომხმარებლის მოთხოვნებით შექმნილ სიტუაციასთან, როდესაც მომსახურების დიდი ნაკადები ქსელის გადატვირთვის მიზეზი ხდება ანა თუ იმ მოწყობილობის ან მოწყობილობათა კომპლექსის შესაძლებლობათა ამოწურვის გამო; ასევე პრობლემატურია პაკეტების გადაცემის პროცესებში მნიშვნელოვანი ფლუქტუაციების წარმოშობა და სხვა.

კომპიუტერული ქსელის ეფექტურად მართვის ორგანიზების ერთერთი მნიშვნელოვანი გზაა ქსელის მონიტორინგი, რაც საშუალებას იძლევა დროულად იქნეს გამოვლენილი „ვიწრო ადგილები“ მის ფუნქციონირებაში, არადაამაკმაყოფილებელი პარამეტრებით ფუნქციონირებადი მოწყობილობა-დანადგარები. ამას გარდა ქსელის მონიტორინგი საშუალებას იძლევა აისახოს ქსელის ფუნქციონირების რეალური სურათი და, რაც მთავარია, შემუშავებულ იქნეს მისი მუშაობის ეტალონური გრაფიკი.

საბოლოოდ კომპიუტერული ქსელის მართვის შემუშავებულმა სისტემამ უნდა უზრუნველყოს მისი უწყვეტი, საიმედო და ეფექტური ფუნქციონირება.

მოცემულ თავში გამოყენებული ზოგიერთი ტერმინის განმარტება.

პაკეტების ნაკადი ან, მოკლედ, ნაკადი ეწოდება პაკეტების თანამიმდევრობას გადამცემიდან მიმღებამდე;

მონიტორინგი (ლათ. monitor – გამაფრთხილებელი) კომპიუტერულ ქსელთან დაკავშირებით გულისხმობს მუდმივი მეთვალყურეობის ორგანიზებას მის ფუნქციონირებაზე, რათა დადგენილ იქნეს ქსელის ძირითადი ხარისხობრივი და რაოდენობითი მაჩვენებლები, მათი შემდგომი ანალიზისათვის და სათანადო გადაწყვეტილებების მისაღებად;

გადატვირთვა ეწოდება სიტუაციას ქსელში, როდესაც პაკეტების ნაკადების რიცხვი აღწევს ისეთ ზღვრულ მნიშვნელობას, რომ ვერ ესწრება მათი მომსახურება და ქსელის წარმადობა იწყებს კლებას;

ფლუქტუაცია (ლათ. fluctuation – მერყეობა) ზოგადად ნიშნავს რაიმე სიდიდის შემთხვევით გადახრებს მისი საშუალო მნიშვნელობიდან, კომპიუტერულ ტექნოლოგიებში ეს შეტყობინების ცალკეული პაკეტების მომხმარებლისათვის მიწოდების დროთა გადახრებია მათი საშუალო მნიშვნელობიდან.

დატვირთვის მოკვეთა ეწოდება მარშრუტიზატორების მიერ, გადატვირთვის რეჟიმში მოხვედრის აღმოფხვრის მიზნით, მიწოდებული პაკეტების გარკვეული რიცხვის იგნორირებას.

3.2. გადატვირთვის პრობლემები და მათი აღმოფხვრის გზები

ქსელში პაკეტების გადაცემის პროცესში შეიძლება ადგილი ჰქონდეს გადატვირთვას. გადატვირთვა შეიძლება შეეხოს ცალკეულ კვანძს, ქსელის რომელიმე უბანს ან უბანთა ჯგუფს, მთელ ქსელს.

გადატვირთვები ქსელის ნორმალური ფუნქციონირების მნიშვნელოვან შემაფერხებელ ფაქტორს წარმოადგენენ, ამიტომ აუცილებელია მათი წარმოშობის მიზეზების შესწავლა, ანალიზი და აღმოფხვრის ღონისძიებების დასახვა, შემდგომ კი მათი ზედმიწევნით გატარება.

ქსელის გადატვირთვის არსი

ქსელის ნორმალური ფუნქციონირების პირობებში ადრესანტების (გადამცემი სააბონენტო კომპიუტერების) მიერ ქსელისთვის მიწოდებული შეტყობინებები წარმოდგენილი სათანადო პაკეტების სახით გადაიცემა ქსელის მიერ და მიეწოდებათ შესაბამის ადრესატებს (მიმღებ სააბონენტო კომპიუტერებს, ტერმინალებს). რა თქმა უნდა, გარდა სხვადასხვა სახის შეცდომების გამო დაზიანებული პაკეტებისა, რომელთა აღმოჩენა და აღდგენაც მიმდინარეობს წინასწარ შემუშავებული მეთოდებით.

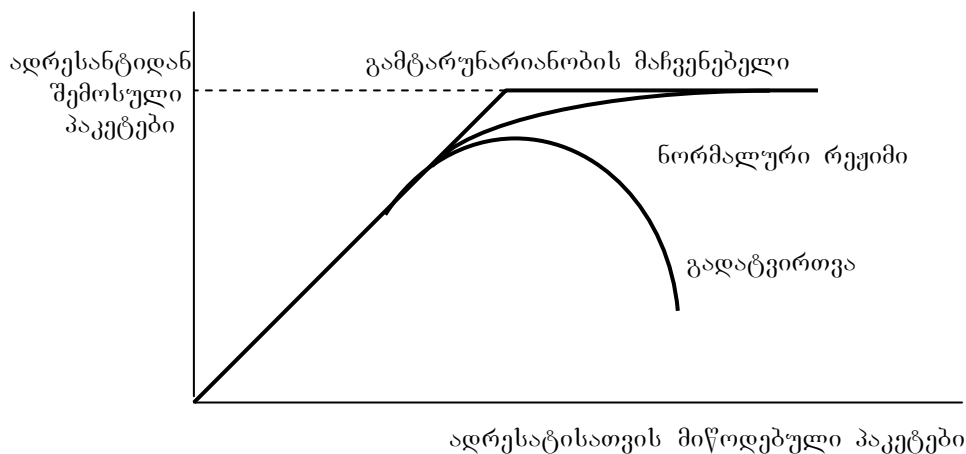
ერთიანად ასეთი სურათი იქმნება: მომხმარებლისათვის მიწოდებულ პაკეტთა რიცხვი შემოსულ პაკეტთა რიცხვის ტოლია და ქსელის ფუნქციონირებაც ნორმალურ რეჟიმში მიმდინარეობს.

ამ სახით შეტყობინებათა გადაცემის პროცესი წარიმართება თუ ქსელში გადაადგილებადი პაკეტების რიცხვი არ აღემატება ქსელის გამტარუნარიანობას.

თუ ქსელში შემოსულ პაკეტთა რიცხვი, ამა თუ იმ მიზეზის გამო, იწყებს სწრაფ მატებას, ე.ი. ტრაფიკი მნიშვნელოვნად იზრდება და მარშრუტიზატორები ვეღარ ასწრებენ მის მომსახურებას, ქსელში წარმოიშევა გადატვირთვა. ქსელის წარმადობა კლებულობს.

აქ მარშრუტიზატორების გადატვირთვას იმიტომ ესმება ხაზი, რომ ისინი წარმოადგენენ ძირითად მოწყობილობებს როგორც შიდა საქსელო, ასევე ქსელთაშორისი გადაცემების ორგანიზების პროცესებში.

ქსელის გადატვირთვის სიმპტომები წარმოდგენილია ნახაზზე 3.1 გრაფიკის სახით.



ნახ. 3.1. ქსელის გადატვირთვის სიმპტომები

ტრაფიკის შემდგომი ზრდის პირობებში წარმადობა კიდევ უფრო ეცემა და შეიძლება ისეთი მდგომარეობაც კი შეიქმნას, რომ საერთოდ შეწყდეს პაკეტების გადატანა ადრესანტიდან ადრესატამდე.

გადატვირთვა რამდენიმე ფაქტორმა შეიძლება გამოიწვიოს: ასე მაგალითად, პაკეტების ნაკადების ერთდროულმა შემოსვლამ რამდენიმე მიმართულებიდან, რომელთა გადაცემაც საჭიროა მხოლოდ ერთი გარკვეული მიმართულებით ან როდესაც რამდენიმე ადრესანტს სურვილი აქვს შეტყობინება ერთდროულად მიაწოდოს ერთ და იგივე ადრესატს. ეს კი რიგების წარმოშობის მიზეზი ხდება.

გადატვირთვების მიზეზი შეიძლება გახდნენ ნელმოქმედი პროცესორები. რაც არ უნდა დიდი გამტარუნარიანობა ახასიათებდეს გადამცემ ხაზს, თუ პროცესორი ნელა ასრულებს მასზე დაკისრებულ ფუნქციებს, რაც დაკავშირებულია პაკეტების

აღრიცხვასთან, რიგების მართვასთან, სამარშრუტო ცხრილების შედგენასთან და სხვა, ეს კი ერთიანად ქსელის გადატვირთვის მიზეზი გახდება.

გადატვირთვის მიზეზი შეიძლება გადამცემი ხაზები შეიქმნენ. პროცესორები დამაკმაყოფილებელი სიჩქარით ართმევენ თავს მათზე დაკისრებულ მოვალეობას, მაგრამ გადამცემი ხაზები ვერ ასწრებენ პაკეტთა ნაკადების დროულ გადაცემას. ამ შემთხვევაშიც ერთიანად ქსელის გადატვირთვას ექნება ადგილი.

საერთო სურათი ასეთია: ქსელში ყოველთვის იქნება „ვიწრო ადგილის“ პრობლემა თუ მისი კომპონენტების ფუნქციონირება არ არის სათანადოდ ურთიერთ ბალანსირებული.

გადატვირთვასთან ბრძოლის ზოგადი პრინციპები

კომპიუტერული ქსელების მართვა შეიძლება განხორციელდეს ორი სახით, როგორც ეს მიღებულია ზოგადად რთული სისტემების მართვის პროცესების რელიზების დროს: უკუკავშირების არ არსებობის და არსებობის პირობებში.

რთული სისტემების მართვა უკუკავშირების არ არსებობის პირობებში გულისხმობს ისეთ მდგომარეობას, როდესაც პირველად მხარეს, მიმწოდებელს, არ აქვს პირდაპირი, კონკრეტული ინფორმაცია თუ როგორ ხდება მიმღებ მხარეს იმ გადაწყვეტილებების რეალიზება, რომლებიც მიღებულია გადამცემი მხარის მიერ.

მართვა უკუკავშირების არსებობის პირობებში კი გულისხმობს გადამცემი მხარის მუდმივ პირდაპირ ინფორმირებას მიმღებ მხარეს მიმდინარე პროცესებზე.

სისტემებში უკუკავშირების გარეშე წინასწარ ტარდება მიზანდასახული ღონისძიებები, რათა გარანტირებულ იქნეს დასმული ამოცანების ეფექტური გადაწყვეტა. უკუკავშირების არ არსებობის პირობებში სისტემის ფუნქციონირებაში მუშაობის პროცესში ჩარევა და რაიმე კორექტივის შეტანა გათვალისწინებული არ არის.

კომპიუტერული ქსელების შემთხვევაში უკუკავშირების არ არსებობის პირობებში ფუნქციონირება, პირველ რიგში, მოითხოვს პაკეტების გადაცემის ისეთ ორგანიზებას, რომელიც გამორიცხავს ქსელის გადატვირთვას. ასეთი მიდგომა კი განპირობებულია იმით, რომ ამ დროს მხედველობაში არ მიიღება, უფრო სწორად, ვერ მიიღება ქსელის მიმდინარე მდგომარეობა და შესაბამისად გამოირიცხება რაიმე კორექტივის შეტანის შესაძლებლობა.

სისტემები უკუკავშირით დაფუნქციონირებულია მიმდინარე პროცესების ანალიზზე და მისი შედეგების შესაბამისი კორექტივების განხორციელებაზე.

კომპიუტერული ქსელების შემთხვევაში, როდესაც საქმე ეხება გადატვირთვას, უკუკავშირის რეალიზება სამი ეტაპისაგან შედგება:

1. ქსელზე დაკვირვება, რათა განსაზღვრულ იქნეს სად და როდის მოხდა გადატვირთვა;

2. გადატვირთვის შესახებ ინფორმაციის გადაცემა იქ, სადაც შეიძლება დაიგეგმოს და განხორციელდეს მისი აღმოფხვრის ღონისძიებები;

3. იმ ღონისძიებების გატარება, რომლებიც აღმოფხვრიან გადატვირთვას.

ქსელზე დაკვირვების დროს, როდესაც გადატვირთვის შესაძლებლობის აღმოჩენაა საჭირო, განისაზღვრება რამდენიმე მნიშვნელოვანი პარამეტრი, რომელთა შორისაც აღსანიშნავია:

- იმ პაკეტების პროცენტული რაოდენობა, რომელთა მიღების იგნორირებაც ხდება მახსოვრობის კვანძების გადავსების გამო;
- იმ პაკეტების პროცენტული რაოდენობა, რომელთა გადაცემაც მეორდება მიღების დადასტურების არქონების გამო;
- პაკეტების დაყოვნების საშუალო დრო;
- პაკეტების დაყოვნების დროის გადახრის საშუალო კვადრატული მნიშვნელობა.

ამ პარამეტრების რიცხვითი მნიშვნელობების ზრდა ყოველთვის იმის მაჩვენებელია, რომ გადატვირთვის შესაძლებლობა მატულობს.

ქსელზე დაკვირვების მეორე ეტაპი გულისხმობს ქსელში დამატებითი ინფორმაციის გადაცემას, რაც კიდევ უფრო ამძიმებს მის ისედაც რთულ მდგომარეობას.

ამ მდგომარეობიდან გამოსვლა შესაძლებელია თვითონ სამომხმარებლო პაკეტში დამატებითი სპეციალური ველის შეტანით, რომელშიც აისახება გადატვირთვის მდგომარეობა და მარშრუტიზატორი მას მიიღებს სამომხმარებლო პაკეტის სამსახურებრივი ნაწილის მოცულობის უმნიშვნელო ცვლილების გზით.

კომპიუტერული ქსელი უკუკავშირით უკვე იდიაში გულისხმობს, რომ მიღებული ინფორმაცია გადატვირთვასთან დაკავშირებით გამოყენებულ იქნება გადატვირთვის აღმოფხვრის მიზნით.

გადატვირთვის არსებობა ნიშნავს იმას, რომ დატვირთვა დროებით ჭარბობს ქსელის რესურსების შესაძლებლობებს მოცემულ ადგილზე არსებულ მოწყობილობებით.

ასეთ პირობებში პირველ რიგში გამოყენებულ უნდა იქნეს ქსელის შიდა რესურსები: თუ ჩვეულებრივ პირობებში პაკეტების გადაცემა ოპტიმალური გზებით ხორციელდება, ადგილობრივი კვანძების გადატვირთვის შემთხვევებში გადაცემა უნდა განხორციელდეს სხვა ნაკლებად ეფექტური მარშრუტებით, თუ კი ეს შესაძლებელს გახდის დაკმაყოფილდეს მომხმარებელთა მოთხოვნები.

