საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

ირაკლი ჯორჯაძე

მონაცემთა გადაცემის ქსელებით ხმის სიგნალის გატარებასთან დაკავშირებული პრობლემების აღმოფხვრა და შესაბამისი დაცვის მექანიზმების შემუშავება

დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარდგენილი დისერტაციის

ა ვ ტ ო რ ე ფ ე რ ა ტ ი

სადოქტორო პროგრამა: ”ტელეკომუნიკაცია“

შიფრი: 0402

თბილისი

2019

სამუშაო შესრულებულია საქართველოს ტექნიკურ უნივერსიტეტში
ენერგეტიკისა და ტელეკომუნიკაციის ფაკულტეტი
ტელეკომუნიკაციის დეპარტამენტი

ხელმძღვანელი: ასოცირებული პროფესორი ვ. აბულაძე

რეცენზენტები:

დაცვა შედგება 2019 წლის ”-------” ”---------- ”-------” საათზე საქართველოს ტექნიკური უნივერსიტეტის ენერგეტიკისა და ტელეკომუნიკაციის ფაკულტეტის სადისერტაციო კოლეგიის სხდომაზე, კორპუსი VIII, აუდიტორია
მისამართი: 0175, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ის ბიბლიოთეკაში,
ხოლო ავტორეფერატისა - ფაკულტეტის ვებგვერდზე

სადისერტაციო საბჭოს მდივანი, გ. გიგინეიშვილი
ასოცირებელი პროფესორი

სამუშაოს ზოგადი დახასიათება

სადისერტაციო ნაშრომის შესავალ ნაწილში აღნიშნულია თანამედროვე კომუნიკაციების ეპოქაში ინტერნეტის როლისა და მულტიმედიური აპლიკაციების მოთხოვნით გამოწვეული მონაცემთა გადაცემის სიხშირისა და სიჩქარისადმი წაყენებული მოთხოვნების გაზრდის აუცილებლობის შესახებ, რომელთა პრაქტიკული განხორციელება მრავალ პრობლემასთან აღმოჩნდა დაკავშირებული. ამ დროს ისეთი მოქნილი ტექნოლოგიის დანერგვა, როგორიცაა მრავალპროტოკოლიანი კომუტაცია ნიშნულების მიხედვით (MPLS - Multi Protocol Label Switching), უზრუნველყოფს მონაცემთა გადაცემის უსაფრთხოებას, პაკეტების დაგვიანების მინიმიზაციასა და მათ გადაცემას მაღალი სიჩქარით. ის სტანდარტული მარშრუტიზაციის ნაცვლად იყენებს კომუტაციის მეთოდს და არსებულ IP-ქსელებს (Internet Protocol) და იძლევა მომსახურების უკეთესი ხარისხის უზრუნველყოფისა და ნაკადის მართვისთვის შესაფერისი გარემოს შექმნის საშუალებას.

MPLS-ტექნოლოგიის ერთ-ერთი მნიშვნელოვანი ფუნქცია ტრაფიკის ინჟინერინგია (TE - Traffic Engineering), რომელიც ქსელური დატვირთვის მინიმიზაციისთვის, რესურსების რეზერვაციისთვის, ბალანსისა და მართვისთვის მნიშვნელოვან როლს ასრულებს.

MPLS-TE-ს საშუალებით განისაზღვრება მონაცემების უსაფრთხო და ხარისხიანი მარშრუტიზაცია. ქსელში ტრაფიკის დიდი მოცულობა და ისეთი მოულოდნელი ინციდენტები, როგორებიცაა ფიზიკური შეერთების გათიშვა, ქსელური შეტევები, განაწილებული შეტევა მომსახურების დაბლოკვის მიზნით, მარშრუტიზატორის, კომუტატორის და ცალკეული აპარატურული პრობლემა იწვევს მონაცემთა გადაცემის არხებში ტრაფიკის კრიტიკულ დონემდე მატებას. ასეთ დროს უნდა მოხდეს მარშრუტიზაციის კონფიგურაციის მყისიერი ცვლილება. ქსელის სპეციალისტის

ჩართულობის შემთხვევაში ეს პროცესი მოითხოვს დიდ დროს და, გარდა ამისა, იზრდება მექანიკური შეცდომების ალბათობა.

თემის აქტუალურობა. საბანკო, საგანმანათლებლო და სამეცნიერო-კვლევით საქმიანობასა და სოციალურ ქსელებში ხმოვანი და ვიდეო ინფორმაციის ინტერნეტ-პროტოკოლის საშუალებით (VoIP - Voice Over Internet Protocol) გადაცემა ერთ-ერთი ყველაზე იაფია. VoIP-სისტემებმა პოპულარობა მოიპოვა თავისი ეფექტურობის, ცოცხალი (Live) ვიდეოზარების, ზარის ხარისხის, მოქნილობისა და იაფი სერვისის გამო. თუმცა ინტერნეტითა და ტრადიციული IP (Internet Protocol)-ქსელის გამოყენებით რეალურ დროში ისეთი ინფორმაციის გადაცემა, როგორიცაა VoIP, რთული ამოცანაა, რადგან IP- ქსელს არ შეუძლია უზრუნველყოს ხმის და ვიდეო სიგნალების საიმედო მიწოდება. ტრადიციული IP-ქსელი იყენებს საუკეთესო მეთოდს, რომელსაც მხოლოდ შეცდომის კონტროლისა და გარკვეული შეზღუდული გადანაწილების სტრატეგიის განხორციელება შეუძლია. ამ და სხვა პრობლემების დაძლევის მიზნით ინტერნეტ-ინჟინერიის სამუშაო ჯგუფის მიერ შემუშავდა ტექნოლოგია სახელწოდებით MPLS.

MPLS-ტექნოლოგიით შესაძლებელია ისეთი პრობლემების გადალახვა, როგორიცაა დიდი დაყოვნებები და პაკეტების კარგვა, რაც ხშირია ტრადიციულ IP-ქსელებში. MPLS-ტექნოლოგიაა, რომელიც სერვის-პროვაიდერების მიერ ძირითადად გამოიყენება რეალურ დროში გადაცემული ხმოვანი და ვიდეოსერვისების გაუმჯობესებული ხარისხით მისაწოდებლად და იგი შეიძლება ჩაითვალოს როგორც ხმისა და ვიდეოკომუნიკაციის იდეალური საშუალება.

კომუნიკაციასთან დაკავშირებული პრობლემური საკითხების გადაწყვეტა შესაძლებელია მონაცემთა მართვის ინჟინერინგის (TE) ტექნოლოგიით, რომელიც წარმოადგენს ინსტრუმენტების კომპლექტსა და ტექნიკას ქსელური მონაცემების სრულყოფილად სამართავად.

სადისერტაციო ნაშრომის მიზანი. ზემოთ თქმულიდან გამომდინარე, ნაშრომის ძირითადი მიზანია ისეთი ამოცანის გადაწყვეტის გზების ძიება, როგორიცაა მონაცემთა გადაცემის პაკეტური საკომუტაციო ქსელის მონიტორინგის სისტემის შემუშავება, რომელიც ქსელში დაფიქსირებული პრობლემების დროს შესაბამისი ალგორითმების დახმარებით გადაწყვეტს ქსელური მოწყობილობების კონფიგურაციის ოპტიმიზაციის ამოცანას, დაახარისხებს შესრულებულ ქმედებებს და, ამასთანავე, შესაძლებელს გახდის პროცესებისადმი დაკვირვებას რეალურ დროში.

კვლევის ამოცანები. დასახული მიზნის მიღწევისთვის ნაშრომში გადაწყვეტილი იქნა შემდეგი ამოცანები:

1. VoIP-ქსელების უსაფრთხოების რისკების შეფასება, მათი ანალიზი და უსაფრთხოების შესაბამისი მოდელის შემუშავება;
2. MPLS-ქსელის არქიტექტურის ანალიზი: MPLS-TE, მონაცემთა ნაკადის გვირაბების (Tunnels) ვირტუალური მარშრუტიზაცია-გადამისამართების (VRF) პროტოკოლების ავტომატიზაციის პროგრამული უზრუნველყოფის მოდულებთან მორგება;
3. ქსელის მონიტორინგის პროგრამული უზრუნველყოფის დანერგვა და სატესტო გარემოში სიმულაცია;
4. ინტერნეტის და ხმოვანი სიგნალების მონაცემების ერთმანეთისგან იზოლირება. ხმოვანი სიგნალის ტრაფიკის წყაროზე დაფუძნებული მარშრუტიზაციის (SR) განხორციელება.
5. მონაცემთა გადაცემის პაკეტური საკომუტაციო ქსელის მონიტორინგის სისტემის აგება;
6. ვირტუალურ გარემოში MPLS-ქსელის აგება და მისი სიმულაცია, რომელიც SNMP-პროტოკოლის საშუალებით ინტეგრირდება მონიტორინგის სისტემასთან.