გადატვირთვის პრობლემის გადაჭრის მიმართ ორი მიდგომა არსებობს:

- დამატებითი რესურსების ამოქმედება;
- დატვირთვის შემცირება.

თუმცა არც ორივე მიდგომის ერთდროული გამოყენებაა გამორიცხული.

კომპიუტერული ქსელების შემთხვევაში დამატებითი რესურსების გამოყენების მაგალითად შეიძლება მოყვანილ იქნეს მოდემების საშუალებით სატელეფონო ქსელის გამოყენება პაკეტების გადაცემის ორგანიზებისათვის. ქსელის ფუნქციონირების ნორმალური რეჟიმისათვის ეს საშუალება არ არის მიზანშეწონილი (ღირებულების, ნელმოქმედების, საიმედოობისა და სხვა მაჩვენებლების მიხედვით), მაგრამ გადატვირთვის აღმოფხვრის პროცესში კი შეიძლება გამართლებული აღმოჩნდეს.

ასევე შეიძლება მოყვანილ იქნეს მაგალითი ტელეკომუნიკაციური თანამგზავრული სისტემების ამ მიზნით გამოყენების შესახებ. თუ ქსელის ნორმალურ რეჟიმში გამოიყენება თანამგზავრული ხაზების შეზღუდული რაოდენობა, რაც განპირობებულია მათი დიდი ღირებულებით, გადატვირთვის პროცესში შეიძლება გამართლებული აღმოჩნდეს მათი უფრო ფართომასშტაბიანი გამოყენება.

თუ გადატვირთვებთან ბრძოლის პროცესში შიდა და გარე რესურსების გამოყენების ყველა გზა ამოიწურება და, მიუხედავად ამისა, გადატვირთვა არ აღმოფხვრება, მიმართავენ დატვირთვის შემცირებას.

დატვირთვის შემცირება ნიშნავს მომხმარებელთა მოთხოვნების გარკვეული ნაწილის შეუსრულებლობას.

ქსელის მიერ დატვირთვის შემცირების დროს მომხმარებელი მომსახურების მოთხოვნაზე უარყოფით პასუხს იღებს და იგი იძულებული ხდება დაელოდოს ქსელში მომსახურების შესაძლებლობის აღდგენას.

ქსელისათვის ეს არ არის კარგი მაჩვენებელი. ამ დროს მომხმარებლის თვალში ქსელის ავტორიტეტის გაუფასურება ხდება, ამიტომ იგი არასასურველ იძულებით ღონისძიებად უნდა ჩაითვალოს.

მიუხედავად ამისა უმჯობესია მომხმარებელი ნაწილობრივ შეიზღუდოს, ვიდრე ქსელმა საერთოდ შეწყვიტოს ფუნქციონირება, როგორც ეს მოსალოდნელია გადატვირთვის უმართავი პროცესების წარმოშობის შემთხვევებში.

გადატვირთვის თავიდან აცილების სტრატეგიები

გადატვირთვის თავიდან აცილების სტრატეგიები მნიშვნელოვანია, როგორც უკუკავშირების არმქონე, ასევე უკუკავშირების მქონე ქსელებისათვის. განსხვავება ძირითადად მდგომარეობს იმაში, რომ უკუკავშირების არმქონე ქსელებში უნდა

გატარდეს ღონისძიებები, რომლებიც მის წარმოშობას თუ არ გამოორიცხავს, ყოველ შემთხვევაში ნაკლებად შესაძლებელს გახდის, ხოლო უკუკავშირების მქონე ქსელებში კი მათი წარმოშობის (ან წარმოშობის შესაძლებლობის) პირობებში უნდა გატარდეს ღონისძიებები მათი აღმოფხვრის მიზნით.

უკუკავშირების არმქონე ქსელებისათვის შემუშავებულია გადატვირთვებთან ბრძოლის რამდენიმე სტრატეგია:

- განმეორებითი გადაცემა;
- მიღების დადასტურება;
- პაკეტების იგნორირება.

განმეორებით გადაცემის, ანუ კვლავგადაცემის სტრატეგიაში დგინდება გარკვეული დროითი ინტერვალი, რომლის განმავლობაშიც მიმწოდებელი ელოდება მიმღებისაგან შეტყობინების მიღების დადასტურებას. ამ დროის გასვლის შემდეგ თუ მიმწოდებელს არ აქვს მიღებული დადასტურება, იგი იწყებს შეტყობინების კვლავგადაცემას.

კვლავგადაცემის სტრატეგიაში მეტად მნიშვნელოვანია თუ დროის რა მონაკვეთი შეირჩევა დადასტურების დალოდებისათვის.

თუ ეს დრო მცირე აღმოჩნდება, ვიდრე შეტყობინების ნორმალურ გადაცემას სჭირდება ქსელში, მაშინ მიმწოდებელი დაიწყებს კვლავგადაცემას, თუმცა არსებობს თუ არა მისი საჭიროება, არ არის ცნობილი. ამ შემთხვევაში ქსელში იგზავნება უკვე ყოველად უსარგებლო პაკეტები, რომლებიც ქსელის მდგომარეობის დამძიმების მიზეზი გახდნენ და მისი გადატვირთვა გამოიწვიეს.

თუ ეს დრო მეტი აღმოჩნდება, ვიდრე შეტყობინების ნორმალურ გადაცემას სჭირდება ქსელში, მაშინ მიმწოდებელი უქმად კარგავს დროს დადასტურების მოლოდინში. ეს ვარიანტი განსაკუთრებით მიუღებელია თუ დადასტურების მიღება მიმწოდებლისათვის რაიმე შემდგომი მოქმედების მასტიმულირებელია.

აქედან გამომდინარე, დადასტურების დალოდების დროის შერჩევას დიდი მნიშვნელობა ენიჭება და იგი ზედმიწევნით უნდა განისაზღვროს ქსელის მონიტორინგის მონაცემების საფუძველზე.

მიღების დადასტურების სტრატეგიაში მნიშვნელოვანია თუ როგორ ხორციელდება დადასტურება. იგი შეიძლება ხორციელდებოდეს თითოეული პაკეტის, პაკეტთა ჯგუფის ან მთელი შეტყობინების მიღების შემდეგ. ასეთი დამადასტურებელი შეტყობინებები თვითონ შეიძლება გახდნენ ქსელის გადატვირთვის მიზეზი, ამიტომ დადასტურების სტრატეგია ასევე ზედმიწევნით უნდა განისაზღვროს.

განსაკუთრებით მისაღებია დადასტურების გაგზავნა არა დამოუკიდებელი შეტყობინების სახით, არამედ საჭირო მიმართულებით გადაადგილებადი სხვა მომხმარებლის შეტყობინების გამოყენებით; მის სამსახურებრივ ნაწილში გამოიყოფა სპეციალური ველი, რომელშიც განთავსდება ინფორმაცია დადასტურების საჭიროების მქონე შეტყობინების მიმღების მიერ მიღების შესახებ. ეს მეთოდი რელიზაციის პროცესში მეტ დროს მოითხოვს და დადასტურების მიღებას გარკვეულწილად აყოვნებს, მაგრამ ასევე გარკვეულწილად ქსელს იცავს გადატვირთვებისაგან.

დადასტურების ამ სახით გადაგზავნას „ზედღების“ მეთოდს უწოდებენ.

პაკეტების იგნორირების სტრატეგიის დროს პაკეტები, რომლებიც დიდი დროის განმავლობაში გადაადგილდებიან ქსელში შეიძლება იგნორირებულ იქნენ უახლოესი მარშრუტიზატორის მიერ თუ ის გადატვირთვის პრობლემის წინაშეა. ამ მოქმედების ლოგიკა ასეთია: თუ პაკეტი დიდი დროის განმავლობაში გადაადგილდება ქსელში და ვერ აღწევს მიმღებამდე, შესაბამისად, ვერც მიმწოდებელი მიიღებდა მისი მიღების დადასტურებას და მას თავიდან გადასცემდა. აქედან გამომდინარე ქსელში ორი ერთნაირი პაკეტის ყოფნაა მოსალოდნელი, ამიტომ პირველის იგნორირება მისაღებია.

ზოგადად შეიძლება ითქვას, რომ კარგად მოფიქრებული, დასაბუთებული სტრატეგია გადატვირთვის პრობლემას თუ არ მოხსნის, ყოველ შემთხვევაში მნიშვნელოვნად შეამსუბუქებს და, პირიქით, მოუფიქრებული, დაუსაბუთებული სტრატეგია კი სიტუაციას კიდევ უფრო დაამძიმებს.

გადატვირთვებთან ბრძოლა ვირტუალურ არხებიან ქსელებში

ვირტუალურ არხებიან ქსელებში გადატვირთვებთან ბრძოლის ორი მეთოდი გამოიყენება:

1. შედწვევის მართვა;
2. საცობების გვერდის ავლა.

შედწვევის მართვის მეთოდის გამოყენების დროს გადატვირთვის სიგნალის მიღებისთანავე იკრძალება ნებისმიერი ახალი ვირტუალური არხის წარმოქმნა მანამ, სანამ გადატვირთვა არ აღმოიფხვრება. ცხადია, ერთი მხრივ, გადატვირთულ ქსელში ყოველი ახალი მომხმარებლის შედწვევა კიდევ უფრო გაართულებს მდგომარეობას, მეორე მხრივ, ასეთი მიდგომა მომხმარებლისათვის მეტად ხისტია და შინაგანად მიუღებელი. ეს ქსელის მესვეურთათვის იაფი, საიმედო და პრაქტიკული მეთოდია, თუმცა ქსელის ავტორიტეტის ნაწილობრივი შელახვის ხარჯზე.

საცობის გვერდის ავლის მეთოდის გამოყენების დროს გადატვირთვის სიგნალის მიღებისას არ იკრძალება ახალი მომხმარებლის შედწვევა და

ვირტუალური არხის წარმოქმნა მიმდინარეობს გადატვირთული კვანძის, საცობის, გვერდის ავლით.

ცხადია, რომ ამ მეთოდის გამოყენება შესაძლებელია თუ მთელი ქსელი არ არის სრულად გადატვირთვის სიტუაციაში და როდესაც გადატვირთვა არ შეხებიან უშუალოდ ადრესანტთან და ადრესატთან დაკავშირებულ მარშრუტიზატორებს.

საცობის გვერდის ავლის მეთოდის გამოყენების საილუსტრაციოდ გამოვიყენოთ ნახაზზე 3.2 მოცემული ქსელის ფრაგმენტი.

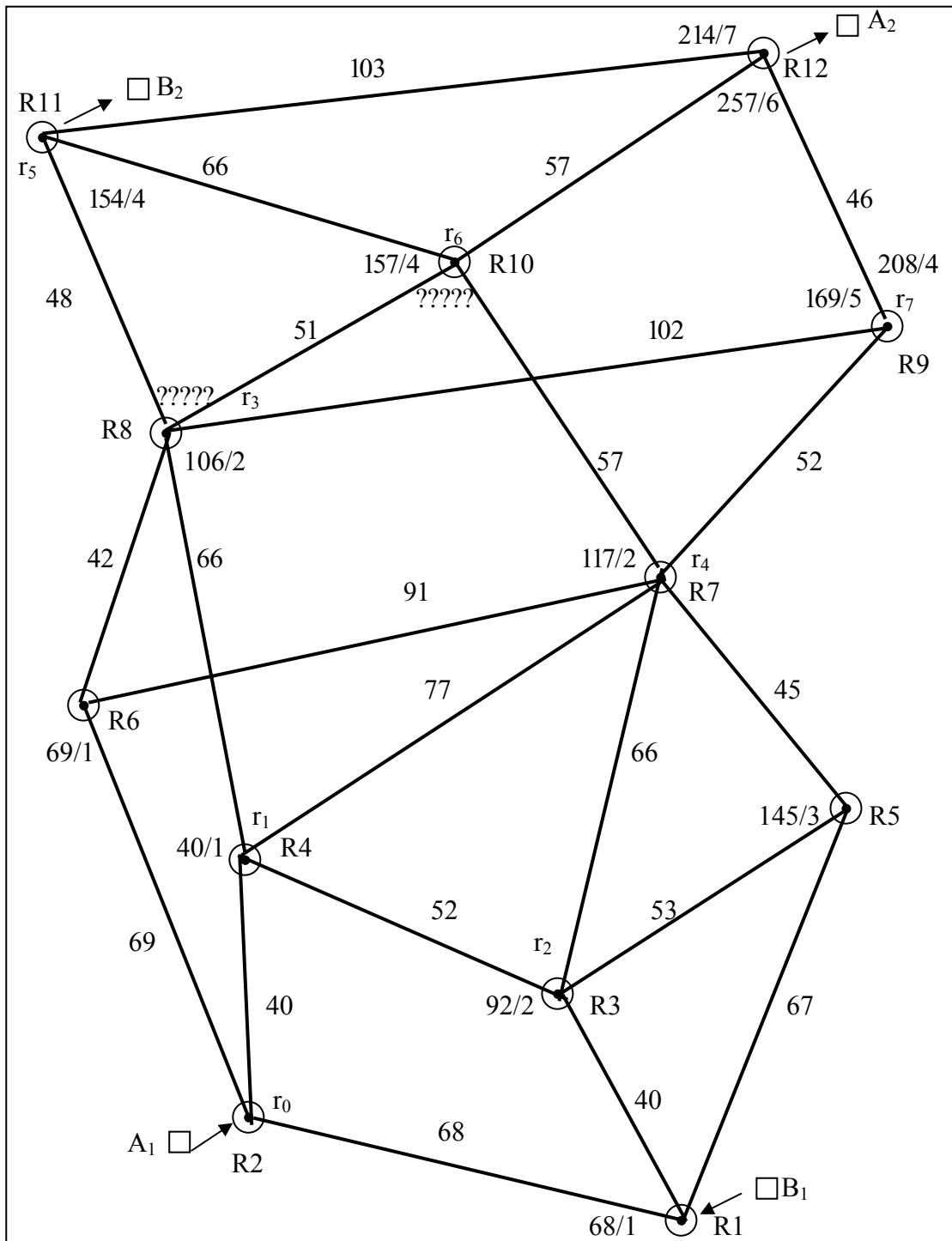
ვთქვათ, რომ მოცემული ქსელის ფრაგმენტის მიხედვით გადაიტვირთნენ მარშრუტიზატორები R8 და R10. მომხმარებელის მოითხოვნა კი განაპირობებს შეტყობინების გადაცემას R1 მარშრუტიზატორიდან R11 მარშრუტიზატორამდე. საცობის გვერდის ავლის მეთოდის გამოყენების პირველი პირობა, რომ უშუალოდ ადრესანტთან და ადრესატთან დაკავშირებული მარშრუტიზატორები არ არიან გადატვირთულნი - დაცულია. ასევე დაცულია პირობა, რომ ქსელი არ არის სრულად გადატვირთვის სიტუაციაში.

დაუშვათ, რომ დეიქსტრას ალგორითმის მიხედვით შერჩეულია ოპტიმალური მარშრუტი R1-სა და R11-ს შორის: R1 – R2 - R4 - R8 - R11, საერთო სიგრძით $68 + 40 + 66 + 48 = 222$ კმ; ასევე შერჩეულია სარეზერვო მარშრუტი R1-სა და R11-ს შორის: R1 – R3 - R7 - R10 - R11, საერთო სიგრძით $40 + 66 + 57 + 66 = 229$ კმ.

შექმნილ სიტუაციაში აღმოჩნდა, რომ ორივე მარშრუტზე, როგორც ოპტიმალურზე, ასევე სარეზერვოზე არის გადატვირთული მარშრუტიზატორი: ოპტიმალურზე R8 და სარეზერვოზე R10. ამავე დროს R1-სა და R11-ს შორის არსებობს სხვა მარშრუტები, რომლებზეც გადატვირთვები არ ფიქსირდება. ასეთია მაგალითად, მარშრუტი R1 – R3 - R7 - R9 - R12 - R11, რომლის საერთო სიგრძეც შეადგენს $40 + 66 + 52 + 46 + 103 = 307$ კმ.

როგორც ვხედავთ, ახლად შერჩეული მარშრუტის სიგრძე (307 კმ), გაცილებით მეტია ვიდრე ოპტიმალურსა (222 კმ) და სარეზერვოსი (229 კმ), მაგრამ გადატვირთვის შექმნილ სიტუაციაში მისი გამოყენება უთუოდ მისაღებია.

ერთიანად შეიძლება გაკეთდეს დასკვნა, რომ ვირტუალურ არხებიან ქსელებში გადატვირთვებთან ბრძოლის ორივე მეთოდი, როგორც შედწევის მართვა, ასევე საცობების გვერდის ავლა პრინციპიალურად მისაღებია, მხოლოდ ყოველ კონკრეტულ შემთხვევაში მათი გამოყენების დასაბუთება უნდა მოხდეს უარყოფითი მხარეების ანალიზის შედეგად.



⊙ - მარშრუტიზატორი (Router, R)

□ - სააბონენტო პუნქტი (Subscriber point, SP)

ნახ. 3.2. ქსელის ფრაგმენტი (ტოპოლოგიური სურათი)

გადატვირთვებთან ბრძოლა დატვირთულ არხებთან ქსელებში

დატვირთულ არხთან ქსელებში თითოეულმა მარშრუტიზატორმა თვალყური უნდა ადევნოს თუ როგორი რიგები იქმნება შემომავალ მხარეს და როგორია მასთან დაკავშირებული ხაზების მდგომარეობა, ყოფნით თუ არა მათ გამტარუნარიანობა. მიღებული მაჩვენებლები უნდა შედარდეს წინასწარ დადგენილ ზღვრულ მნიშვნელობებს. თუ მიღებული მაჩვენებლები უახლოვდებიან ზღვრულ მნიშვნელობებს ეს ნიშანი იქნება იმის, რომ ახლოვდება სასიფათო მდგომარეობა – საცობის წარმოშობის სიტუაცია. ამ დროს თითოეული პაკეტი გადის შემოწმებას და თუ მას უწევს გადატვირთვასთან მიახლოვებულ მარშრუტიზატორთან გავლა ისახება დაცვის ღონისძიებები.

დატვირთულ არხთან ქსელებში მიღებულია გადატვირთებისაგან დაცვის ორი მეთოდის გამოყენება: გამაფრთხილებელი ბიტით და შემაკავებელი პაკეტით.

განვიხილოთ ორივე მეთოდი.

გამაფრთხილებელი ბიტი. პაკეტი გაივლის რა მარშრუტიზატორს, რომლის ფუნქციონირებაც გადატვირთვის ზღვარზეა, მისი სამსახურებრივი ნაწილის დადგენილ ადგილზე ჩაიწერება „ერთიანი“- გამაფრთხილებელი ბიტი. ამით გადამცემი მხარე როცა მიიღებს მიწოდების დადასტურების პაკეტს, გაფრთხილების ზონის ანალიზით შეიტყობს გადატვირთვის სიტუაციის შესახებ და მას გაითვალისწინებს პაკეტების შემდგომი გადაცემის დროს, ცხადია, მათი შემცირების მიმართულებით; თუ ეს პროცესი – გაფრთხილების მიღება – გაგრძელდება, წყარომ კიდევ უფრო უნდა მეტად შეზღუდოს მიწოდება. ასე მანამ, სანამ არ შეწყდება გამაფრთხილებელი ბიტების შემოსვლა. გამაფრთხილებელი ბიტის შემოსვლის შეწყვეტის შემდეგ მიმწოდებელი ნელ-ნელა მოუმატებს გადაცემის სიჩქარეს დააკვირდება მიმდინარე სიტუაციას: ხომ არ შემოდის ისევ გამაფრთხილებელი ბიტი და სათანადო რეაგირებას მოახდენს ან ისევ შეამცირებს ან ისევ გაზრდის მიწოდებას.

ამგვარად, ხორციელდება მიმდინარე პროცესების დინამიური თვალყურის დევნება და მასზე შესაბამისი რეაგირება ქსელში გადატვირთვის წარმოშობის გამორიცხვის მიზნით.

გამაფრთხილებელი ბიტის მეთოდის გამოყენების დროს ქსელის ფუნქციონირების ალგორითმი ისეა აწყობილი, რომ გადატვირთვის პრობლემის მოგვარება თითქოს არაპირდაპირი ჩარევით ხორციელდება: მომხმარებელმა, კონკრეტულად შეტყობინების მიმწოდებელმა, თვითონ უნდა გამოიტანოს დასკვნა შექმნილ მდგომარეობასთან დაკავშირებით და შესაბამისად იმოქმედოს.

შემაკავებელი პაკეტი. ამ მეთოდის რეალიზება ითვალისწინებს გადატვირთვის ზღვარზე მყოფი მარშრუტიზატორის მიერ უშუალოდ მიმწოდებლისათვის შემაკავებელი პაკეტის გაგზავნას. გადატვირთვის ზღვარზე მყოფი მარშრუტიზატორი დაკავებული, დაყოვნებული პაკეტის სამსახურებრივი ნაწილიდან იღებს მონაცემებს მიმწოდებლის შესახებ და ამ მიმწოდებელს უგზავნის შემაკავებელ პაკეტს, მოთხოვნით: შეამცირე მიწოდება.

წინასწარი შეთანხმებების შესაბამისად მიმწოდებელი, რომელიც მიიღებს შემაკავებელ პაკეტს, ვალდებულია შეამციროს მიწოდებულ პაკეტთა ნაკადი. მოთხოვნა მიწოდების ნაკადის შემცირების შესახებ შეიძლება იყოს სამი დონის: მსუბუქი, მკაცრი და ულტიმატუმის ხასიათის. შესაბამისად ნაკადის შემცირება ხორციელდება წინასწარ დადგენილი ზღვრების მიხედვით: გარკვეული პროცენტით, ორჯერადით, ოთხჯერადით, ან საერთოდ მიწოდების შეწყვეტით. ცხადია, ეს დონისძიებები დროებითია და გრძელდება ქსელის ფუნქციონირების ნორმალური რეჟიმის აღდგენამდე.

დატვირთვის მოკვეთა

გადატვირთვასთან ბრძოლის მრავალი მეთოდია შემუშავებული. კონკრეტულ ქსელში, ჩვეულებრივად, დანერგილია მათი გარკვეული რაოდენობა და გადატვირთვის ზღვართან ყოფნისას ყველა ეს მეთოდი იქნება გამოყენებული გადატვირთვის აღმოფხვრის მიზნით. თუ მოცემულ კონკრეტულ სიტუაციაში გადატვირთვასთან ბრძოლის მიღებულმა არც ერთმა მეთოდმა სასურველი შედეგი არ გამოიღო, მაშინ მიმართავენ ყველაზე რადიკალურ მეთოდს – დატვირთვის მოკვეთას. ამ დროს პაკეტების ნაწილი აღარ ექვემდებარება დამუშავებას და ქსელში შექმნილი სიტუაცია მარტივდება. ცხადია, ეს მიიღწევა მომხმარებელთა მომსახურების ნაწილობრივი გაუარესების ხარჯზე, მაგრამ ეს უმჯობესია ვიდრე გადატვირთვით გამოწვეული სრული ქაოსი ქსელში.

დატვირთვის მოკვეთის ალგორითმის რეალიზება საკმაოდ რთულია. პაკეტებს ქსელში სხვადასხვა პრიორიტეტი გააჩნიათ. ზოგიერთი მათგანის გადაცემის უზრუნველყოფა ქსელისათვის ყველა შემთხვევაში აუცილებელია და თანაც ყოველგვარი შეფერხების გარეშე. ნაწილის იგნორირება კი პრინციპულად, ალბათ, შესაძლებელია, მაგრამ ქსელი თვითონ, ცხადია, ვერ განსაზღვრავს შეტყობინების პრიორიტეტულობას. ეს მომხმარებლის პრეროგატივაა. მომხმარებელმა უნდა აღჭურვოს შეტყობინება ამ მაჩვენებლით, ე.ი. განსაზღვროს შეტყობინება დიდი პრიორიტეტის მატარებელია თუ მას პრიორიტეტულობის დაბალი მაჩვენებელი ახასიათებს.

ამავე დროს, მომხმარებელმა, რომელმაც იცის, რომ მისი შეტყობინება შეიძლება მოხვდეს დატვირთვის მოკვეთის ზონაში, მისი გარანტირებული უფრო სწრაფი მომსახურების მიზნით შეიძლება ყველა შეტყობინება აღჭურვოს პრიორიტეტული ნიშნით: „ძალიან მნიშვნელოვანია, დაუყოვნებლად გადაიცეს“.

ამ მდგომარეობიდან გამოსავალი ასეთია: პრიორიტეტულობის მაჩვენებლის გაზრდასთან ერთად უნდა გაიზარდოს გადაცემის მომსახურების ღირებულება. მომხმარებელმა კი თვითონ შეაფასოს უღირს კი მას გადასცეს შეტყობინება ძვირადღირებული პრიორიტეტით, თუ დაკმაყოფილდეს ნაკლებადღირებულით. საბოლოო შემთხვევაში ხომ არც ერთი პაკეტი არ იკარგება (უიშვიათეს გამონაკლისს გარდა, რაც პრიორიტეტულ მაჩვენებელზე სულაც არ არის დამოკიდებული) და ყველა მათგანი მიაღწევს ადრესატემდე მხოლოდ შედარებით უფრო მეტი დაყოვნებით.

ფლუქტუაციები და მათთან ბრძოლა

თანამედროვე რთული ქსელებით გავრცელებული პაკეტები მრავალი სახის გზებით გადაადგილდებიან და დაყოვნების სხვადასხვა დროით მიაღწევენ მომხმარებლებამდე. ამგვარად წარმოიქმნება ფლუქტუაციების პროცესები.

შეტყობინების აღწარმოების დროს ფლუქტუაციების ზეგავლენა მიღებული ინფორმაციის ხარისხზე სხვადასხვაა იმის და მიხედვით თუ რა სახისაა იგი და როგორ წარმოებს მისი აღწარმოება მიმღების მხარეს. ასე მაგალითად, თუ მიღებული შეტყობინება წინასწარ ჩაიწერება, ე.ი. აუცილებელი არ არის მისი მომხმარებლისათვის დროის რეალურ მასშტაბში მიწოდება, ცხადია, მიღების პროცესში წარმოშობილ ფლუქტუაციებს არავითარი ზეგავლენის მოხდენა არ შეუძლიათ აღწარმოების პროცესზე. თუ პაკეტების გადაცემა დაკავშირებულია მაგალითად, ინტერნეტ-ტელეფონიასთან ან ვიდეოკონფერენციასთან, გადაცემასთან ინტერაქტიურ რეჟიმში, ფლუქტუაციების უმნიშვნელო დონეც კი მიუღებელი ხდება.

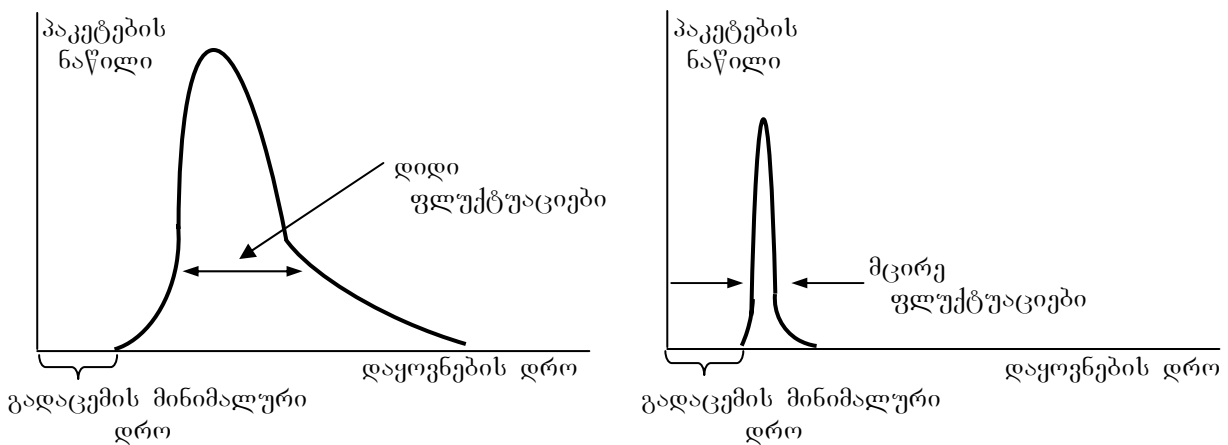
ქსელში ნებისმიერი შეტყობინების გადაცემა გარკვეულ დროს მოითხოვს. როგორც ცნობილია იდეალურ შემთხვევაშიც კი გადაცემის სიჩქარე უსასრულო არ არის და დაკავშირებულია სინათლის გავრცელების სიჩქარესთან. რეალურ სისტემებში წარმოიშობა დამატებითი დაყოვნებები დაკავშირებული შეტყობინების დამუშავებასა და საკომპუტაციო წრედების მოქმედებებთან, ხოლო დაყოვნების დროის ხანგრძლივობა კი დაკავშირებულია ამ მოქმედებების სისწრაფეზე, რაც მით უმეტეს, შემოსაზღვრულია.

მიღებულია, რომ თუ პაკეტების მიწოდების დრო 20-30 მლწმ-ის ფარგლებშია, შეტყობინების გადაცემა ნორმალურად მიმდინარეობს; თუ იგივე შეტყობინების პაკეტების ნაწილის მიწოდების დრო 20 მლწმ-ია, ხოლო ნაწილის კი 30 მლწმ,

ფლუქტუაციის მნიშვნელობა დიდი იქნება იგი შესამჩნევი გახდება შეტყობინების აღწარმოების დროს გამოსახულებისა და ხმის დამახინჯების სახით.