კვლევის მეთოდოლოგია. დისერტაციაში დასმული ამოცანების გადაჭრისათვის თეორიული და პრაქტიკული საკითხების დამუშავებისას გამოყენებულ იქნა ქსელის გრაფიკული ემულატორი EVE-NG, რომელიც

მიესადაგება მარშრუტიზატორის, კომუტატორისა და სასერვერო ოპერაციულ სისტემებს. სიმულაციური ქსელი აიგო შემდეგი ქსელის პროტოკოლებისა და ტექნოლოგიების გამოყენებით: ინტერნეტ-პროტოკოლი IP (Internet Protocol); მრავალპროტოკოლიანი კომუტაცია ნიშნულების მიხედვით MPLS (Multi Protocol Label Switching); ნიშნულების განაწილების პროტოკოლი LDP (Label Distribution Protocol); რესურსების რეზერვირების პროტოკოლი RSVP (Resource reservation protocol); ქსელის მარტივი მართვის პროტოკოლი SNMP (Simple Network Management Protocol); პირველადი უმოკლესი მარშრუტი OSPF (Open Shortest Path First); სასაზღვრო ქსელთაშორისი პროტოკოლი BGP (Border gateway protocol); ტრაფიკის ინჟინერია TE (Traffic Engineering); ვირტუალური მარშრუტიზაცია/გადამისამართება VRF (Virtual-Routing/Forwarding); მომსახურების ხარისხი QoS (Quality Of Service). ქსელის პროგრამული უზრუნველყოფის დასამუშავებლად გამოყენებული იქნა Node.JS-პლატფორმა და პროგრამირების ენა javascript.

მეცნიერული სიახლე. ნაშრომის თემასთან დაკავშირებული კვლევის შედეგად მიღწეული სამეცნიერო სიახლეა შემუშავებული ალგორითმი, რომელიც საჭირო დროს ახდენს ქსელური მოწყობილობების კონფიგურაციის ოპტიმიზაციას, რაც უზრუნველყოფს მონაცემთა პაკეტების უსაფრთხო მარშრუტიზაციას.

პრაქტიკული ღირებულება და სამუშაოს შედეგების გამოყენების სფერო. ნაშრომის პრაქტიკულ ღირებულებას განაპირობებს დამუშავებული პროგრამა, რომელიც უზრუნველყოფს MPLS-ქსელში გამოყენებული მონიტორინგის სისტემის ავტომატიზაციას და რომლის დანიშნულებაა ქსელში დაფიქსირებული სხვადასხვა ტიპის ავარიების დროს ქსელური მოწყობილობების კონფიგურაციის ავტომატური ცვლილება.

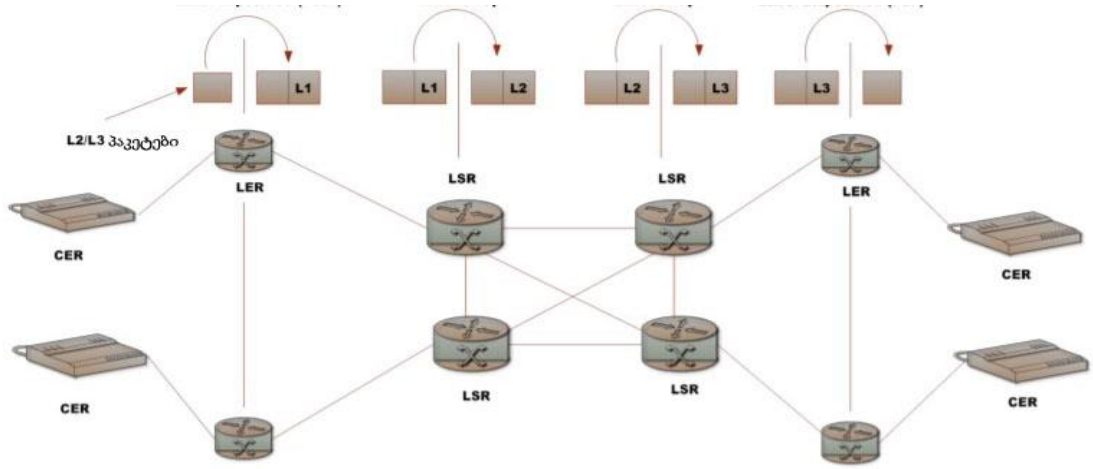
აპრობაცია. სადისერტაციო ნაშრომის ძირითადი შედეგები მოხსენებული და განხილული იქნა: სტუ-ს ტელეკომუნიკაციის დეპარტამენტში პირველ, მეორე და მესამე კოლოქვიუმებზე 2017-2019

წლებში; სტუ-სა და ფოჯას უნივერსიტეტის პირველ ერთობლივ R&D საერთაშორისო კონფერენციაზე “მრეწველობის დარგების დინამიკა და თანამედროვე ტენდენციები საქართველოსა და ევროკავშირში: საინფორმაციო-საკომუნიკაციო ტექნოლოგიები მიწოდების ჯაჭვის მენეჯმენტში” (17-19 ოქტომბერი, 2018 წელი, თბილისი, საქართველო); მიღებული შედეგები აისახა, აგრეთვე, სამეცნიერო-ტექნიკურ რეფერირებად ჟურნალში “ენერგია” (No 1 (89), თბილისი 2019 წ.) გამოქვეყნებულ სტატიასა და ჟურნალში “მართვის ავტომატიზებული სისტემები” (სტუ-ს თემატური სამეცნიერო შრომების კრებული No 1 (28), 2019) გამოქვეყნებულ 2 სტატიაში, სტუ-ს ტელეკომუნიკაციის დეპარტამენტის გაფართოებულ სხდომაზე წინასწარი დაცვისას გაკეთებულ მოხსენებაში (2019 წ.) და, აგრეთვე, თანაავტორებთან ერთად შედგენილ ლექციების კონსპექტში “სატელეკომუნიკაციო სიგნალების გადაცემის ტექნოლოგიები IP ინტერნეტ-პროტოკოლის გამოყენებით” (2018 წ.).

ცნობები დისერტაციის მოცულობისა და სტრუქტურის შესახებ. ნაშრომი შედგება შესავლისაგან, ლიტერატურის მიმოხილვისაგან, ხუთი თავისაგან, დასკვნისაგან, გამოყენებული ლიტერატურის 44 დასახელებისაგან და დანართისაგან. სამუშაოს მოცულობა შეადგენს 153 გვერდს, რომელიც შეიცავს 76 ნახაზს.

ნაშრომის შინაარსი

ნაშრომის პირველ თავში განხილულია მონაცემთა გადაცემის ქსელის აგების ტექნოლოგიის "მრავალპროტოკოლიანი კომუტაცია ნიშნულების მიხედვით (MPLS)" არქიტექტურა. მისი ფუნქციონირებისთვის გამოიყენება ნიშნულებიანი მარშრუტიზატორი (LSR), რომელსაც შეუძლია MPLS-ნიშნულების გარჩევა, მიღება და გადაცემა. არსებობს სამი სახის - შემსვლელი, გამსვლელი და შუამავალი ნიშნულებიანი მარშრუტიზატორი. მათგან შემსვლელი და გამსვლელი პროვაიდერის მოსაზღვრე მარშრუტიზატორებია. MPLS-VPN-ის შემთხვევაში შემსვლელი და გამსვლელი მარშრუტიზატორები პროვაიდერის სასაზღვრო მარშრუტიზატორებს (PE) წარმოადგენენ, ხოლო შუამავალი კი - პროვაიდერის მარშრუტიზატორია (P) (ნახ. 1).

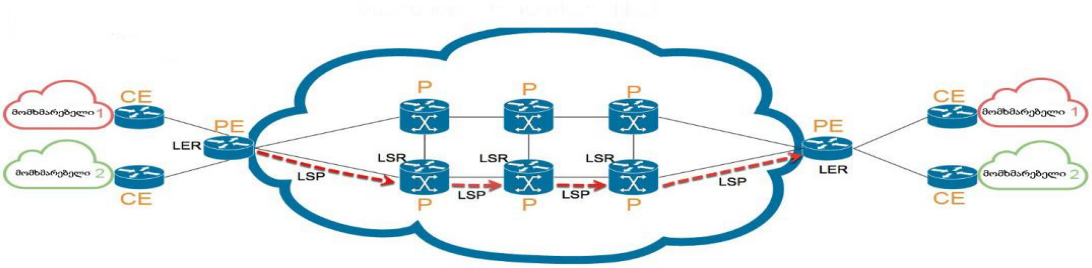


ნახ. 1. MPLS-ის ნიშნულების ოპერაცია

MPLS-ქსელისთვის გამოიყენება, აგრეთვე, ტერმინი "ნიშნულებიანი გზა (LSP)", რომელიც წარმოადგენს იმ ნიშნულებიანი მარშრუტიზატორების მიმდევრობას, რომლებიც დანიშნულ პაკეტებს გადასცემენ MPLS-ქსელში და რომელთაგან პირველი და ბოლო შემსვლელი

და გამსვლელი მარშრუტიზატორებია, ხოლო ყველა დანარჩენი - შუამავალი (ნახ. 2).