თუ მიიღწევა ისეთი შედეგი, რომ ფლუქტუაცია 24-25 მლწმ ფარგლებში მოექცეს, მაშინ იგი პრაქტიკულად არ იქნება შესამჩნევი და მაშინ ასეთი ხარისხით შეტყობინების აღწარმოება მისაღები გახდება. ცხადია, ფლუქტუაციის დაშვებული დიაპაზონი რეალურ ტექნიკურ შესაძლებლობებს უნდა შეესაბამებოდეს და მისი მიღწევა არ უნდა მოითხოვდეს რაიმე განსაკუთრებული და ძვირადღირებული ღონისძიებების გატარებას.

ნახაზზე 3.3 წარმოდგენილია დიდი და მცირე ფლუქტუაციის გრაფიკული გამოსახულება.



ნახ. 3.3. პაკეტების გადაცემის დიდი და მცირე ფლუქტუაციები

პაკეტების გადაცემის ფლუქტუაციების სრულად თავიდან აცილება თანამედროვე რთულ ქსელებში პრაქტიკულად შეუძლებელია. მათი შემცირების მიზნით კი სხვადასხვა მეთოდი შემუშავებული.

განვიხილოთ ფლუქტუაციის შემცირების ერთერთი მეთოდი. როდესაც მნიშვნელოვანი ფლუქტუაციაა მოსალოდნელი და მისი სიდიდე მიუღებელია, პირველ რიგში განსაზღვრავენ გადაცემის აუცილებელ დროებს გადაცემის ხაზის ნებისმიერ სატრანზიტო უბანზე და ამ მონაცემებს განათავსებენ პაკეტების სამსახურებრივ ნაწილში. შემდეგ ამ ხაზზე განათავსებული ნებისმიერი მარშრუტიზატორი მიიღებს რა მოცემული შეტყობინების შემადგენელ პაკეტს, დაადგენს იგი გრაფიკის მიხედვით იგვიანებს, თუ წინსწრებით გადაადგილდება. დაგვიანებული მაჩვენებლის დადგენის შემთხვევაში ტარდება ღონისძიება მისი შემდგომი სწრაფი გადაადგილების მიზნით, ხოლო თუ გადაადგილება წინმსწრებია, პირიქით, გატარდება ღონისძიება მისი მოძრაობის შეყოვნების მიზნით. პაკეტების გადაადგილების პროცესების ამ სახით

დარეგულირებით მიიღება ფლუქტუაციის მისაღები მნიშვნელობა და მიიღწევა შეტყობინების გადაცემის მოთხოვნების შესაბამისი ხარისხი.

დასკვნის სახით ავლნიშნოთ, რომ გადატვირთვების საკითხი ერთერთ უმნიშვნელოვანეს საკითხს წარმოადგენს ქსელების მომსახურების პროცესში და მისი წარმატებით გადაწყვეტა ქსელის საიმედო და ეფექტური ფუნქციონირების საუკეთესო მაჩვენებელია.

3.3. მომსახურების ხარისხი და მისი უზრუნველყოფა

ქსელებისადმი წაყენებული გაზრდილი მოთხოვნები სვამენ ამოცანას, რომ უზრუნველყოფილ იქნეს მათ მიერ გაწეული მომსახურების მაღალი ხარისხი. ქსელის მომსახურების მაღალმა ხარისხმა კი უნდა შექმნას იმის წინა პირობა, რომ წარმატებით გამოვლინდეს ქსელის მრავალფეროვანი შესაძლებლობები და ჩაყენებულ იქნენ ისინი მისი მომხმარებლების სამსახურში.

მოთხოვნები მომსახურების მიმართ

მომსახურების დონის შესაფასებლად საერთაშორისო ორგანიზაციების მიერ დადგენილია სათანადო პარამეტრები. ეს პარამეტრები წარმოდგენილია მომსახურების ხარისხის განმსაზღვრელ ცნებაში: Quality of Service (QoS).

ქსელის მიერ გაწეული მომსახურების ხარისხის დასახასიათებლად მიღებულია მისი ოთხი პარამეტრი: საიმედოობა, დაყოვნება, ფლუქტუაციები, გამტარუნარიანობა.

სადღეისოდ ქსელის გამოყენების მრავალი მიმართულება არსებობს; დავასახელოთ მათგან ძირითადები: ტელეფონია, ელექტრონული ფოსტა, ფაილების გადაცემა, ვებ-შედწევა, შორეული შედწევა, აუდიომომსახურება, ვიდეომომსახურება და ვიდეოკონფერენცია.

ქსელის გამოყენების თითოეულ ამ სახეს მომსახურების ხარისხის პარამეტრების მიმართ განსხვავებული მოთხოვნები ახასიათებენ: ზოგიერთის მიმართ - მეტი, ზოგიერთის მიმართ - ნაკლები. მრავალრიცხოვანი დაკვირვებების საფუძველზე შემუშავებულია მოთხოვნები ქსელის ძირითადი პარამეტრების მიმართ გამოყენების ამა თუ იმ სახის დროს. პარამეტრების მიმართ მოთხოვნების საერთო სურათი წარმოდგენილია ცხრილში №3.1.

როგორც ამ ცხრილიდან ჩანს, გამოყენების დასახელებული სახეებიდან ორიც კი არ არის ერთნაირი მოთხოვნების მქონე მიღებული ოთხი პარამეტრის მიმართ.

შეგაფასოთ, გამოყენების თითოეული სახე პარამეტრებისადმი წაყენებული მოთხოვნების კუთხით:

ტელეფონია

ტელეფონია, ანუ გარკვეულ მანძილზე ადამიანებს შორის ბგერითი ინფორმაციის გაცვლა ელექტრონული საშუალებების გამოყენებით.

მოთხოვნები პარამეტრების მიმართ ცხ. №3.1

გამოყენების სახე	საიმედოობა	დაყოვნება	ფლუქტუაციები	გამტარუნარიანობა
ტელეფონია	დაბალი	მაღალი	დიდი	დაბალი
ელექტრონული ფოსტა	მაღალი	დაბალი	მცირე	დაბალი
ფაილების გადაცემა	მაღალი	დაბალი	მცირე	საშუალო
ვებ-შედწევა	მაღალი	საშუალო	მცირე	საშუალო
შორეული შედწევა	მაღალი	საშუალო	საშუალო	დაბალი
აუდიო მომსახურება	დაბალი	დაბალი	დიდი	საშუალო
ვიდეო მომსახურება	დაბალი	დაბალი	დიდი	დიდი
ვიდეო კონფერენცია	დაბალი	მაღალი	დიდი	დიდი

ამ დროს მოთხოვნა საიმედოობის მიმართ დაბალია, ვინაიდან ადამიანის მეტყველებას დიდი სიჭარბე ახასიათებს და მომსმენი მხარე ადვილად ართმევს თავს წარმოშობილ უზუსტობებსა და ხარვეზებს ლაპარაკის მოსმენის პროცესში.

დაყოვნების მიმართ მაღალი დონის მოთხოვნები განპირობებულია იმით, რომ მისი მნიშვნელობის ზრდა იწვევს ლაპარაკის პროცესის ერთიანობის წყვეტის ხასიათს და ლაპარაკში მონაწილე მხარეებს აგდებს გაუგებრობაში: უსმენენ თუ არა ერთმანეთს, გაწყდა კავშირი თუ არსებობს და ა.შ. ასე მაგალითად, ყველა სიტყვის მოსვლა დაყოვნებით 2წმ, მომსმენისათვის უკვე ყოვლად მიუღებელი ხდება.

ფლუქტუაციების მიმართ დიდი მოთხოვნები განპირობებულია იმით, რომ ლაპარაკის პროცესში მისი მნიშვნელოვანი სიდიდე წარმოშობს ხმის დამახინჯებას და ართულებს ლაპარაკის საინფორმაციო აღქმას.

გამტარუნარიანობის მიმართ დაბალ მოთხოვნებს განაპირობებს სალაპარაკო სიგნალის სპექტრის უმნიშვნელო სიგანე, რომელიც არ აღემატება 8,0 კჰც და, შესაბამისად არ მოითხოვს დიდ გამტარებლობას.

ელექტრონული ფოსტა

ელექტრონული ფოსტა, ანუ ერთი მომხმარებლის მიერ მეორე მომხმარებლისათვის (მომხმარებელთა ჯგუფისათვის) რაიმე ინფორმაციის, ელექტრონული შეტყობინების სახით წარმოდგენილის, გადაგზავნა.

მიღებული მასალა, ჩვეულებრივად, მოღებისთანავე არ კონტროლირდება, მიმღები მხარე უშუალოდ არ შედის მომწოდებელთან არც პირდაპირ და არც ვირტუალურ კავშირში, ე. ი. არ არის მიღებული ინფორმაციის უშუალოდ დაზუსტების საშუალება, ამიტომ საიმედოობის მაღალი დონე გარანტირებული უნდა იყოს. ელექტრონული ფოსტის ფუნქციონირების პრინციპებიდან გამომდინარე დაყოვნება არ წარმოადგენს მნიშვნელოვან ფაქტორს: ქსელში იგი შეიძლება, ვთქვათ, შეადგენდეს წუთზე ნაკლებ სიდიდეს, მაშინ როდესაც მომხმარებელმა ამ ინფორმაციით შეიძლება ისარგებლოს, ვთქვათ, დღეების შემდეგ. ფლუქტუაციების ზემოქმედება, ხომ საერთოდ არ მიიღება მხედველობაში; ასევე დაბალია მოთხოვნა გამტარუნარიანობის მიმართ, ვინაიდან ინფორმაციას, როგორც წესი, წერილობითი ხასიათი აქვს და მისი შესაბამისი სიგნალების სიხშირული სპექტრი უმნიშვნელო სიგანისაა.

ფაილების გადაცემა

ფაილების გადაცემა, ანუ მომხმარებლის მიერ ქსელის საშუალებით სხვადასხვა სახის საინფორმაციო, დოკუმენტური, ლიტერატურული და სხვა სახის მასალის მიღების ორგანიზება.

ფაილების გადაცემის პროცესში საიმედოობისადმი წაყენებული მოთხოვნები მასალის ხასიათის მიხედვით მაღალია; უნდა გამოირიცხოს სათანადო ბიტების არაკორექტული მიწოდება. დაყოვნების მიმართ კი მოთხოვნა დაბალია, ვინაიდან, ჩვეულებრივად, ეს არ არის ოპერატიულად გამოსაყენებელი მასალა. შესაბამისად, ფლუქტუაციების გავლენა არ არსებობს და მათდამი მოთხოვნებიც მცირეა. მოთხოვნა გამტარუნარიანობის მიმართ საშუალო დონისაა; ალბათ, ასე უნდა ჩაითვალოს, ვინაიდან ფაილების სახით მიღებული მასალა მეტად დიდ ფარგლებში იცვლება და ზოგადი, ცალსახა შეფასება შეუძლებელია.

ვებ-შედწევა

ვებ-შედწევა, ანუ მომხმარებლის მიერ მისთვის საინტერესო მასალის მოძიება და მასთან შედწევა. ეს პროცესი საიმედოობას მაღალ მოთხოვნებს უყენებს, ქსელში სათანადო ბიტების არაკორექტული გადაცემა უნდა გამოირიცხოს, დაყოვნების

მიმართ კი მოთხოვნები არ არის მკაცრი, საშუალოა; ვებ-შედგენის დროს შესაძლებელია ფლუქტუაციების ზემოქმედების იგნორირება და, შესაბამისად, მოთხოვნებიც მცირეა; მოცულობით მასალის სიდიდე კი განაპირობებს გამტარუნარიანობისადმი წაყენებული მოთხოვნების საშუალო დონეს.

შორეული შედგენა

შორეული შედგენა, ანუ როდესაც მომხმარებელი არ არის ქსელის უშუალო აბონენტი და რაიმე გზით, მაგალითად მოდემის გამოყენებით, იღებს მომსახურებას ქსელისაგან. ასეთი მომხმარებელი, რომელიც, ასე ვთქვათ, გარედან შედის ქსელში, უზრუნველყოფილ უნდა იქნეს შესვლის დიდი საიმედოობით; დაყოვნების დრო ნაკლებად კრიტიკულია, მაგრამ მაინც მნიშვნელოვანი, ამიტომ მისთვის საშუალო დონეა მისაღები; ასევე საშუალოა ფლუქტუაციების ზემოქმედება. გამტარუნარიანობისადმი წაყენებული მოთხოვნების დაბალ დონეს განაპირობებს ამ კატეგორიის მომხმარებელთა ქსელში შედგენის აპარატურული შესაძლებლობები.

აუდიო მომსახურება

აუდიო მომსახურება, ანუ მომხმარებლის მიერ სხვადასხვა სახის აუდიო (სმენითი) ინფორმაციის არაპირდაპირი გადაცემით მიღება; ასე მაგალითად, რომელი რადიოსადგურის მიერ ადრე გადაცემული მასალის მოსმენა; რომელიმე პიროვნების საკონფერენციო გამოსვლის ჩანაწერის მოსმენა და სხვა.

ადამიანის აღქმის უნარი ლაპარაკის მოსმენის დროს მეტად მაღალია, რაც განაპირობებს ასეთი სახის მომსახურებისადმი საიმედოობის მიმართ წაყენებული მოთხოვნების დაბალ დონეს. ასევე დაბალია მოთხოვნა დაყოვნების მიმართ, ვინაიდან ეს საინფორმაციო მასალა არა პირდაპირი გადაცემით მოდის, ჩვეულებრივად, რამდენიმე საათის, რამდენიმე დღის შემდეგაც, და ასეთ პირობებში ქსელის მიერ მიღების პროცესში შეტანილი მცირე დაყოვნების როლი უმნიშვნელოა და, შესაბამისად, მოთხოვნებიც დაბალია. ფლუქტუაციების მიმართ კი მოთხოვნები დიდია, ვინაიდან აუდიო მასალას რა დაყოვნებითაც არ უნდა ვისმენდეთ, მისი სმენითი აღქმა მაინც ბუნებრივი სახით უნდა მიმდინარეობდეს და არ უნდა იწვევდეს მსმენელში გაუგებრობისა და, ზოგადად, დაუკმაყოფილებლობის შეგრძნობას. არადა, სმენითი სიგნალების აღქმისას რამდენიმე მილიწამიანი ფლუქტუაციებიც კი შესამჩნევია. რაც შეეხება გამტარუნარიანობისადმი წაყენებული მოთხოვნებს იგი სალაპარაკო სიგნალების ვიწრო სიხშირული სპექტრის გამო საშუალო დონისაა.