ნაშრომში გაანალიზებულია MPLS-ტექნოლოგიის მარკერების განაწილების პროტოკოლი (LDP) და რესურსების რეზერვირების პროტოკოლი (RSVP) და დასაბუთებულია MPLS-ქსელის უპირატესობები.



ნახ. 2. ნიშნულებიანი გზა (LSP)

MPLS-ის დანიშნულებაა შემოსული პაკეტის მონიშვნა ამ პაკეტის მიმღების მისამართის ან სხვა წინასწარ დაკონფიგურირებული კრიტერიუმის მიხედვით და ტრაფიკის კომუტაციის განხორციელება საერთო ინფრასტრუქტურის გავლით, რაც მის უდიდეს უპირატესობას წარმოადგენს მხოლოდ IP-მარშრუტიზაციის გამოყენებასთან შედარებით. MPLS-ის IP-ისთან ერთად გამოყენებისას შესაძლებელია ქსელური ტრანსპორტირების შესაძლებლობების გაზრდა. პაკეტებზე ნიშნულების დამატებით შესაძლებელია სხვადასხვა (მაგალითად, IPv4, IPv6, Ethernet, HDLC, PPP და სხვა) პროტოკოლების გადატანა IP/MPLS-ქსელში. MPLS-ქსელში პაკეტებს ნიშნულის სახით ენიჭება გადამისამართების ექვივალენტობის კლასი (FEC), რომელიც გამოიყენება კვანძებზე გადამისამართებისთვის IP-თავსართის გადამოწმების გარეშე. ყველა მარშრუტიზატორს აქვს FEC-ცხრილი. MPLS მოქმედებს OSI-მოდელის მონაცემთა და ქსელის დონეებს შორის. ამიტომ მას უწოდებენ 2.5 დონის პროტოკოლს.

MPLS-VPN-ის ერთრანგიან მოდელში სერვის-პროვაიდერის მარშრუტიზატორები მომხმარებლის ინფორმაციას ატარებენ თავიანთ ქსელში, თუმცა ისინი ასევე მონაწილეობენ მომხმარებლის მარშრუტიზაციაშიც. სხვა სიტყვებით რომ ვთქვათ, სერვის-პროვაიდერის მარშრუტიზატორები ამყარებენ მესამე დონის პირდაპირ კავშირს მომხმარებლის მარშრუტიზატორებთან. შედეგად სერვის პროვაიდერისა და მომხმარებლის მარშრუტიზატორებს შორის მყარდება ურთიერთკავშირი რომელიმე დინამიური მარშრუტიზაციის პროტოკოლის გამოყენებით (ნახ. 3).

ნახ. 3. MPLS-VPN სერვისი

მომხმარებლის მარშრუტიზატორი MPLS-VPN-სერვისით, რომელსაც მომხმარებლის მოსაზღვრე მარშრუტიზატორსაც (CE) უწოდებენ, IP-შრეზე ამყარებს კავშირს სერვის-პროვაიდერის მინიმუმ ერთ მარშრუტიზატორთან, რომელსაც პროვაიდერის მოსაზღვრე მარშრუტიზატორს (PE) უწოდებენ.

MPLS-VPN-ქსელში მონაცემების კონფიდენციალურობა მიიღწევა ვირტუალური მარშრუტიზაცია-გადამისამართებისა (VRF) და ქსელში მონაცემების გადაცემით მონიშნული პაკეტების სახით. VRF უზრუნველყოფს სხვადასხვა მომხმარებლების მარშრუტიზაციის შესახებ ინფორმაციის განცალკევებას, ხოლო MPLS-ქსელში - პაკეტების გადაცემას ნიშნულებით და არა IP-თავსართში არსებული ინფორმაციით. მომხმა-

რებლის დამატების შემთხვევაში საკმარისია PE-მარშრუტიზატორზე მხოლოდ CE-მარშრუტიზატორთან კავშირის დამატება, რაც მარტივია.

როგორც ცნობილია, ტრაფიკის ინჟინერიის ძირითადი არსია ქსელის ინფრასტრუქტურის ოპტიმალურად გამოყენების უზრუნველყოფა მონაცემთა გადაცემის შედარებით დაუტვირთავი არხების ჩათვლით. ეს იმას ნიშნავს, რომ ტრაფიკის ინჟინერია ქსელში ტრაფიკის ისეთი მარშრუტით მოძრაობის შესაძლებლობას იძლევა, რომელიც IP-მარშრუტიზაციის მიხედვით ყველაზე ნაკლებად ღირებულია, ანუ ისეთი მარშრუტით, რომელიც დინამიური შიდა მარშრუტიზაციის პროტოკოლით განსაზღვრული მონაცემების მიხედვით ყველაზე ნაკლებადაა პრიორიტეტული. MPLS-ქსელში ტრაფიკის ინჟინერია იძლევა A წერტილიდან B წერტილამდე ტრაფიკის სასურველი გზით მოძრაობის საშუალებას, ანუ გარკვეულმა ტრაფიკმა შეიძლება იმოძრაოს ნაკლებად დატვირთული ან საერთოდ დაუტვირთავი მაგისტრალით, რაც ქსელის ადმინისტრატორს აძლევს ქსელის არსებული რესურსების ოპტიმალურად გამოყენების შესაძლებლობას.

ნაშრომის მეორე თავში განხილულია VoIP-ქსელები და მისი უსაფრთხოების საკითხები და დამუშავებულია VoIP-უსაფრთხოების მოდელი.

VoIP არის ხმისა და მასთან დაკავშირებული სამოსამსახურო ინფორმაციის მარშრუტიზაცია ციფრულ ფორმატში ინტერნეტ-პროტოკოლის (IP) გამოყენებით. VoIP-ქსელი არ არის შეზღუდული მხოლოდ ხმოვანი კომუნიკაციით, არამედ მისი საშუალებით შესაძლებელია, აგრეთვე, როგორც ვიდეო ზარების განხორციელება (ვიდეოკონფერენცია), ასევე სხვა ტიპის მონაცემთა გადაცემა საკონფერენციო კავშირისთვის. ის მნიშვნელოვანი ტექნოლოგიაა, რადგან უზრუნველყოფს ადამიანთა ერთმანეთთან კომუნიკაციის საშუალებების ნაირფეროვნებას. შეიძლება ითქვას, რომ თავისი გამოყენებადობისა და მოქნილობის წყალობით VoIP-ს შეუძლია სხვადასხვა ქსელების დაახლოება

და კონვერგენცია, ანუ ჰიბრიდული ქსელის შექმნა. VoIP-ტექნოლოგია შეიძლება განვიხილოთ ინტერნეტ-კომუნიკაციის მეგზურის როლში, ვინაიდან ის მომხმარებლებს აძლევს მომსახურების სხვადასხვა სახეობებისადმი წვდომის საშუალებას. VoIP ქსელის დონეზე იყენებს ინტერნეტ პროტოკოლს (IP), ხოლო ტრანსპორტის დონეზე - ისეთ პროტოკოლებს, როგორებიცაა გადამცემი საკონტროლო (TCP), სამომხმარებლო დატაგრამებისა (UDP) და ნაკადის კონტროლის გადაცემის პროტოკოლები (SCTP). აპლიკაციის დონეზე იგი იყენებს პროტოკოლებს - DNS-ს, DHCP-ს და ორ ან ორზე მეტ მომხმარებელს შორის ხმისა და/ან მულტიმედიური ტრაფიკის გაცვლისთვის გამოყენებად სასიგნალო პროტოკოლებს (H.323, SIP, MGCP, RTP, SRTP და ZRTP).

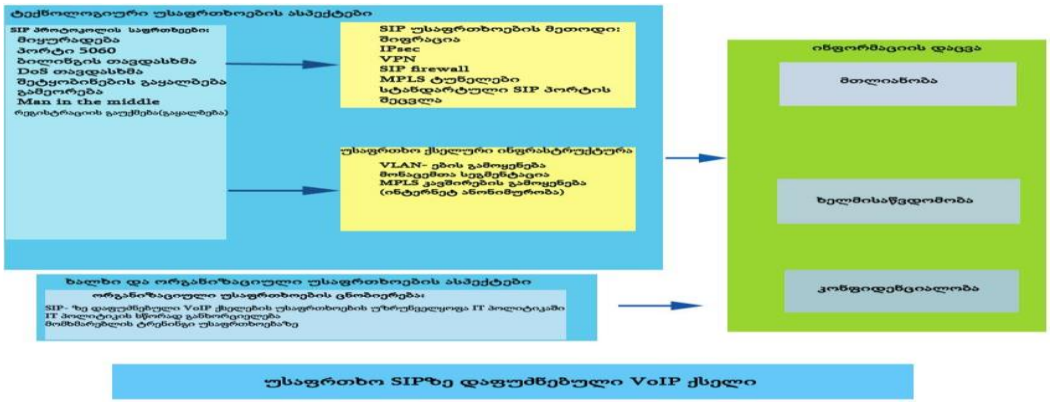
ნაშრომში აღნიშნულია, რომ MPLS-ში უსაფრთხოების უზრუნველყოფა ხდება "ბუნდოვანებით", ანუ მის გარემოში მომხმარებლის ტრაფიკი მიუწვდომელია ინტერნეტის სხვა მომხმარებლებისთვის. ეს იმას ნიშნავს, რომ მომხმარებელს ეძლევა კერძო LAN-ქსელის შექმნის შესაძლებლობა, რაც უზრუნველყოფს მისი ტრაფიკის უსაფრთხო გავრცელებას ინტერნეტ სერვის-პროვაიდერის (ISP-ის) საჯარო ქსელში. ამასთანავე, MPLS-ის უსაფრთხოება დამოკიდებულია პროვაიდერის კიდის (EDGE) და ძირითადი (CORE) ქსელების უსაფრთხოებაზე. სერვის- პროვაიდერები ინტერნეტიდან წვდომების შეზღუდვისა და გაფილტვრის მიზნით თავიანთ მარშრუტიზატორებზე იყენებენ ისეთ მეთოდებს, როგორებიცაა პაკეტის ფილტრაცია და „დაშვების კონტროლის სიები“ (ACL).