ვიდეო მომსახურება

ვიდეო მომსახურება, ანუ მომხმარებლის მიერ სხვადასხვა სახის ვიდეო ინფორმაციის არაპირდაპირი გადაცემით მიღება. ასეთი მომსახურება შეიძლება

მოიცავდეს, ვთქვათ, კონცერტის, საფეხბურთო მატჩის, საკარნავალო მსვლელობების და სხვა რაიმე სახის ვიდეოჩანაწერს. ზოგადად, მასალის ხასიათის მიხედვით საიმედოობისადმი წაყენებული მოთხოვნები დაბალია; ბუნებრივად გამოიყურება, აგრეთვე, დაბალი მოთხოვნები დაყოვნების მიმართ. ასე მაგალითად, თუ ყველა კადრი ორ წამიანი დაყოვნებით შემოვა, მომხმარებელი მას აღიქვამს ნორმალურად, მაგრამ თუ კადრების მიღების პროცესი მიმდინარეობს ერთი წამიდან ორ წამამდე ცვლილებების პირობებში, შედეგი აღქმის თვალსაზრისით მეტად პრობლემური გახდება. რაც შეეხება ფლუქტუაციებს, მოთხოვნები მის მიმართ დიდია, ვინაიდან მნიშვნელოვანი ფლუქტუაციებით მოსული ვიდეო მასალის ნორმალური აღქმა ან შეუძლებელია ან აღიქმება მეტისმეტად უარყოფითი ემოციონალური ფონის პირობებში. გამტარუნარიანობისადმი წაყენებული მოთხოვნები ასევე დიდია, ვინაიდან ვიდეო ინფორმაციის სიგნალები ფართო სიხშირული სპექტრით ხასიათდებიან და მათ გასატარებლად ზოლიც ფართო უნდა იყოს.

ვიდეო კონფერენცია

ვიდეო კონფერენცია, ანუ ერთმანეთისაგან გარკვეული მანძილით დაშორებული ადამიანების მონაწილეობის პროცესი კონფერენციების, შეხვედრების, გასაუბრებების და სხვა ანალოგიური სახის ღონისძიებებში.

ამ სახით რეალიზებული ღონისძიებებისათვის საიმედოობის მიმართ მოთხოვნები დაბალია, მაგრამ დაყოვნების მიმართ კი მაღალი, ვინაიდან დიდი დაყოვნება პროცესში მონაწილეთა ერთად ყოფნის ეფექტს მნიშვნელოვნად ამცირებს, შეხვედრის ბუნებრივობა ირღვევა და უარყოფითად აღიქმება.

ნებისმიერი ფლუქტუაციებით მოსული ვიდეო მასალის ნორმალური აღქმა ან შეუძლებელია ან აღიქმება მეტისმეტად უარყოფითი ემოციონალური ფონის პირობებში და, შესაბამისად, მის მიმართ მოთხოვნები დიდია. ასევე დიდია გამტარუნარიანობისადმი წაყენებული მოთხოვნები, ვინაიდან ვიდეო ინფორმაციის სიგნალები ფართო სპექტრით ხასიათდებიან და მათ გასატარებლად ზოლიც ფართო მოითხოვება.

ქსელის გამოყენების ასეთი მრავალფეროვანი მიმართულებების არსებობის პირობებში თითოეული მათგანისათვის სათანადო პარამეტრების უზრუნველყოფა მეტად რთული საქმეა. ამ მოთხოვნათა დასაკმაყოფილებლად განსხვავებული არქიტექტურით აგებული ქსელები სხვადასხვა მეთოდსა და გზას იყენებენ.

ასე მაგალითად, ფართოდ გავრცელებულ ATM (Asynchronous Transfer Mode) ქსელებში მომსახურების სათანადო ხარისხის უზრუნველსაყოფად პაკეტების ნაკადების კლასიფიკაციას ოთხი მანქანების მიხედვით ახორციელებენ:

1. ბიტების მუდმივი სიჩქარე (მაგალითად, ტელეფონია);

2. ბიტების ცვლადი სინქარე რეალურ დროში (მაგალითად, ვიდეომონაცემები ვიდეოკონფერენციის ჩატარებისას);
3. ბიტების ცვლადი სინქარე არა რეალურ დროში (მაგალითად, ფილმების ნახვის დროს);
4. ბიტების შესაძლო სინქარე (მაგალითად, ფაილების გადაცემისას).

პაკეტების ნაკადების კლასიფიკაციას მიმართავენ სხვა არქიტექტურის მქონე ქსელებშიც.

მომსახურების მაღალი ხარისხის მიღწევის მეთოდები

ზოგადად შეიძლება ითქვას, რომ არ არსებობს რაიმე უნივერსალური მეთოდი, რომელის გამოყენებაც უზრუნველყოფდა მომსახურების მაღალ ხარისხს. ამ მხრივ სპეციალისტების მიერ შემუშავებულია მრავალი მეთოდი, რომლებიც საშუალებას იძლევიან გაუმჯობესდეს ქსელის ესა თუ ის პარამეტრი. პრაქტიკული გამოყენების თვალსაზრისით მნიშვნელოვანი შედეგების მისაღწევად ხშირად მიზანშეწონილია რამდენიმე მეთოდის ერთდროული, შერწყმული გამოყენება.

ხარისხის უზრუნველყოფა სიჭარბით

ეს გზა თეორიულად ყველაზე მარტივია: გამოყენებულ იქნეს მძლავრი, დიდი ტევადობების მქონე მარშრუტიზატორები, მახსოვრობის ბლოკები და დიდი გამტარუნარიანობის მქონე არხები. ასეთი მოწყობილობებისაგან აგებულ ქსელებში პაკეტთა ნაკადები დაუბრკოლებლად გადაადგილდებიან ქსელის ერთი ბოლოდან მეორე ბოლომდე. ყველაფერი ეს ძალიან კარგია, მაგრამ იმდენად ძვირადღირებულია, რომ ქსელის ასეთი სახით წარმოდგენა მხოლოდ ვირტუალურ სამყაროში შესაძლებელია.

სპეციალისტების წინაშე, რომლებიც ქსელის სათანადო მოწყობილობადანადგარებით აღჭურვაზე მუშაობენ, დგას მეტად მნიშვნელოვანი საკითხი, დადგენილ და შემდგომ რეალიზებულ იქნეს ქსელის აუცილებელი და საკმარისი პარამეტრები; მათ შესაბამისად კი შეირჩეს სათანადო აპარატურა.

სიჭარბის თვალსაზრისით გამოირჩევა ერთერთი პირველი ტელეკომუნიკაციური ქსელი, სატელეფონო ქსელი. ამ ქსელით სარგებლობისას, მართლაც, რომ იშვიათია მოითხოვო მომსახურება (აიღო ყურმილი) და არ მიიღო მზადყოფნის სიგნალი.

სატელეფონო ქსელებში არსებული სიჭარბის დონის გავრცობა მთელ ინფორმაციულ ქსელებზე პრაქტიკულად მიუღწეველი და მიუღებელია. ამიტომ დგება სპეციალისტების წინაშე პრობლემატური საკითხი, თუ როგორი საშუალებებით იქნეს მიღწეული ქსელის აუცილებელი და საკმარისი პარამეტრები.

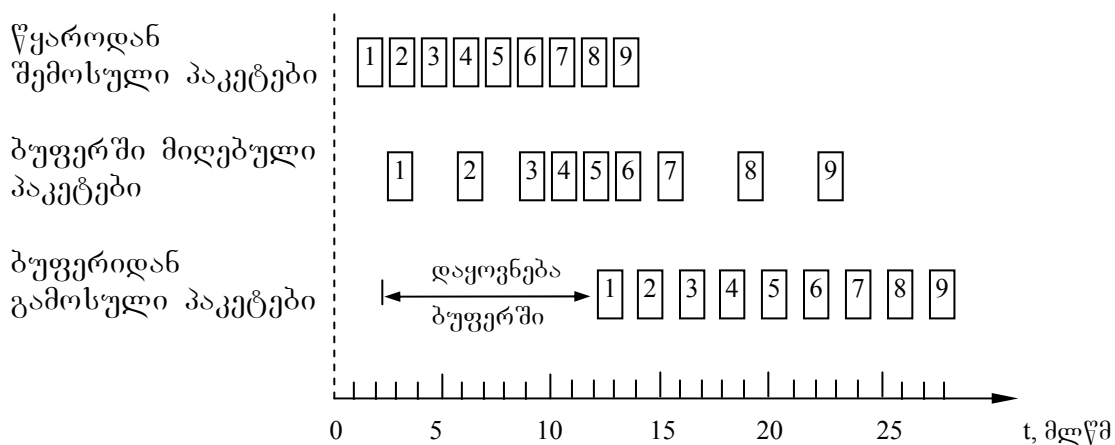
ხარისხის უზრუნველყოფა ბუფერიზაციით

ბუფერი (ინგ. buffer – შემამსუბუქებელი) ამ სიტყვის სემანტიკა თავის საფუძველში გულისხმობს დარტყმების შემსუბუქებას, მაგალითად, მატარებლის ვაგონებს შორის, მანქანების ავარიული შეჯახებების დროს და სხვა. კომპიუტერულ ტექნოლოგიებში კი ამ სიტყვის ქვეშ იგულისხმება პაკეტების ნაკადების წინასწარი განთავსება მასსოვრობის მოწყობილობებში, რათა შემდგომ მოხდეს მათი თანამიმდევრული, შექმნილ სიტუაციასთან მორგებული, დამუშავება (გაგზავნა, პროცესორისათვის გადაწოდება და სხვა).

ამგვარად, ბუფერიზაცია გულისხმობს პაკეტების ნაკადების წინასწარ განთავსებას მასსოვრობის მოწყობილობებში და შემდგომ მის მიწოდებას მომხმარებლისათვის.

ბუფერიზაცია ქსელის საიმედოობაზე და გამტარუნარიანობაზე არ ახდენს გავლენას, მაგრამ ვლინდება დაყოვნების პარამეტრის ზრდის სახით. ამავე დროს, ბუფერიზაცია საშუალებას იძლევა ზეგავლენა მოვახდინოთ ფლუქტუაციებზე, მათი შემცირების მიმართულებით. აუდიო – ვიდეო გადაცემების დროს ფლუქტუაციებს დიდი მნიშვნელობა აქვთ, ბუფერიზაცია კი საშუალებას იძლევა მოგვარდეს ეს პრობლემა.

ბუფერიზაციით ფლუქტუაციების შემცირების თვალსაჩინო მაგალითი წარმოდგენილია ნახაზზე 3.4.



ნახ. 3.4. ფლუქტუაციების შემცირება ბუფერიზაციის გზით

მომხმარებლის შეტყობინება ნახაზზე წარმოდგენილია 9 პაკეტის სახით. ეს პაკეტები ბუფერში მიღებულ იქნა დიდი ფლუქტუაციებით. გარკვეული დროის შემდეგ დაიწყო მათი ბუფერიდან ამოღება და აღწარმოება, მიუხედავად იმისა, რომ პაკეტების ნაწილი (მე-5 და შემდგომები) ჯერ კიდევ არ იყო შემოსული. შემდეგ კი

წინა პაკეტების ამოღებამდე შემდგომებიც შემოვიდნენ და საბოლოოდ გამოსული პაკეტების ნაკადმა სრულიად თანაბარი ხასიათი მიიღო.

ბუფერიზაციის მეთოდის რეალიზების დროს ძალიან მნიშვნელოვანია თუ რამდენი ხნის შემდეგ უნდა დაიწყოს ბუფერული მახსოვრობიდან პაკეტების ამოღება. თუ ბუფერიზაციის დრო დიდი იქნება, ეს მოითხოვს მისი მოცულობის მნიშვნელოვან გაზრდას, ამას გარდა დაყოვნება შეიძლება აისახოს გადაცემის ხარისხზე; თუ ამოღების დრო მცირე იქნება, მაშინ შეიძლება ვერ მოხერხდეს პაკეტების სრული ნაკადის მოცვა ბუფერიზაციის პროცესით და ეს ისევ გადაცემის ხარისხზე აისახოს.

აქედან გამომდინარე, ბუფერიზაციის დროის დადგენა უნდა განხორციელდეს დიდი ყურადღებით ქსელის მონიტორინგის მონაცემების შესაბამისად.

მაგალითის სახით დავასახელოთ ის, რომ ხშირ შემთხვევებში აუდიო-ვიდეო მომსახურების პროცესში პაკეტთა ნაკადის აღწარმოებას იწყებენ 10 მლწმინანი ბუფერიზაციის შემდეგ, როგორც ეს დაახლოებით ასეა ნაჩვენები ნახაზზე 3.4.

ამავე დროს ავლნიშნოთ, რომ ბუფერიზაციის გამოყენება ყოველთვის არ არის მისაღები, მაგალითად ვიდეოკონფერენციების ორგანიზებისას.

ზოგადად შეიძლება ითქვას, რომ როდესაც ხორციელდება ბუფერიზაციის მეთოდის რეალიზება, ეს არის ღონისძიება ჩატერებული გადაცემის ხარისხის ამაღლების მიზნით მიმღების მხარეს.

ტრაფიკის ფორმირება

გადაცემითა მაღალი ხარისხის უზრუნველყოფის ერთერთი უმნიშვნელოვანესი მეთოდია ტრაფიკის ფორმირება.

ტრაფიკის ფორმირების მეთოდი გულისხმობს პაკეტების ნაკადზე ზემოქმედებას მიმწოდებლის მხარეს.

ზოგადად ტრაფიკის ფორმირება მნიშვნელოვანწილად უზრუნველყოფს ქსელში მონაცემთა ნაკადების გათანაბრებას. არადა არათანაბარი ნაკადების არსებობა, სერვერების ფუნქციონირების რეჟიმების პირობებში, ჩვეულებრივი ამბავია ქსელში. არათანაბარი ნაკადების წარმოშობის მრავალი მიზეზი არსებობს, მაგალითად გარკვეული მასალის სწრაფი ე.წ. „გადახვევა“ და შემდეგ კი უკან დაბრუნება, მომხმარებელთა დიდი ჯგუფის სასწრაფო იდენტიფიკაცია და სხვა. ასეთ პირობებში თუ მოხერხდება მონაცემთა ნაკადების მეტ-ნაკლებად გათანაბრება შედეგად მივიღებთ მომსახურების ხარისხის ამაღლებას.

მონაცემთა ნაკადების გათანაბრებას ემსახურება ტრაფიკის ფორმირების მეთოდი.

ტრაფიკის ფორმირების მეთოდი გულისხმობს მიმწოდებლისა და ქსელის ოპერატორის შეთანხმებას ორივესათვის მისაღები დატვირთვების (მონაცემთა ნაკადების) შესახებ. ამ შეთანხმებების საფუძველზე შესაძლებელი ხდება მონაცემების გადაცემის საშუალო და პიკური მნიშვნელობების დარეგულირება, საერთო დატვირთვის გათანაბრება ქსელში.

ტრაფიკის ფორმირების ფარგლებში მონაცემთა ნაკადების გათანაბრების მიზნით შემუშავებულია რამდენიმე ალგორითმი. განვიხილოთ ორი მათგანი, რომლებიც ცნობილია საკმაოდ ორგინალური სახელებით:

1. ნახვრეტიანი ვედროს ალგორითმი;
2. მარკერიანი ვედროს ალგორითმი.

სიტყვა „მარკერი“ წადმოდგება ფრანგულისაგან *marguer* – მონიშვნა. აქედან გამომდინარე მეორე ალგორითმის სახელი ქართულად ასეთ სახეს მიიღებდა: „მონიშვნებიანი ვედროს ალგორითმი“.

ამ ალგორითმების ავტორია ამერიკელი სპეციალისტი ტერნერი (Turner,1986).

ქსელში მონაცემთა ნაკადების მოძრაობის ალგორითმისთვის ასეთი სახელის შერჩევა განპირობებულია ამ ალგორითმის მოქმედების პრინციპის გარკვეული მსგავსებით წყლიანი ძირგახვრეტილი ვედროდან წყლის ნაკადის გამოსვლის პროცესთან.

თუ ავიღებთ გახვრეტილ ვედროს და დავიწყებთ წყლით მის შევსებას, ნახვრეტიდან წყალი დაიწყებს გამოდენას თანაბარი ნაკადის სახით (ცხადია, ნახვრეტის მცირე დიამეტრის პირობებში). ასე გაგრძელდება მანამ, სანამ წყალი არ გადაავსებს ვედროს, შემდეგ კი წყალი დაიწყებს დაღვრას. თუ წყლის ჩასხმა შეწყდება, ვედროში მყოფი წყალი ჩამოიცილება წვრილი ნაკადის სახით; ვედრო მზად იქნება კვლავ აივსოს წყლით და იგივე პროცესი გაიმეოროს.

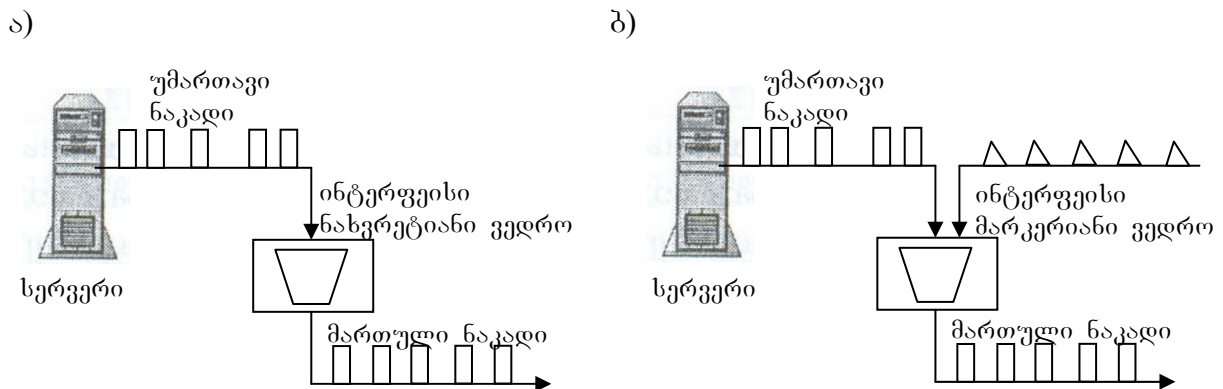
ქსელში ნახვრეტიანი ვედროს ალგორითმის რეალიზების სურათი ასეთი სახით შეიძლება წარმოვიდგინოთ (ნახ. 3.5ა): სერვერი, რომელიც ამუშავებს დიდი მოცულობის საინფორმაციო მასალას, გარკვეული ინტერფეისით დაკავშირებულია ქსელის დანარჩენ ნაწილთან. ამ ინტერფეისში ხორციელდება ნახვრეტიანი ვედროს ალგორითმის რეალიზება. ინტერფეისში არათანაბარ ნაკადად შემოსული ბიტების ერთობლიობა თანაბარ ნაკადად ტოვებს მას.

ამგვარად, ინტერფეისის შესავალზე მიღებული უმართავი ნაკადი მართული ნაკადის სახით მიიღება მის გამოსავალზე. ნაკადის მართვა მიმდინარეობს წინასწარ დადგენილი ტაქტის მიხედვით.

ინტერფეისს, პირობითად ვედროს, გარკვეული ტევადობა გააჩნია. ნახვრეტიანი ვედროს ალგორითმის რეალიზების პროცესში შესაძლებელია ამ

ტევადობის გადასება, რაც პაკეტების ნაწილის დაკარგვის (იგნორირების) მიზეზი გახდება. იგნორირებული პაკეტები შემდეგში მოიძიება, კვლავ გადაიცემა, მაგრამ ყველაფერი ეს ნეგატიური მაჩვენებელია ქსელის ფუნქციონირებისათვის. ასე რომ გადატვირთვებისაგან თავის დაზღვევა პაკეტების იგნორირებით შექმნილი მდგომარეობიდან არასასურველ, იძულებით გამოსავალს წარმოადგენს.

აქედან გამომდინარე, ნახვრეტიანი ვედროს ტევადობის შერჩევა ხორციელდება ქსელის მონიტორინგის საფუძველზე და იმის მაქსიმალური გათვალისწინებით, რომ რაც შეიძლება ნაკლები ალბათობით მოხდეს პაკეტების იგნორირება.



ნახ. 3.5. ნახვრეტიანი და მარკერიანი ვედროების ალგორითმების სურათი

ინტერფეისი, რომელიც ახორციელებს ნახვრეტიანი ვედროს ალგორითმის რეალიზებას, შეიძლება წარმოადგენდეს დამოუკიდებელ მოწყობილობას. ასევე შესაძლებელია ნახვრეტიანი ვედროს ალგორითმის რეალიზება სერვერის ოპერაციული სისტემის სათანადო პროგრამული აღჭურვილობით.

ამგვარად, ნახვრეტიანი ვედროს ალგორითმის რეალიზების ორი გზა არსებობს: აპარატურული საშუალებებით ან პროგრამულად.

საბოლოოდ ვიღებთ, რომ ნახვრეტიანი ვედროს ალგორითმი, მიუხედავად შემოსული მონაცემთა ნაკადების მრავალფეროვნებისა, გამოსავალზე მკაცრად გათანაბრებული ნაკადების შექმნას უზრუნველყოფს.

ქსელის ოპტიმალურ რეჟიმში მუშაობისათვის ნახვრეტიანი ვედროს ალგორითმი ყოველთვის არ არის სასურველი. ქსელის გამოყენების ზოგიერთი სახისათვის უკეთესი იქნებოდა გამოსავალი ნაკადის ფორმირება არ მომხდარიყო ისეთი სიმკაცრით, როგორც ეს ხდება ნახვრეტიანი ვედროს ალგორითმის რეალიზების დროს. ამან მოითხოვა უფრო მოქნილი ალგორითმის შექმნა. ასეთ ალგორითმს წარმოადგენს მარკერიანი ვედროს ალგორითმი (ნახ. 3.5ბ). ამ ალგორითმში სპეციალური სიგნალი – მარკერი – არეგულირებს ნაკადების გამოსვლას ვედროდან. პროცესი, რომელიც მიმდინარეობს მარკერიან ვედროში,

იძლევა იმის საშუალებას, რომ დასაწყისში, ანუ როცა ვედრო ჯერ კიდევ ცარიელია, გამოსავალი სინქარე გაიზარდოს, შემდეგ კი მოხდეს მისი მორგება შექმნილ სიტუაციასთან. პროცესის ამ სახით წარმართვის დროს უფრო დიდი ნაკადების მომსახურება ხდება შესაძლებელი, ვიდრე ნახვრეტიანი ვედროს ალგორითმის გამოყენების დროს. ეს კი ქსელის ფუნქციონირების პოზიტიური მაჩვენებელია.

ქსელის ტრაფიკის მართვა ნახვრეტიანი და მარკერიანი ვედროების ალგორითმების საფუძველზე ამცირებს გადატვირთვების წარმოშობის შესაძლებლობებს და ოპერატორს საშუალებას აძლევს უფრო მაღალ დონეზე მოემსახუროს მომხმარებელს.

დასკვნის სახით ავლნიშნავთ, რომ ბუფერიზაცია და ტრაფიკის მართვა მნიშვნელოვანი ნაბიჯებია მომსახურების გარანტირებული ხარისხის მიღწევის გზაზე.

3.4. ქსელის მონიტორინგი

ზოგადი მიმოხილვა

ქსელის მართვა რთული და მრავალფეროვანი პროცესია. მის ერთერთ მნიშვნელოვან ასპექტს წარმოადგენს ქსელის მონიტორინგი. იგი მიზნად ისახავს ქსელისათვის გარკვეული კანონზომიერებით თვალყურის დევნებას მისი პარამეტრებისა და მასში მიმდინარე პროცესების სრული სურათის წარმოსადგენად.

მონიტორინგის განხორციელება ხელს უწყობს ქსელში პრობლემების წარმოშობის თავიდან აცილებას, ხოლო მათი წარმოშობის შემთხვევებში დროულ აღმოფხვრას.

ცხადია, რომ ქსელის მომსახურების საუკეთესო გადაწყვეტილებაა ისეთი ღონისძიებების გატარება, რომლებიც პრობლემების წარმოშობის შესაძლებლობას მოსპობენ. ასევე ცხადია, რომ პრობლემების საერთოდ გამორიცხვაც პრაქტიკულად მიუღწეველია.

ზოგადად ქსელში პრობლემების თავიდან აცილებას შემდეგი ღონისძიებების გატარება უზრუნველყოფს:

- დაგეგმვა;
- მონიტორინგი;
- მომხმარებელთა სწავლება;
- „ვიწრო ადგილთა“ დადგენა და შემდგომ მათი აღმოფხვრა;
- ქსელის შესაძლებლობების შეთანხმება მის წინაშე დასმულ ამოცანებთან;
- რეგულარული სარეზერვო კოპირება;

- მონაცემების არსებობა სპეციალისტთა იმ კატეგორიის შესახებ, რომელთაც შეუძლიათ ქსელის პრობლემების მოგვარება.

საერთოდ, ქსელის პრობლემების თავიდან აცილება, ხოლო წარმოშობის შემთხვევაში მათი დროული აღმოფხვრა, წარმატებითაა შესაძლებელი თუ დაგეგმვისა და მონიტორინგის ღონისძიებები ქსელის ადმინისტრატორისა და სისტემური ინჟინერის მიერ მიზანდასახულად და სწორად არის რეალიზებული.

აქ შენიშვნის სახით ავლნიშნავთ, რომ მოსხენებული „ქსელის ადმინისტრატორი და სისტემური ინჟინერი“, ნათქვამია ზოგადად, რეალურად ქსელის ფუნქციონირებას შეიძლება წარმართავდნენ საადმინისტრაციო და სისტემურ ინჟინერთა სხვადასხვა შემადგენლობისა და კვალიფიკაციის ჯგუფები. რაც დამოკიდებულია ქსელის სირთულესთან და მის წინაშე დასმული ამოცანების სირთულესთან.

შემდგომშიც გამოთქმა „ქსელის ადმინისტრატორი და სისტემური ინჟინერი“ ამ გაგებით იქნება გამოყენებული.

თუ ქსელის ფუნქციონირება წარმატებით არის ორგანიზებული, მაშინ მომხმარებლისათვის ადმინისტრატორისა და სისტემური ინჟინერის მოქმედებები არც კი შეიმჩნევა.

საქსელო პრობლემების მოგვარება ორი პოზიციიდან უნდა განხორციელდეს:

- პრობლემების თავიდან აცილება დაგეგმვისა და მართვის მეთოდებით;
- წარმოშობილი პრობლემების მოგვარება შესაბამისი სპეციალისტების ოპერატიული ჩარევით.

ქსელის მართვა და პრობლემათა მოგვარება მისი ფუნქციონირების საერთო გეგმის შემადგენელი ნაწილებია. ეს გეგმა კი უნდა იცვლებოდეს ქსელში მიმდინარე შიდა ცვლილებებთან და ქსელის გაფართოებასთან ერთად.

ქსელის ფუნქციონირების საერთო გეგმის ძირითადი ნაწილებია:

- საკაბელო სისტემის სქემები;
- ქსელის გამტარუნარიანობის პარამეტრები;
- პროტოკოლები;
- მოწყობილობა - დანადგარების სტანდარტები;
- მოთხოვნათა და განვითარების პროგნოზები.

პრობლემების თავიდან აცილება დაგეგმვის საშუალებით

პოლიტიკა და პროცედურები, რომლებმაც უნდა უზრუნველყონ პრობლემების თავიდან აცილება, განსაზღვრულ უნდა იქნენ ქსელის დაგეგმვის საწყის სტადიაში.

პოლიტიკისა და პროცედურების ელემენტებს მიეკუთვნება:

- სარეზერვო ასლის გადაღება;

- უსაფრთხოება;
- უნიფიკაცია;
- მოდერნიზაცია;
- დოკუმენტაცია.

სარეზერვო ასლის გადაღება

ქსელში პრობლემების თავიდან აცილების ერთერთი მნიშვნელოვანი გზაა სარეზერვო კოპირების ორგანიზება. ეს საკმაოდ ძვირადღირებული ღონისძიებაა, მაგრამ მისი რეალიზება ყოველმხრივ გამართლებულია. დაკარგული ინფორმაციის აღდგენა შესაძლებელიც რომ იყოს, მაინც გაცილებით მეტ ხარჯებთან არის დაკავშირებული, ვიდრე კოპირების ორგანიზება.

უსაფრთხოება

ქსელში უსაფრთხოების უზრუნველყოფა, ძირითადად, ხორციელდება სერვერებთან შედწევის მეთოდების ზედმიწევნითი დამუშავების გზით, რათა გამოირიცხოს ქსელში არსებული ინფორმაციის არასანქციონირებული გამოყენება.

ქსელში უსაფრთხოების უზრუნველყოფის პოლიტიკა რამდენიმე ფაქტორზეა დამოკიდებული, რომელთაგან აღსანიშნავია:

- ქსელის განთავსების არეალის ზომები – ტერიტორია;
- ქსელის მიერ დამუშავებული ინფორმაციის მნიშვნელობის ხარისხი;
- გარემო, რომელშიც ქსელი ფუნქციონირებს.

ქსელში უსაფრთხოების უზრუნველყოფა ადმინისტრატორის ერთერთი უმნიშვნელოვანესი ამოცანაა და მან უნდა გაატაროს ყველა ღონისძიება მისი მაღალი ღონის მისაღწევად.

უნიფიკაცია

უნიფიკაცია, ანუ ქსელში ფუნქციონირებადი მოწყობილობა - დანადგარების მაქსიმალური ერთსახოვნება, აადვილებს და ამარტივებს როგორც მის მართვას, ასევე რემონტსა და მოდერნიზაციას. აქედან გამომდინარე, ქსელის დაგეგმვის დროს მიღწეულ უნდა იქნეს უნიფიკაციის მაღალი დონე და იგი უნდა გადაწყდეს ადმინისტრატორისა და სისტემური ინჟინერის აქტიური მონაწილეობით.

მოდერნიზაცია

მოდერნიზაცია ქსელის ფუნქციონირების უმნიშვნელოვანესი ასპექტია. იგი პრაქტიკულად უწყვეტად მიმდინარე პროცესია. ჯერ ერთი, ხორციელდება არსებული მოწყობილობა – დანადგარების შეცვლა, მეორეც იცვლება ქსელის პროდუქტი; საერთო ცვლილებას განიცდის მომსახურების სფეროები.