იმ დროს, როდესაც ორგანიზაციები განსაკუთრებულ ყურადღებას უთმობენ თავიანთი ინფორმაციის, შესაბამისი ქსელებისა და ინფრასტრუქტურის დაცვისათვის საჭირო ტექნოლოგიის გამოყენებას, მათ ავიწყდებათ, რომ პროცესში ადამიანებიც მონაწილეობენ. კერძოდ, უნდა აღინიშნოს, რომ სატელეკომუნიკაციო უსაფრთხოებაზე შესაძლოა გავლენა იქონიოს პირის ინფორმაციული უსაფრთხოების ცოდნის ნაკლებობამ, რაც გამოიწვევს ორგანიზაციის ფინანსურ და, აგრეთვე, კონფიდენციალურობისა და ინფორმაციის მთლიანობის დაცვის

პრობლემებს. ამიტომ ორგანიზაციის თანამშრომლებს უნდა ჰქონდეთ ცოდნა ინფორმაციული უსაფრთხოებისა და რისკების შესახებ, რათა გაითვალისწინონ უსაფრთხოების ნიუანსები, სიმძიმე და მათი მასშტაბები. VoIP-ქსელების უსაფრთხოების პრობლემა გადაიჭრება მისი ინტერნეტისაგან იზოლაციის საშუალებით.

ხმოვანი მომსახურების მიმწოდებლის ქსელის ბოლოს არსებულ SIP-სერვერებთან მომხმარებლის კავშირი შეიძლება მიღწეულ იქნას VoIP-ის ჩართვით MPLS-ქსელის ინფრასტრუქტურაში. ამ დროს ორგანიზაციაში განთავსებული მომხმარებლის მოწყობილობები ინტერნეტის ქსელიდან იზოლირებულნი არიან, რითაც გარანტირებული ხდება მათი უსაფრთხოება. ეს კი უზრუნველყოფს მომხმარელთა ხმოვანი ტრაფიკის ხელმისაწვდომობას, მთლიანობასა და კონფიდენციალობას. შემოთავაზებული მოდელი მიზნად ისახავს SIP-ზე დაფუძნებული VoIP-ქსელის უსაფრთხოების დაცვას ინტერნეტისგან იზოლაციით.

ნახ. 4-ზე წარმოდგენილია SIP-ზე დაფუძნებული VOIP-ის უსაფრთხოების მოდელის არქიტექტურა (მისი კონცეპტუალური სტრუქტურა), რაც გულისხმობს ქსელურ ინფრასტრუქტურაში არსებული უსაფრთხოების გამოწვევებისა და ორგანიზაციული უსაფრთხოების ინფორმირებულობის ერთმანეთთან დამოკიდებულებას. აღნიშნული მოდელით შესაძლებელია ორგანიზაციის SIP-ზე დაფუძნებული VoIP-ქსელის უსაფრთხოების დაგეგმვა.



ნახ. 4. VoIP-ის უსაფრთხოების მოდელი

ხმოვანი კომუნიკაციის უსაფრთხოებისა და რისკებისაგან თავის არიდების მიზნით ორგანიზაციებმა უნდა განახორციელონ ქსელური ტრაფიკის სეგმენტაცია, რაც, ძირითადად, ხორციელდება სხვადასხვა ვირტუალური ლოკალური ქსელების (VLAN-ების) გამოყენებით. მოდელი წარმოადგენს სახელმძღვანელოს და იგი წარმოაჩენს საჭირო პროცედურებს, რომელთა მეშვეობითაც ორგანიზაციებს შეუძლიათ SIP-ზე დაფუძნებული VoIP-ქსელების განხორციელება. მოდელი შედგება სამი ძირითადი კომპონენტისგან: ტექნოლოგია, საინფორმაციო უსაფრთხოება და ორგანიზაცია-ადამიანები. ქსელის ინფრასტრუქტურა, არსებული უსაფრთხოების რისკები და ორგანიზაციული უსაფრთხოების ინფორმირების დონე არის მნიშვნელოვანი ფაქტორები, რომლებიც განიხილება შემოთავაზებული მოდელის განვითარების დროს. მოდელი საშუალებას აძლევს ორგანიზაციას უკეთ დაიცვას უსაფრთხოების ძირითადი საინფორმაციო კომპონენტები, ინფორმაციის კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა. ორგანიზაციის გარემოში მოდელი რომ ეფექტურად ჩამოყალიბდეს, მნიშვნელოვანია, რომ ყურადღება მიექცეს არა მხოლოდ ტექნოლოგიურ ასპექტებს, არამედ ორგანიზაციისა და თანამშრომლების მოლოდინებს. უსაფრთხოება, თავის მხრივ, სხვა ფაქტორებზეცაა დამოკიდებული, კერძოდ VoIP-ქსელის კომპონენტების შესაბამისი აპარატურის მწარმოებლისა და მისი კომპანიაში შემომტანი შუამავლის (ინტეგრატორის) კრიტიკულად შერჩევაზე, რაც მოდელის წარმატებით განხორციელების წინაპირობაა.

განვიხილოთ უსაფრთხოების მოდელის ტექნოლოგიური და ადამიანური ასპექტები. როგორც უკვე აღინიშნა, უსაფრთხოების მოდელი საჭიროა არა მხოლოდ ტექნოლოგიური ასპექტებისთვის, არამედ ორგანიზაციული საჭიროებებისთვისაც. უსაფრთხოება არის კავშირში ადამიანებთან და მათ ურთიერთქმედებასთან ტექნოლოგიებთან. ადამიანები, რომლებიც ურთიერთქმედებენ ამ ტექნოლოგიებთან, არ არიან სათანადოდ მომზადებული მისი გამოყენებისა და უსაფრთხოების

რისკებზე, რაც გავლენას ახდენს სისტემის უსაფრთხოებაზე. ამიტომ ორგანიზაციებმა უნდა აწარმოონ სათანადო პოლიტიკა საინფორმაციო ტექნოლოგიებში (IT) გასათვითცნობიერებლად, რომელიც უზრუნველყოფს არა მარტო უსაფრთხოების ტექნოლოგიურ ნაწილს, არამედ იმასაც, რაც დაკავშირებულია პერსონალის გაწვრთნასთან. იმის გამო, რომ ყველა თანამშრომელი, როგორც წესი, არ არის ტექნიკური პერსონალი, ორგანიზაციებმა უნდა უზრუნველყონ ქსელების შიდა უსაფრთხოება და თანამშრომლების სწორად ინფორმირება ტექნოლოგიის გამოყენების შესახებ. ინფორმაციული ტექნოლოგიების პოლიტიკა არა მარტო უნდა შეიქმნას, არამედ ის ეფექტურად უნდა განხორციელდეს ორგანიზაციაში უსაფრთხოების მაღალი დონის უზრუნველსაყოფად. ინფორმაციული უსაფრთხოების უზრუნველყოფის ძირითადი კომპონენტებია: ინფორმაციის კონფიდენციალურობა, ხელმისაწვდომობა და მთლიანობა.

მესამე თავში განხილულია მარშრუტიზაციის პრინციპები, ინტერნეტის სერვის-პროვაიდერის ქსელი, მისი პროტოკოლები და მათი სამომავალო განვითარება.