აქედან გამომდინარე, მოდერნიზაციის პროცესი დიდ ყურადღებას მოითხოვს: ერთი მხრივ, დროზე უნდა მოხდეს მისი დაგეგმვა, მეორე მხრივ, ის ისე უნდა

განხორციელდეს, რომ მომხმარებლისათვის ხელშეშლისა და შეფერხების მიზეზად არ იქცეს. ქსელთან დაკავშირებით მიუღებელია, მაგალითად ასეთი მიდგომა: „მოდერნიზაციასთან დაკავშირებით ქსელი დროებით წყვეტს მუშაობას.“

მოდერნიზაციის პროცესში შემუშავებული ახალი ვერსიის ტესტირება მიზანშეწონილია განხორციელდეს მომხმარებელთა შეზღუდული ჯგუფისათვის და მისი ეფექტურობის დადასტურების შემდეგ მოხდეს მისი გავრცობა მთელ ქსელზე.

ამგვარად, მოდერნიზაცია ქსელის ეფექტური და საიმედო ფუნქციონირების მაჩვენებელია და მისი რეალიზაცია უნდა მიმდინარეობდეს ზედმიწევნით გააზრებულ და დახვეწილ სიტუაციაში.

დოკუმენტაცია

ქსელში დოკუმენტაციის წარმოება მნიშვნელოვანი პროცესია. იგი დიდი ზედმიწევნით უნდა ხორციელდებოდეს, მასზე გაწეული ხარჯები ყოველთვის მრავალჯერადად იქნება გამოსყიდული.

ქსელში წარმოშობილი პრობლემების მოგვარების უმნიშვნელოვანესი ფუნდამენტია დოკუმენტაციის მაღალხარისხოვანი წარმოება. დოკუმენტაციამ უნდა უზრუნველყოს, თუ როგორი კონფიგურაციით ფუნქციონირებს ქსელი მოცემულ მომენტში, რა რესურსები გააჩნია მას და როგორია მისი ფუნქციონირების პერსპექტივა.

ქსელის დოკუმენტაცია უნდა შეიცავდეს:

- ქსელის სრულ სქემას, მოწყობილობებისა და კაბელების ჩვენებით;
- ინფორმაციას დაკავშირებულს სერვერებთან – განლაგება, შესაძლებლობა;
- ინფორმაციას პროგრამული უზრუნველყოფის შესახებ;
- მონაცემებს მწარმოებლების, მომწოდებლებისა და სხვათა შესახებ;
- ქსელის ფუნქციონირებასთან დაკავშირებული ყველა დოკუმენტის ასლს;
- ჩანაწერებს დაკავშირებულს ქსელში პრობლემურ საკითხებთან, მათი მოგვარების გზების ჩვენებით და სათანადო პერსონალის მონაცემებით.

ზოგადად საჭიროა აღინიშნოს, რომ დოკუმენტაცია უნდა იყოს სრული, მოწესრიგებული და ადვილად ხელმისაწვდომი.

ქსელის მონიტორინგის უტილიტები

მონიტორინგის მაღალხარისხიანი პროგრამები საშუალებას იძლევიან დროულად გადაწყდეს პრობლემები და არ იქნეს დაშვებული ქსელის მტყუნება.

ამ მიზნით საქსელო ოპერაციულ სისტემებში ჩაშენებულია ქსელის მონიტორინგის სპეციალური უტილიტები. ისინი საშუალებას იძლევიან ქსელი გაკონტროლდეს უწყვეტ რეჟიმში და პრაქტიკულად მის ფუნქციონირებაზე ყოველგვარი ზემოქმედების გარეშე.

ამ პროცესებში გამოიყენება:

- მოვლენათა ჟურნალი, რომელშიც რეგისტრირებულია შეცდომები, მოქმედებები და სიტუაციები, დაკავშირებული ქსელის ფუნქციონირების პრობლემურ საკითხებთან;
- ქსელის რესურსებთან შეღწევის სტატისტიკური მონაცემები: ვინ და როგორ იყენებს მათ;
- მწარმოებლობის სტატისტიკა, რომელიც პროცესორების დატვირთვას, სერვერების გამტარუნარიანობასა და მახსოვრობის მოწყობილობების მდგომარეობას ასახავს.

ეტალონური გრაფიკი

ცოდნა იმისი, თუ როგორ მუშაობს ქსელი ნორმალურ რეჟიმში, ისევე მნიშვნელოვანია, როგორც წარმოშობილი პრობლემების მოგვარების საკითხი. სწორედ ქსელის ნორმალურ რეჟიმში ფუნქციონირების ცოდნაა ერთერთი ხელშემწყობი პირობა პრობლემების უმტკივნეულოდ მოგვარებისათვის.

მონიტორინგი საშუალებას იძლევა შემუშავებულ იქნეს ქსელის ფუნქციონირების ეტალონური გრაფიკი, რომელიც ასახავს ქსელის ფუნქციონირებას ნორმალურ რეჟიმში.

კრიტიკულ სიტუაციაში ხორციელდება ქსელის მოცემული მომენტის პარამეტრების შედარება ეტალონური გრაფიკის მონაცემებთან. მიმდინარე მახასიათებლებისა და ეტალონური მაჩვენებლების შედარება კი აადვილებს ვიწრო ადგილების გამოვლენას და შემდგომ იმ ღონისძიებების დასახვას, რომლებიც კრიტიკული სიტუაციის დაძლევის უზრუნველყოფენ.

ეტალონური გრაფიკი, რომელიც იქმნება ქსელის კორექტული, ნორმალური მუშაობის რეჟიმის დროს საშუალებას იძლევა განისაზღვროს:

- ქსელის სადღეღამისო დატვირთვის მახასიათებელი;
- სუსტი, ანუ ვიწრო ადგილები;
- ცალკეული მომხმარებლის მიერ ქსელის გამოყენების მაჩვენებელი;
- საქსელო პროტოკოლების გამოყენების ტრაფიკი.

ეტალონური გრაფიკის ანალიზი გვიჩვენებს მთელი სისტემის ფუნქციონირების სურათს და შესაბამისად საშუალებას იძლევა გაკეთდეს დასკვნა, მაგალითად:

- ქსელის სეგმენტებად დაყოფის აუცილებლობის შესახებ;
- საქსელო სერვერების რაოდენობასთან დაკავშირებით;
- საქსელო ადაპტერების მოთხოვნებთან შესაბამისობის მიმართ;
- ქსელის გარკვეულ უბანზე გამტარუნარიანობის გაზრის შესახებ.

დასკვნის სახით, შეიძლება ითქვას, რომ მონიტორინგის მიზანდასახული და ტექნიკურად გამართლებული წარმართვა ქსელის ეფექტური ფუნქციონირების

მძლავრი იარაღია; მის ორგანიზებაზე გაწეული ხარჯები გამართლებულია და იგი ყოველთვის გამოისყიდის თავისთავს.

3.5. საქსელო პრობლემების მოგვარება

ზოგადად პრობლემების შესახებ

მიუხედავად იმისა, თუ რამდენად დახვეწილი გეგმა იქნება შედგენილი, კარგად მოფიქრებული მონიტორინგი იქნება რეალიზებული და წარმატებული მხარდაჭერა იქნება ორგანიზებული, ქსელში პერიოდულად მაინც წამოიჭრება პრობლემური საკითხები და, ცხადია, ისინი უნდა მოგვარდნენ.

პრობლემების მოგვარება კი, პირველ რიგში, ქსელის ადმინისტრატორისა და სასისტემო ინჟინერის საქმიანობის პრიორიტეტული ამოცანაა.

იმისთვის, რომ ქსელის ადმინისტრატორმა და სასისტემო ინჟინერმა წარმატებით გაართვან თავი პრობლემური საკითხების მოგვარებას რეკომენდირებულია მისადმი ე. წ. სტრუქტურული მიდგომის განხორციელება.

სტრუქტურული მიდგომა

პრობლემატური საკითხების მიმართ სტრუქტურული მიდგომა გულისხმობს ამოცანების გარკვეულ ჯგუფებად წარმოდგენას და მათი თანამიმდევრობით მოგვარებას.

მიღებულია სტრუქტურული მიდგომის ხუთ ნაბიჯად წარმოდგენა:

1. პრობლემის პრიორიტეტის დადგენა;
2. ინფორმაციის შეგროვება მტყუნებათა სიმპტომების გამოსავლენად;
3. მტყუნებათა მიზეზების ჩამონათვალის შემუშავება;
4. პრობლემის იზოლაცია;
5. შემოწმების შედეგების ანალიზი გადაწყვეტილების მისაღებად.

პრიორიტეტის დადგენა

ზოგადად, ნებისმიერი პრობლემა არასასურველია და მოითხოვს მოგვარებას, მაგრამ ყოველთვის არსებობს პრობლემათა სახეები, რომელებიც პირველ რიგში უნდა მოგვარდნენ. დაუშვათ, მოცემულ მომენტში წარმოშობილი პრობლემების ნაწილი ეხება მომხმარებელთა გარკვეული ჯგუფის მომსახურებას, ნაწილი კი ქსელის გარკვეული სეგმენტის საიმედო ფუნქციონირებას. ასეთ სიტუაციაში პრიორიტეტულად, ალბათ, მიჩნეულ უნდა იქნეს ქსელის სეგმენტის ნორმალური ფუნქციონირების უზრუნველყოფა.

ცხადია, წარმოშობილი ყველა პრობლემა ერთდროულად ვერ მოგვარდება, ამისთვის საკმარისი არც ტექნიკური და არც ადამიანური რესურსი არ იარსებებს.

აქედან გამომდინარე, საჭიროა პრიორიტეტების წინასწარი დადგენა და შემდგომ მის შესაბამისად მოქმედება.

ინფორმაციის შეგროვება

ინფორმაციის შეგროვება ფუნდამენტია პრობლემათა მოგვარების საკითხში. ინფორმაცია უნდა მოიცავდეს ყველაფერს დაკავშირებულს ქსელის ფუნქციონირებასთან დაკავშირებით, როგორც ნორმალურ, ასევე ექსტრემალურ რეჟიმში. ასევე უნდა მოიცავდეს მასალებს ადრე წარმოშობილი პრობლემების შესახებ, მათი აღმოფხვრის მიზნით განხორციელებული ღონისძიებების ჩვენებით.

საქსელო სამსახურებრივი ინფორმაციის მნიშვნელოვან ნაწილს შეადგენს მომხმარებლების გამოკითხვით მიღებული ინფორმაცია. ეს საშუალებას იძლევა გამოვლინდეს პრობლემის სიმპტომები და შემდგომ დაისახოს სათანადო ღონისძიებები მათი არ წარმოშობის მიზნით.

მაგალითისათვის განვიხილოთ ასეთი სიტუაცია:

მომხმარებლებს ეძლევათ შეკითხვა: „ ხომ არ შეიმჩნება რაიმე უწყესიერობა?“

მიღებულ იქნა პასუხები:

- ქსელი შედარებით ნელა მუშაობს;
- მიჭირს სერვერთან დაკავშირება;
- სერვერთან კავშირი ხშირად მიწყდება;
- შეუძლებელია მასალების ამობეჭდვა;

ასეთი სახით მიღებული პასუხები ქსელის ადმინისტრატორსა და სასისტემო ინჟინერს საშუალებას აძლევს უკეთ წარმოიდგინონ ქსელში მიმდინარე პროცესები და მათზე სათანადო რეაგირება მიახდინონ.

ქსელის დაყოფა სეგმენტებად

ქსელის ადმინისტრატორმა და სასისტემო ინჟინერმა წარმოსახვით უნდა დაჰყონ ქსელი სეგმენტებად და წარმოშობილი პრობლემები ამ სეგმენტების მიმართ განიხილონ. განსახილველ სეგმენტში კი შემოწმებას უნდა დაუქვემდებარონ მისი ნებისმიერი კომპონენტი: ადაპტერები, კონცენტრატორები, სერვერები, დამაკავშირებელი მოწყობილობა-დანადგარები (კაბელები, კონექტორები, გამმეორებლები, ბოგირები, მარშრუტიზატორები და სხვა).

განსაკუთრებული ყურადღება უნდა მიექცეს საქსელო პროტოკოლების მდგომარეობას. ზოგ შემთხვევაში მათი არადაამაკმაყოფილებელი ფუნქციონირება შეიძლება არ იყოს თვალშისაცემი. ასე მაგალითად, ბევრ პროტოკოლში ჩადებულია მისი მოქმედების ასეთი ალგორითმი: წარუმატებელი ოპერაცია გაიმეოროს დადებითი შედეგის მისაღწევად. ეს მომენტი, ერთი მხრივ მისაღებია, ვინაიდან მოცემული კონკრეტული ამოცანის წარმატებით გადაწყვეტის საშუალებას იძლევა, მაგრამ

მეორე მხრივ, ანელებს ერთიანად ქსელის ფუნქციონირების სინქარეს. ამის გამო აუცილებელია გამოვლენილ იქნეს პროტოკოლის პირველ ცდაზე წარუმატებელი შედეგის მიზეზი და მოხდეს მისი აღმოფხვრა.

მტყუნებათა მიზეზების ჩამონათვალის შემუშავება

პრობლემურ სიტუაციაში მტყუნებათა მიზეზების სწრაფი და ყოველმხრივი გააზრება ქსელის ადმინისტრატორისა და სასისტემო ინჟინერის მიერ პრაქტიკულად წარმოდგენილია, ამიტომ აუცილებელია მათი ჩამონათვალის წინასწარი შემუშავება და საჭიროების შემთხვევაში მათზე თვალის გადავლება.

ჩამონათვალის წარმატებით გამოყენების შესაძლებლობას მნიშვნელოვნად ამაღლებს თუ მისი რიგი შედგენილია მიზეზთა ალბათობის გათვალისწინებით: მეტად ალბათები თავში და ნაკლებად ალბათები ბოლოში.

პრობლემის იზოლაცია

პრობლემის იზოლაცია გულისხმობს იმ მიზეზთა გამოყოფას, რომელთა არსებობა უფრო მეტადაა მოსალოდნელი და მათზე რეაგირების მოხდენას. თუ შედეგი არ აღმოჩნდება მისაღები, მხოლოდ მაშინ გადასვლა სხვა მიზეზებზე.

შემოწმების შედეგების ანალიზი

შემოწმების შედეგების ანალიზის პროცესში უდიდეს როლს თამაშობს ქსელის ადმინისტრატორისა და სასისტემო ინჟინერის გამოცდილება და ინტუიცია. თუ მათი ძალისხმევით აღდგენილ იქნება პრობლემური მთელი ქსელის თუ მისი რომელიმე კვანძის ნორმალური ფუნქციონირება, ეს იმის მაჩვენებელია რომ ქსელს მაღალი კვალიფიკაციის პერსონალსაერთოლი ემსახურება და საერთოდ პრობლემებიც ნაკლები იქნება.