ქსელური კომუნიკაციისთვის ერთ-ერთ მნიშვნელოვან მოწყობილობას წარმოადგენს მარშრუტიზატორი, რომელიც ერთმანეთთან აკავშირებს სხვადასხვა ქსელებს და მართავს დანიშნულების ქსელის მიმართულებით მონაცემების გადაცემის პროცესს. მონაცემების დანიშნულების მიმართულებით გადასაცემად მარშრუტიზატორები იყენებენ ე.წ. მარშრუტიზაციის ცხრილს, რომელშიც ინახება ინფორმაცია მარშრუტიზატორისთვის ნაცნობი გზების შესახებ. მარშრუტიზაციის განხორციელებისთვის მას უხდება შემდეგი ოპერაციების ჩატარება: სატელეკომუნიკაციო ქსელში ფიზიკურად ან/და ლოგიკურად დაკავშირებულ მარშრუტიზატორებთან მარშრუტიზაციის მონაცემების გაცვლა; მარშრუტიზაციის საკუთარი ცხრილის შევსება მარშრუტიზაციაზე მიღებული მონაცემებით; მარშრუტიზაციის საკუთარი ცხრილის სკანირება და იქ არსებული ჩანაწერების მიხედვით დანიშნულების ქსელისკენ

მიმავალი გზებიდან ერთი ან რამდენიმე საუკეთესოდ შეფასებული გზის არჩევა; მონაცემების გადაცემისას მისი ურთიერთქმედება იმ მეზობელ მარშრუტიზატორთან, რომელიც განთავსებულია დანიშნულების ქსელის მიმართულების გზაზე; მარშრუტიზაციის საკუთარი ცხრილიდან იმ ადაპტერის იდენტიფიცირება, რომლისკენაც უნდა მოხდეს მონაცემების გადაცემა; მონაცემების მიღების შემთხვევაში შესაბამისი პაკეტის შემოწმება და დანიშნულების ქსელის მისამართის მიღება; მიღებული მისამართის შედარება მარშრუტიზაციის საკუთარ ცხრილში არსებულ ჩანაწერებთან და შემდეგი შესაბამისი მოქმედებების განსაზღვრა. ჩანაწერის პოვნის შემთხვევაში პაკეტი აგრძელებს გზას დანიშნულების ქსელისკენ, წინააღმდეგ შემთხვევაში კი როუტერი არ გააგზავნის მას.

ზემოთ აღწერილი ყოველი მოქმედება მეორდება დანიშნულების ქსელისკენ მიმავალ გზაზე განთავსებულ ყველა მარშრუტიზატორზე. მარშრუტიზატორები მონაცემების დანიშნულების მიმართულებით გადასაცემად მიმართავენ მარშრუტიზაციის საკუთარ ცხრილს, რომელიც შეიცავს ინფორმაციას დაშორებული ქსელების შესახებ. მარშრუტიზაციის ცხრილში ინფორმაცია ამა თუ იმ ქსელის შესახებ შეიძლება გამოჩნდეს ორი (სტატიკური და დინამიური) სახით.

ინტერნეტ-პროვაიდერების ქსელები, მათი მასშტაბებიდან გამომდინარე, კომპლექსურია, რაც იმას ნიშნავს, რომ მათი ფიზიკური და ლოგიკური ტოპოლოგია იერარქიულადაა განაწილებული. ქსელი იწყება მომიჯნავე მარშრუტიზატორებით, რომლებიც უზრუნველყოფენ კავშირს ეგრეთ წოდებულ აღმავალ პროვაიდერებთან, ინტერნეტის მიმოცვლის წერტილებთან (IXP) და, სურვილისამებრ, სხვადასხვა მსხვილ ორგანიზაციებთან. მათ ფიზიკური და ლოგიკური კავშირი აქვთ როგორც ერთმანეთთან, ასევე ქსელის ბირთვთან (CORE-თან). აქედან გამომდინარე, შემდეგი შრეა ქსელის ბირთვი, რომელიც, ძირითადად, უზრუნველყოფს ქსელის სხვადასხვა ნაწილში ტრაფიკის გატარებას მაქსიმალურად სწრაფად. ქსელის ბირთვის როუტერები, უმეტეს წილად, არ არიან

დატვირთულნი კონფიგურაციებითა და ფუნქციებით, რადგან უზრუნველყოფილი უნდა იყოს მათი წარმადობის მაქსიმალურად სრულად გამოყენება. ისინი უზრუნველყოფენ მაღალსიჩქარიან კავშირს განაწილების შრისა და მომიჯნავე როუტერებს შორის. განაწილების შრეზე (Distribution layer) ხორციელდება მომხმარებლებისთვის საჭირო თითქმის ყველანაირი კონფიგურაცია, წესები და დგება დაშვების სიები (Access Lists). ქსელის ბოლო შრეა დაშვების შრე (Acess layer), რომელიც უზრუნველყოფს უშუალოდ მომხმარებლების ჩართვას. დაშვების შრის ქსელური მოწყობილობები სხვადასხვა ტიპისაა, რაც იმაზეა დამოკიდებული, თუ რომელი ტექნოლოგიით (P2P, DSL, GPON, GE-LINK, WIFI და ა.შ.) მიეწოდება მომხმარებელს სერვისი.

მეოთხე თავში მოყვანილია სადისერტაციო ნაშრომში დასმული მიზნების გადაჭრისთვის განხორციელებული ექსპერიმენტების შედეგები, რომლებიც დაინერგა IP-MPLS-ქსელში, და ექსპერიმენტის ფარგლებში გაიმართა ტრაფიკ-ინჟინერია (TE), ერთმანეთისგან გამოიყო ხმისა და ინტერნეტის მონაცემთა ტრაფიკები და განხორციელდა აღნიშნული ქსელის ინტეგრაცია მონიტორინგის სისტემასთან.

როგორც ცნობილია, კომპიუტერული ქსელი მოწყობილობათა კომპლექტია, რომლებიც ერთმანეთთან დაკავშირებულია საერთო სატრანსპორტო ან საკომუნიკაციო პროტოკოლის მეშვეობით. მათ შორის კომუნიკაცია შეიძლება განისაზღვროს როგორც მომხმარებლებს ან/და ქსელის კვანძების ისეთ მოწყობილობებს შორის მონაცემთა გადაცემა, როგორებიცაა კომპიუტერები, მობილური მოწყობილობები, გამომავალი მოწყობილობები, მართვის ელემენტები, სერვერები, მარშრუტიზაციისა და გადართვის მოწყობილობები და ა.შ. გეოგრაფიული განაწილების მიხედვით არსებობს ლოკალური (LAN), რეგიონული (WAN) და გლობალური ინტერნეტ-ქსელი. ქსელის დიზაინის ან ტოპოლოგიის მიუხედავად, ნებისმიერი სახეობის ქსელი ემორჩილება მინიშნებებს და წესებს,

რომლებიც აღწერილია მონაცემთა გადაცემისა და კომუნიკაციის OSI-მოდელში.

ქსელის სერვერებისა და სისტემების მონიტორინგისთვის აუცილებელია ქვემოთ ჩამოთვლილი პირობების დაკმაყოფილება:

1. ქსელში არსებული სხვადასხვა ელემენტების მონაცემებისადმი წვდომის შესაძლებლობა;

2. მონიტორინგის პროგრამამ უნდა განახორციელოს მონაცემთა შეგროვება, დამუშავება და მომხმარებლისთვის იოლად აღქმად (ე. წ. „მეგობრულ“) ფორმატში მათი მიწოდება და წინასწარ განსაზღვრული ნორმების (პროგრამული ზღვრების) დარღვევის შემთხვევაში უზრუნველყოს მომხმარებლების ინფორმირება მოსალოდნელი პრობლემების შესახებ;

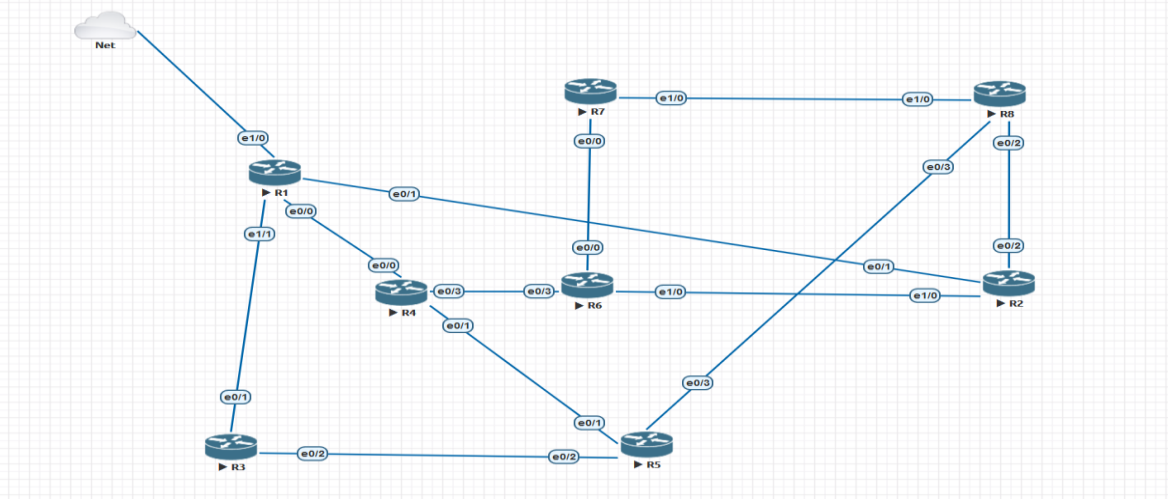
3. მონიტორინგის პროგრამასა და მონიტორინგზე აყვანილ ელემენტს შორის ინფორმაციის გადაცემის პროტოკოლის ან მეთოდის არსებობა.

ქსელის მონიტორინგის განმახორციელებელი სისტემა, მისი ღირებულების გარდა, უნდა იყოს ყოვლის მომცველი, ანუ უნდა მოიცავდეს საწარმოს ყველა ასპექტს, კერძოდ კი ქსელსა და მასთან ასოცირებულ კავშირს, სისტემებსა და მათთან ასოცირებულ უსაფრთხოებას. სისტემა უნდა უზრუნველყოფდეს ქსელის შესახებ ყველა სახის ინფორმაციის (ანგარიშგება, პრობლემის გამოვლენა და მოგვარება და ქსელის მუშა მდგომარეობაში შენარჩუნება) მონიტორინგს.

ნაშრომის მიზნების განხორციელებისათვის MPLS-ქსელის სიმულაციისა და ექსპერიმენტებისთვის EVE-NG ემულირებულ გარემოში გამოყენებულ იქნა მარშრუტიზატორები ოპერაციული სისტემით IOS Version 15.4(2)T.

ნახ. 5-ზე ნაჩვენებ სურათზე მოცემულია საქალაქთაშორისო IP/MPLS-ქსელი. მასში მარშრუტიზატორები განთავსებულია საკვანძო ქალაქებში და ფიზიკურ დონეზე კავშირები დაზღვეულია იმ მიზნით, რომ კაბელის დაზიანებამ არ გამოიწვიოს ამა თუ იმ ქალაქის იზოლირება. ქსელის

სიმულაციისისას გამოყენებულია 8 მარშრუტიზატორი პირობითი დასახელებებით R1, R2, ..., R8.



ნახ. 5. MPLS-ქსელის ტოპოლოგია

მოცემულ ქსელში მარშრუტიზატორებზე გამოყენებულია ურთიერთდამოუკიდებელი მარშრუტიზაციის სამი (გლობალური, vrf INT და vrf VOIP) ცხრილი. ქსელები ერთმანეთისგან იზოლირებულნი არიან, რის გამოც ისინი ვერ შეძლებენ ერთმანეთთან წვდომას. ამ ეტაპზე ქსელებში გამართულია სტანდარტული მარშრუტიზაცია, თუმცა, უნდა აღინიშნოს, რომ ხმის ტრაფიკის გამოყოფისთვის საჭიროა წყაროზე დაფუძნებული მარშრუტიზაციის გამოყენებაც, რაც მიიღწევა MPLS-TE-ს საშუალებით. დასახული მიზნის მისაღწევად ხმის ტრაფიკზე ზემოქმედებისთვის ტრაფიკის ინჟინერიის გამოყენება უნდა მოხდეს მხოლოდ vrf VOIP-ისთვის.

როგორც აღნიშნული იყო, თანამედროვე კომპიუტერული ქსელების მუშაობა წარმოუდგენელია მონიტორინგის სისტემის გარეშე. სწორედ რომ მათი საშუალებითაა შესაძლებელი ქსელში ინციდენტების დაფიქსირება და მათზე რეაგირება.

ნაშრომის ამავე თავში ექსპერიმენტული მოდელირებისთვის გამოყენებულია მონიტორინგის Solarwinds-NPM-სისტემა, რომელიც

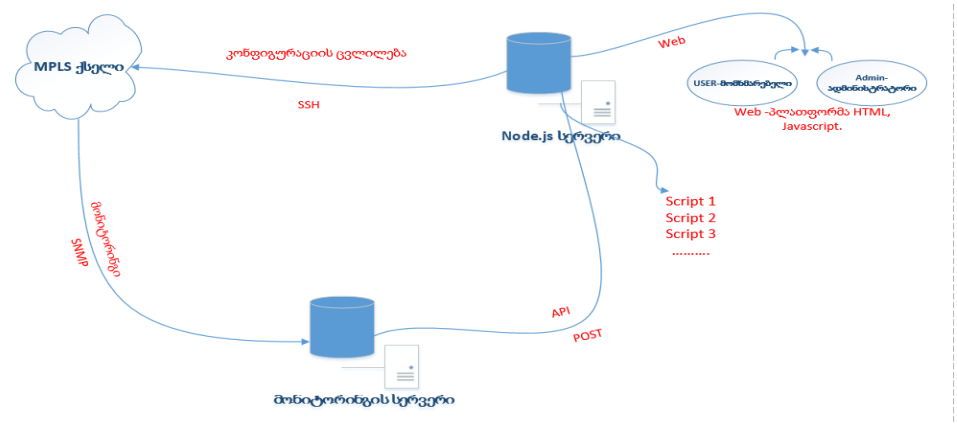
დაინსტალირდა ESXI 6.0 გარემოში მომუშავე შემდეგი მონაცემების მქონე ვირტუალურ პლატფორმა Windows Server 2012 R2-ზე: 50 GB SSD; 8 GB RAM; 6 intel Xeon 2.4 Ghz.

მეხუთე თავში ნაჩვენებია, რომ ქსელის უწყვეტი და ხარისხიანი მუშაობისთვის საჭიროა მისი მუდმივი მონიტორინგი გარკვეული ინციდენტების დროს კონფიგურაციის მყისიერი ცვლილების მიზნით, რათა თავიდან იქნეს აცილებული ის შედეგები, რაც შეიძლება მოყვეს ქსელში დაფიქსირებულ ხარვეზებს.

სადისერტაციო ნაშრომში დასმული ამოცანების განხორციელების მიზნით შედგენილია პაკეტური საკომუტაციო ქსელის ალგორითმის შესაბამისი პროგრამა და მისი რეალიზაციის ლოგიკური მოქმედებების სქემა, რომელიც ურთიერთქმედებაშია ქსელთან და მონიტორინგის სისტემასთან. დამუშავებული ალგორითმის პროგრამულ ნაწილს შეიძლება ეწოდოს ქსელის ავტომატური კონფიგურაციის სისტემა (Network Auto Configuration System - NACS).

თავდაპირველად მონიტორინგის სისტემა ქსელში მომხდარი ნებისმიერი სახის (უტილიზაცია, პროცესორის მაღალი დატვირთვა, ქსელური მოწყობილობის გათიშვა და სხვა) ინციდენტის დაფიქსირების შემდგომ node.js-პლატფორმაზე გამართულ NACS-ს უგზავნის HTTP-POST/GET-შეტყობინებას. NACS-პროგრამა, შეტყობინების შინაარსიდან გამომდინარე, SSH-პროტოკოლის საშუალებით მოახდენს მარშრუტიზატორის კონფიგურაციის გადამოწმებას და, საჭიროების შემთხვევაში, მის ცვლილებას. საბოლოოდ ცვლილებების შესახებ მონაცემები შეინახება Mysql-ბაზაში მათი შემდგომი ანალიზისთვის. NACS - სერვერს ექნება ვებ-ბრაუზერზე დაფუძნებული მომხმარებლისა და ადმინისტრატორის გარემო. მომხმარებლის User-გარემოში შესაძლებელი იქნება მონაცემთა ბაზაში დაფიქსირებული კონფიგურაციის ცვლილებებისა და შესრულებული ქმედებების შემოწმება და სტატისტიკების მოძიება. ადმინისტრატორის გარემოდან შესაძლებელი

უნდა იყოს ქსელის ელემენტების, განსახორციელებელი მოქმედებების სცენარებისა და პარამეტრების ისეთი ცვლილებები, როგორიცაა, მაგალითად, მარშრუტიზატორის დამატება, მარშრუტიზატორის IP-მისამართის ცვლილება ან მარშრუტიზატორის ექსპლუატაციიდან ამოღება და მისი გარკვეული კონფიგურაციის ცვლილება. გარდა ამისა, შესაძლებელი უნდა იყოს გვირაბის შექმნისა და წაშლის ბრძანებების ფორმირება. ნახ. 6-ზე წარმოდგენილია მონიტორინგის დამუშავებული ალგორითმის რეალიზაციის სქემა.



ნახ. 6. მონიტორინგის ალგორითმის სქემა

შემუშავებული NACS-სისტემის ლოგიკური კავშირები შესაძლოა დაიყოს შემდეგნაირად:

1. მონიტორინგის სერვერიდან POST-მეთოდით შეტყობინებების მიღება node.js-ზე. ამ შემთხვევაში Web-სერვერი იღებს შეტყობინებას ქსელური ინციდენტების შესახებ;

2. node.js-დან SSH-პროტოკოლის საშუალებით მარშრუტიზატორების მართვა და ცვლილებების ინფორმაციის ბაზაში დაფიქსირება;

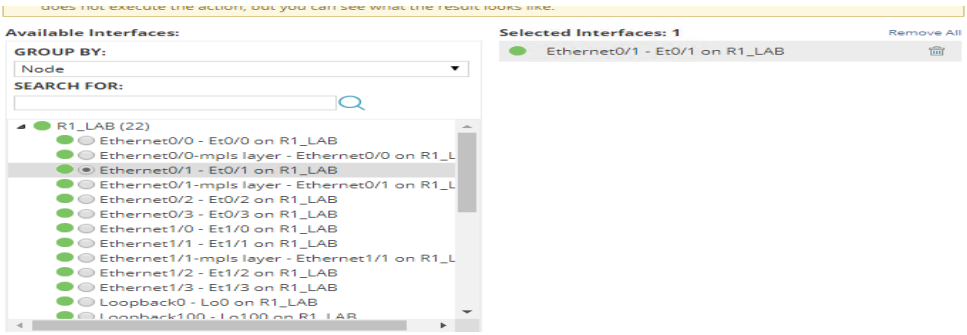
3. node.js-ზე web-სერვერის გამართვა და მომხმარებლისა და ადმინისტრატორის პანელების შექმნა. იგი, თავის მხრივ, შეიძლება დაიყოს შემდეგნაირად:

3.1. პროგრამირების javascript და HTML ენაზე შესრულებულ მომხმარებლის WEB-გარემო იძლევა შესრულებული ქმედებებისა და სტატისტიკის შემოწმებისა და მონიტორინგის საშუალებას;

3.2. პროგრამირების javascript და HTML-ენაზე შესრულებული ადმინისტრატორის WEB-გარემო იძლევა კონფიგურაციის სცენარებისა და ქსელის კომპონენტების პარამეტრების ცვლილების საშუალებას.