პრობლემების მოგვარებაში აქტიურად შეიძლება ჩართულ იყვნენ ქსელის სხვა სპეციალისტებიც, დაკავშირებულნი მისი ფუნქციონირების ამა თუ იმ ასპექტთან. რომელთა რეკომენდაციებმაც შეიძლება უზრუნველყონ წარმოშობილ პრობლემათა გადაწყვეტა.

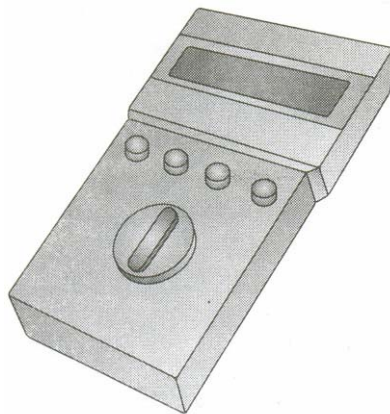
ზოგადად კი უნდა ითქვას, რომ რთულ ქსელებში იმდენად დიდი და მრავალფეროვანი პრობლემები წარმოიქმნება, რომ მათ გადასაწყვეტად ამ დარგის უმაღლესი რანგის სპეციალისტების ჩარევაც კი ხდება საჭირო, ხშირ შემთხვევებში ახალი თეორიული და ინჟინრული გადაწყვეტილებების მიღებით.

საერთო და სპეციალური დანიშნულების გამზომი საშუალებები

საქსელო პრობლემების მოგვარება მარტივდება სათანადო ტექნიკური საშუალებების გამოყენებით. მოკლედ დავახასიათოთ ზოგიერთი მათგანი:

რეფლექტომეტრი

რეფლექტომეტრი საშუალებას იძლევა აღმოჩენილ იქნეს კაბელის გაწყვეტის ადგილი, ასევე დადგენილ იქნეს კაბელის ამა თუ იმ უბანზე იზოლაციის გაუარესების სურათი. ეს მოწყობილობა მასთან დაკავშირებულ კაბელში აგზავნის სპეციალურ იმპულსურ სიგნალს. ეს სიგნალი აირეკლება კაბელის არაერთგვაროვნებებიდან. რეფლექტომეტრი აანალიზებს მიღებულ არეკლილ სიგნალებს, ადგენს მანძილებს მათი არეკვლის ადგილებამდე და იძლევა გაზომვის შედეგებს. მაღალი ხარისხის რეფლექტომეტრი კაბელის გაწყვეტის ადგილს საზღვრავს რამდენიმე დეციმეტრის (მეტრზე ნაკლები) სიზუსტით.



ნახ. 3.6. რეფლექტომეტრი

რეფლექტომეტრები საშუალებას იძლევიან განხორციელდეს როგორც ელექტრული, ასევე ოპტიკურ-ბოჭკოვანი კაბელების ტესტირება.

სპეციალური საკაბელო ტესტერი

სპეციალურ საკაბელო ტესტერები ასახავენ კაბელის ფიზიკურ მდგომარეობას და უჩვენებენ:

- კადრების რაოდენობას;
- კოლიზიების მდგომარეობას;
- შეცდომების შემცველ კადრთა რაოდენობას;
- გადატვირთვას;
- მონიშნის (მარკერის) გაშვებას.

ამ ტესტერების საშუალებით შესაძლებელი ხდება ტრაფიკის თვალყურის დევნება და ქსელის ადმინისტრატორისა და სისტემური ინჟინრის ინფორმირება ქსელში მიმდინარე პროცესებთან დაკავშირებით.

ქსელის მონიტორი

ქსელის მონიტორი – ეს საპროგრამო-სააპარატო მოწყობილობაა, რომელსაც შეუძლია ასახოს მთელი ქსელის ან მისი რომელიმე უბნის სრული ტრაფიკი. ასევე

აკონტროლოს პაკეტების გავლა, შეცდომები მათ გადატანაში; აღრიცხოს კომპიუტერების მიერ გადაცემული პაკეტების რაოდენობა.



ნახ. 3.7. საპროგრამო-სააპარატო მოწყობილობა - ქსელის მონიტორი

პროტოკოლების ანალიზატორი, იგივე საქსელო ანალიზატორი

პროტოკოლების ანალიზატორი, იგივე საქსელო ანალიზატორი – ეს ქსელის მომსახურების უმნიშვნელოვანესი ხელსაწყოა. ეს ხელსაწყოები ფართო მასშტაბიანი ქსელების ადმინისტრატორებისა და სისტემური ინჟინრების ძირითად სამუშაო ინსტრუმენტებს წარმოადგენენ.

პროტოკოლების ანალიზატორი, იგივე საქსელო ანალიზატორი, ქსელის ინტერაქტიური მონიტორინგის მძლავრი იარაღია.

პროტოკოლების ანალიზატორი, იგივე საქსელო ანალიზატორი, იკვლევს ქსელის პრაქტიკულად ყველა მაჩვენებელს, ასახავს მის რეალურ მდგომარეობას და აგროვებს სტატისტიკურ მასალას.

საქსელო ანალიზატორის კონტროლის არე მოიცავს:

- საკაბელო სისტემას;
- საპროგრამო უზრუნველყოფას;
- ფაილების სერვერებს;
- მუშა სადგურებს, იგივე კლიენტებს;
- საინტერფეისო მოწყობილობებს.

საქსელო ანალიზატორი, როგორც წესი, თავის შემადგენლობაში შეიცავს რეფლექტომეტრს და სწავლობს რა ქსელის მდგომარეობას საშუალება აქვს აღმოაჩინოს:

- ქსელის დაზიანებული კომპონენტები;
- ვიწრო ადგილები;
- ტრაფიკის გადახრები;

- უწესიერობები დაკავშირებული პროტოკოლებთან და მრავალი სხვა ფაქტორი, რომელიც ქსელის ფუნქციონირების სხვადასხვა ასპექტს განსაზღვრავს.

მოვიყვანოთ ასეთი მაგალითი, საქსელო ანალიზატორმა შეიძლება გამოავლინოს ის მომხმარებელი, რომელიც განსაკუთრებული ინტენსივობით იყენებს საქსელო რესურსებს და სხვათა მუშაობის შემაფერხებელი ხდება. ამ მონაცემებზე დაყრდნობით ქსელის ადმინისტრატორმა და სისტემურმა ინჟინერმა შეიძლება გაატარონ ღონისძიება ამ მომხმარებლის ქსელზე უარყოფითი ზემოქმედების აღმოფხვრის მიზნით: გარკვეულ წილად შეცვალონ ქსელის კონფიგურაცია მოცემული მომხმარებლის მოთხოვნათა გათვალისწინებით ან იგი გადართონ სხვა ნაკლებად დატვირთულ სერვერებზე.

თანამედროვე ანალიზატორები წარმატებით ართმევენ თავს ყველა ზემოთ მოყვანილ და კიდევ მრავალ სხვა ამოცანას.

ტიპური პრობლემები

პრობლემები, რომლებიც წამოიჭრებიან ქსელში მრავალ ფაქტორზე დამოკიდებული. ყველა კონკრეტულ სიტუაციაში ამ ფაქტორების გარკვეული ნაწილი იწვებს დომინირებას, მაგრამ არსებობს მათი ჩამონათვალი, რომლის გათვალისწინებაც პრაქტიკულად ყოველთვის აუცილებელია.

ასეთი ფაქტორებია:

- ქსელის განთავსების არეალის ზომები – ტერიტორია;
- მომხმარებელთა რიცხვი;
- ქსელის მომსახურების (გამოყენების) სახეები;
- მოწყობილობათა ექსპლუატაციის დრო.

მოვიყვანოთ ასეთი მაგალითი. ცხადია, რომ სულ სხვადასხვა სახე ექნება პრობლემებს, ვთქვათ, გარკვეული რეგიონის მომცველი ქსელისათვის და ქსელისათვის, რომელის განთავსების არეალი, ვთქვათ, ერთი შენობაა. ასევე, ცხადი იქნება პრობლემების განსხვავებულობა, ქსელისათვის, რომელიც აღჭურვილია ახალი აპარატურით და ქსელისათვის, რომლის აპარატურაც უკვე მრავალი წელია ფუნქციონირებს და მისი საექსპლუატაციო რესურსები ამოწურვის ზღვარზეა.

კაბელები და მასთან დაკავშირებული კომპონენტები

საკაბელო სისტემა, ე.ი. თვითონ კაბელები და მასთან დაკავშირებული კომპონენტები, ქსელში მტყუნების წარმოშობის უდიდესი ალბათობის მატარებლები არიან. ქსელის მტყუნების მიზეზი შეიძლება გახდეს:

- კაბელის გაწყვეტა;
- მოკლე ჩართვა კაბელში;

- კაბელის რომელიმე შიგა წრედის გაწყვეტა;
- კაბელის არასწორი შეერთება;
- კაბელის შემაერთებლების (კონექტორების) უწყისივრობები.

საკაბელო სისტემაში წარმოშობილი მტყუნების მიზეზის მოკლე დროში დადგენა შესაძლებელია თუ ქსელის ადმინისტრატორისა და სისტემური ინჟინრის განკარგულებაშია, ვთქვათ, რეფლექტომეტრი და საქსელო ანალიზატორი.

კვების წყაროს მტყუნება

ქსელის ეფექტური ფუნქციონირების უზრუნველყოფის ერთერთი უმნიშვნელოვანესი საკითხია მოწყობილობა–დანადგარების უზრუნველყოფა უწყვეტი, გარანტირებული და საიმედო ელექტროკვებით. ელექტროკვების ეს პირობები თუ არ არის შესრულებული, ქსელის ფუნქციონირებაში ყოველთვის არსებობს პრობლემების წარმოშობის შესაძლებლობა. ამიტომ ქსელის ყველა კვანძი, ყველა მოწყობილობა უზრუნველყოფილ უნდა იყოს როგორც გარეგანი, ასევე შიდა კვების წყაროებით.

აქედან გამომდინარე, ქსელის ადმინისტრატორისა და სისტემური ინჟინრის მუდმივი ზრუნვის საგანს უნდა წარმოადგენდნენ გარანტირებული კვების წყაროები – Uninterruptible Power Supply (UPS).

ქსელის მოდერნიზაცია

ქსელის ეფექტური ფუნქციონირების უზრუნველყოფის ასევე უმნიშვნელოვანესი საკითხია მისი მოდერნიზაცია. ამავე დროს მოდერნიზაცია წარმოშობს პრობლემებს, ვინაიდან იგი უნდა მიმდინარეობდეს ქსელის პრაქტიკულად უწყვეტ რეჟიმში მუშაობის პირობებში.

ქსელის ადმინისტრატორისა და სისტემური ინჟინრის საზრუნავია, ერთი მხრივ მოდერნიზაციის რეალიზება უმოკლეს დროში და, მეორე მხრივ, მომხმარებელთა იმ წრის დადგენა ვისაც მეტნაკლებად მაინც შეეხება მოდერნიზაციის ეს თუ ის პროცესი და შემდგომ მათი დროული ინფორმირება შესაძლო შედეგების შესახებ.

კომპიუტერები

ქსელში პრობლემების წარმოშობის მიზეზი შეიძლება გახდეს მისი ძირითადი კომპონენტი-კომპიუტერი: კომპიუტერი-კლიენტი, კომპიუტერი-სერვერი; კომპიუტერი პერსონალური, მინი და საშუალო კლასის, მენიფრეიმი.

ცხადია, რომ ქსელში, მით უმეტეს, გლობალურ ქსელში, კომპიუტერთა დაზიანებით, მწყობრიდან გამოსვლით გამოწვეული პრობლემები მრავალფეროვანია და განსაკუთრებულ ყურადღებას მოითხოვს. განსაკუთრებით მნიშვნელოვანია იმ ინფორმაციის შენახვის უზრუნველყოფა, რომელსაც ისინი ფლობენ. ამ თვალსაზრისით კატასტროფულია თვითონ კომპიუტერში მახსოვრობის

მოწყობილობის მწყობრიდან გამოსვლა, მაგალითად, მაგნიტური დისკის მექანიკური დაზიანება.

ამ მეტად პრობლემატური საკითხის მოგვარება პირველ რიგში, ქსელის დაგეგმვაშია: თუ მოსალოდნელია, რომ ესა თუ ის კომპიუტერი ძვირფასი და უნიკალური ინფორმაციის მატარებელი გახდება, გათვალისწინებულ უნდა იქნეს ამ ინფორმაციის აუცილებელი და სრული სარეზერვო ასლის გადაღება.

ქსელის არასაკმარისი წარმადობა

წარმადობასთან დაკავშირებით ასეთი სურათი შეიძლება წარმოჩნდეს: ქსელი გარკვეული დროის (წუთები, საათები) ან დიდი დროის (დღეები, კვირები) განმავლობაში ნელა მუშაობს. დასადგენია რა არის ამის მიზეზი: რაიმე გაუთვალისწინებელი შეფერხება, მნიშვნელოვანი დაზიანებები თუ ქსელისადმი წაყენებული მოთხოვნების გაუთვალისწინებელი ზრდა.

გაუთვალისწინებელი შეფერხებებისა და მნიშვნელოვანი დაზიანებების ლიკვიდაცია, ცხადია, უმოკლეს ვადაში უნდა განხორციელდეს. აქ ძირითადი პასუხისმგებლობა ქსელის ადმინისტრატორსა და სისტემურ ინჟინერზეა.

რაც შეეხება წაყენებული მოთხოვნების გაზრდას, უნდა განხორციელდეს ქსელის მიზნობრივი მონიტორინგი, რათა გამოვლინდეს დამატებითი მოთხოვნების წყაროები, იქნება ეს ახალი მომხმარებლების შემოსვლა ქსელში, თუ არსებული მომხმარებლების მიერ დატვირთვების გაზრდა. შემდეგ დაისვას ქსელის გაფართოების საკითხები და მოხდეს მათი რეალიზება.

დაბოლოს, დასკვნის სახით უნდა აღინიშნოს, რომ თანამედროვე ინფორმაციულ-კომუნიკაციური ქსელების მომსახურება რთული და მეტად საპასუხისმგებლო საქმეა; იგი მოითხოვს მაღალკვალიფიციური სპეციალისტების არსებობას და ამ სპეციალისტების მიერ თავის საქმიანობაში დიდ ძალისხმევას.

ლიტერატურა

1. Компьютерные сети.
Microsoft Corporation. Пер. с англ. Москва. 2004 -696с.
2. Э. Таненбаум.
Компьютерные сети. Санкт-Петербург. " Питер". 2005-992с.
3. Олифер В. Г., Олифер Н. А.
Компьютерные сети. Санкт-Петербург. " Питер". 2006 г-762с
4. მ. ქართველიშვილი, თ. ქართველიშვილი
მარშრუტიზაციის ალგორითმები კომპიუტერულ ქსელებში.
თბილისი. სტუ. 2005 წ.
5. Спортак Марк, Паппас Френк и др.
Компьютерные сети и сетевые технологии: Пер. с англ. Киев. 2002-736с.