სადისერტაციო ნაშრომის ამავე თავში წარმოდგენილია ქსელის ემულატორის EVE-NG-ის გამოყენებით შემუშავებული და ზემოთ აღწერილი ალგორითმის მოდელირების შედეგები. ექსპერიმენტი ჩატარდა IP-MPLS-ქსელის 8 კვანძზე მათ მარშრუტიზატორებზე შექმნილი OSPF, MPLS-TE, LDP და RSVP- პროტოკოლების შესაბამისი კონფიგურაციით. VoIP-ტრაფიკის Internet-ტრაფიკისგან იზოლაციის მიზნით გამოყენებულ იქნა vrf-ტექნოლოგია, ხოლო მოდელირებულ IP-MPLS-ქსელში პრობლემების დაფიქსირებისა და იმიტაციისთვის - მონიტორინგის NPM-სისტემა. დამუშავებული ალგორითმის ეფექტურობის დასადგენად დაიგეგმა მონიტორინგის სისტემიდან შემდეგი ოთხი ტიპის განგაშის შესახებ შეტყობინების გაგზავნის სცენარი:

1. შეტყობინება მონაცემთა გადაცემის არხის გადავსების შესახებ. ნახ. 7-ზე წარმოდგენილ სურათზე ნაჩვენებია მონიტორინგის გარემო, საიდანაც მოხდა R1-ის მონაცემთა გადაცემის 0/1 ნომრის მქონე არხის ინტერფეისის გადავსების სიმულაცია.

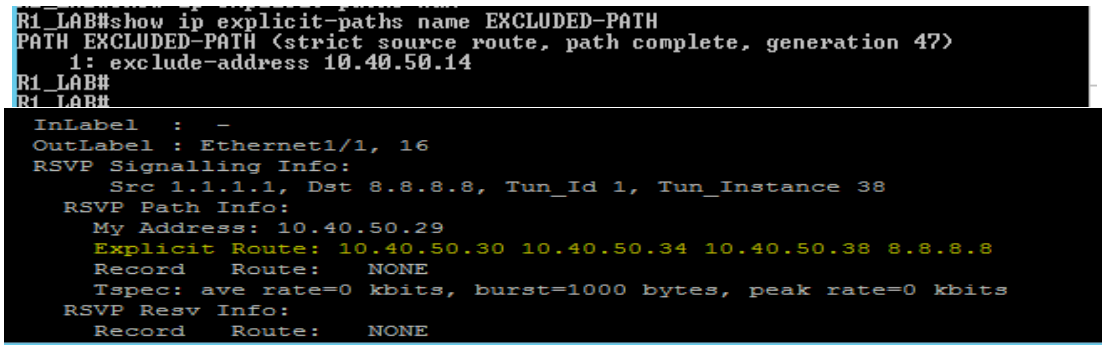


ნახ. 7. არხის გადავსების პროცესის სიმულაცია

აღნიშნული სურათიდან ჩანს, რომ Node.Js-პლატფორმაზე გამართული და ნაშრომის მიზნებისთვის დამუშავებული პროგრამული ალგორითმი, რომელიც სადისერტაციო ნაშრომში წარმოდგენილია დანართის სახით, მონიტორინგის სერვერიდან R1-ის 0/1 ინტერფეისზე იღებს შეტყობინებას ტრაფიკის გადატვირთვის შესახებ. ნახ. 8-ზე მოყვანილია აღნიშნული შეტრობინების მიღებისა და დამუშავების პროცესის ამსახველი სურათი.

ნახ. 8. სერვერის მიერ შეტყობინების მიღება და დამუშავება

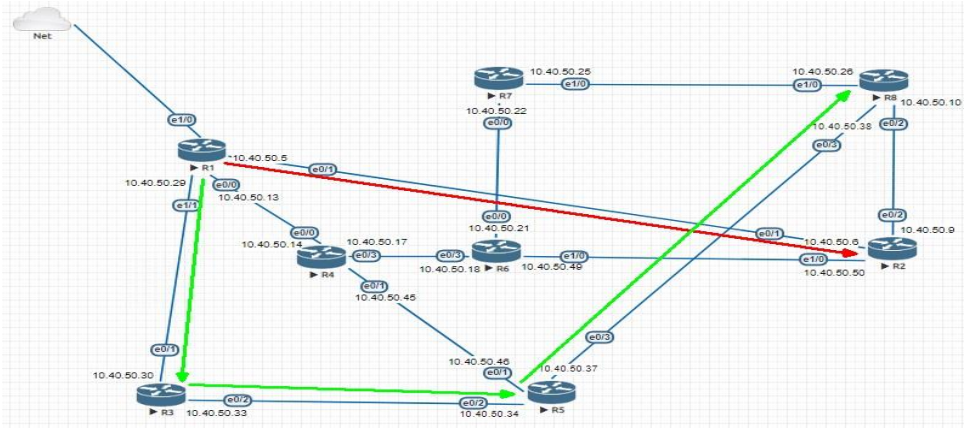
ნახ. 9-ზე ნაჩვენებია R1-დან R8-მარშრუტიზატორისკენ მიმართული გვირაბის კონფიგურაცია, სადაც ჩანს რომ R1-0/1 ინტერფეისი შეიზღუდა, რის გამოც იგი აღარ ფიგურირებს გვირაბში გადაცემული ტრაფიკის მარშრუტში. შესაბამისად, ხმოვანი მონაცემების გადაცემის vrf VOIP-ტრაფიკი უკვე მოძრაობს უსაფრთხო მარშრუტით.



ნახ. 9. დეტალური ინფორმაცია გვირაბში ტრაფიკის გადაცემის შესახებ

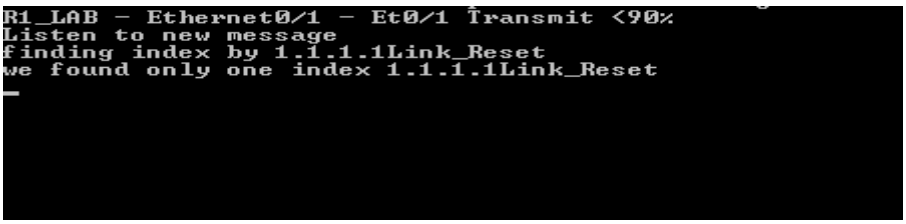
ნახ. 10-ზე წარმოდგენილ სქემაზე მწვანე ისრით ნაჩვენებია R1-დან R8-სკენ მოძრავი vrf VOIP-ტრაფიკის მარშრუტი. გვირაბის ახალი

მარშრუტი შედგა OSPF-პროტოკოლის უმოკლესი გზის მექანიზმის გამოყენებით. შესაბამისად R1-დან R8-სკენ, აღნიშნული შეზღუდვიდან გამომდინარე, ოპტიმალური აღმოჩნდა მარშრუტი R1->R3->R5->R8. ნახაზზე წითელი ისრით კი ნაჩვენებია პრობლემური (არაოპტიმალური) მარშრუტი.



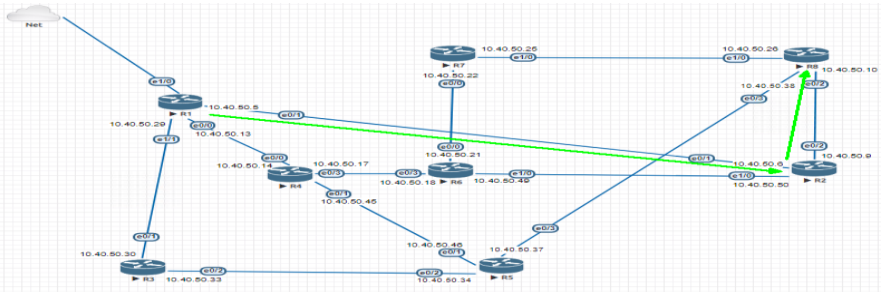
ნახ. 10. vrf VOIP-ტრაფიკის მოძრაობის სქემა

2. მონაცემთა გადაცემის არხში ტრაფიკის მისაღებ დონეზე დაბრუნების შესახებ შეტყობინება და შემუშავებული ალგორითმით გათვალისწინებული შემდგომი ქმედება. ამ შემთხვევაში მონიტორინგის სერვერზე გაკეთდა R1-ის მონაცემთა გადაცემის 0/1 ნომრის მქონე არხის გადავსების პრობლემის მოხსნის იმიტაცია და გაიგზავნა შესაბამისი შეტყობინება პროგრამული ალგორითმის სერვერზე. ნახ. 11-ზე ნაჩვენებია სერვერის მიერ შეტყობინების მიღებისა და დამუშავების დაწყების ამსახველი სურათი.



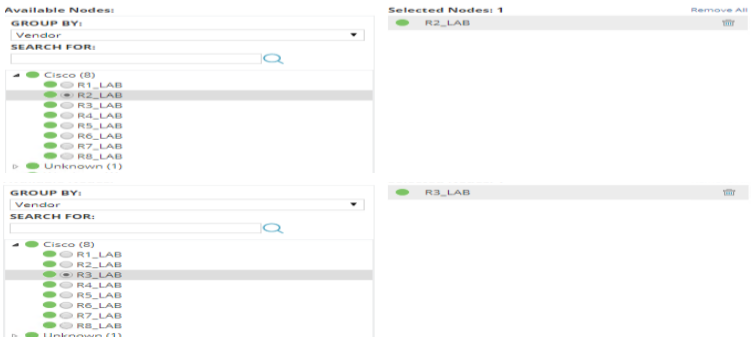
ნახ. 11. NACS-ის მიერ შეტყობინების მიღება და დამუშავება

R1-მარშუტიზატორზე 0/1 ინტერფეისის გადავსების პრობლემის მოგვარების შემთხვევაში აღნიშნული ინტერფეისის შეზღუდვა მოიხსნება და MPLS-TE ხელახლა გამოთვლის მარშრუტს წარმოდგენილი სქემის მიხედვით. ამ შემთხვევაში R1-დან R8-მდე უმოკლესი გზაა R1-R2-R8 (ნახ. 12).



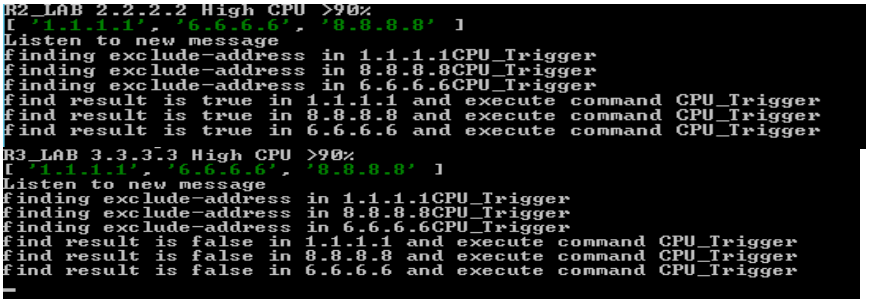
ნახ. 12. vrf VoIP-ტრაფიკის მოძრაობის მიმართულების სურათი პრობლემის მოგვარების შემდგომ

3. შეტყობინება ზემოთ წარმოდგენილ ქსელის R2 და R3 მარშრუტიზატორებზე არასტაბილური კავშირის შემთხვევასთან ან/და მათი აპარატურული ხარვეზების წარმოქმნასთან ასოცირებული ისეთი პრობლემების შესახებ, როგორებიცაა: ცენტრალური პროცესორის მაღალი დატვირთვა, აპარატურული მეხსიერების გადავსება, ტემპერატურის მომატება კრიტიკულ ზღვარს ზემოთ და ქსელურ კვანძთან არასტაბილური კავშირი. მოდელირების შესაბამისი სურათი პროცესორის გადატვირთვის შემთხვევაში წარმოდგენილია ნახ. 13-ზე.



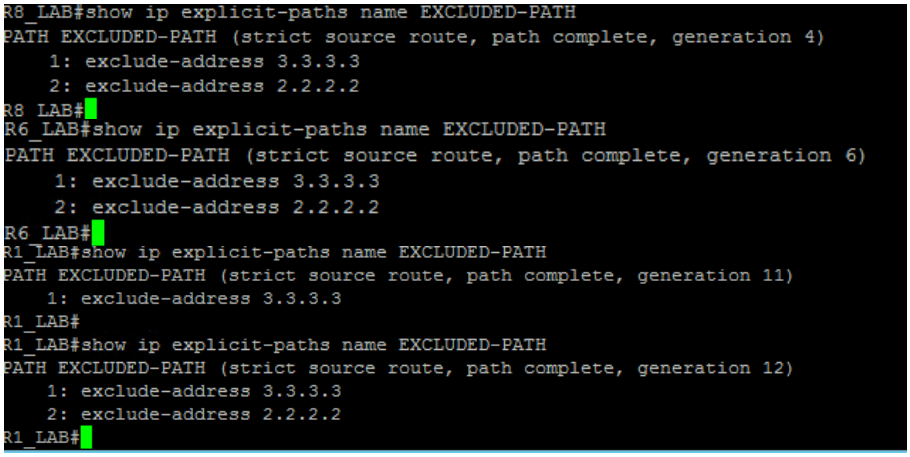
ნახ. 13. ქსელური R2 და R3 კვანძების პროცესორის გადატვირთვის პრობლემის სიმულაცია

ნახ. 14-ზე ნაჩვენებია შემთხვევა, როდესაც პროგრამული ალგორითმის სერვერი ცენტრალური პროცესორის გადატვირთვის შესახებ შეტყობინებას იღებს R2 და R3-კვანძებზე, რის შემდეგაც ალგორითმი იწყებს მოქმედებებს.



ნახ. 14. NACS-ის მიერ შეტყობინების მიღება და დამუშავება

ალგორითმის ამუშავების შედეგად განხილულ შემთხვევაში ექსპერიმენტულ ქსელში vrf VOIP-გვირაბის მარშრუტის გამოთვლისას მონაწილეობენ პრობლემური R2 და R3 კვანძები, რაც ასახულია ნახ. 15-სა და ნახ. 16-ზე.



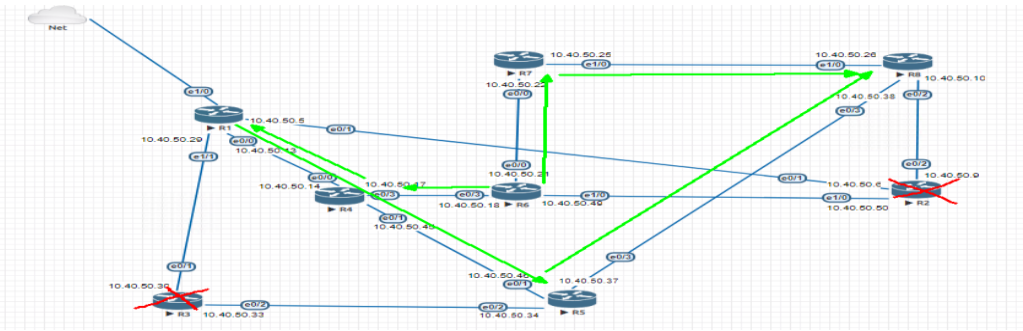
ნახ. 15. vrf VOIP-გვირაბისთვის R2 და R3-მარშრუტიზატორების შეზღუდვა

R2 და R3 მარშრუტიზატორების ცენტრალური პროცესორის გადატვირთვის შესახებ შეტყობინების მიღების შემდეგ vrf VOIP-ის მოქმედებაში არსებულ მარშრუტიზატორებზე ჩართული MPLS-TE გამოთვლის ახალ უსაფრთხო მარშრუტებს (ნახ. 16).

```
 OutLabel : Ethernet1/0, 17
 RSVP Signalling Info:
      Src 8.8.8.8, Dst 6.6.6.6, Tun_Id 1, Tun_Instance 35
   RSVP Path Info:
     My Address: 10.40.50.26
     Explicit Route: 10.40.50.25 10.40.50.21 6.6.6.6
OutLabel : Ethernet0/0, 18
RSVP Signalling Info:
     Src 1.1.1.1, Dst 8.8.8.8, Tun_Id 1, Tun_Instance 44
  RSVP Path Info:
    My Address: 10.40.50.13
    Explicit Route: 10.40.50.14 10.40.50.46 10.40.50.38 8.8.8.8
    Record   Route:   NONE
RSVP Signalling Info:
     Src 6.6.6.6, Dst 8.8.8.8, Tun_Id 1, Tun_Instance 16
  RSVP Path Info:
    My Address: 10.40.50.21
    Explicit Route: 10.40.50.22 10.40.50.26 8.8.8.8
    Record   Route:   NONE
```

ნახ. 16. გვირაბის კონფიგურაცია

ნახ. 17-ზე წარმოდგენილია ისეთი შემთხვევა, როდესაც R2 და R3 პროცესორები გადატვირთულია და ისინი აღარ გამოიყენებიან vrf VOIP-ტრაფიკის გადაცემისათვის.



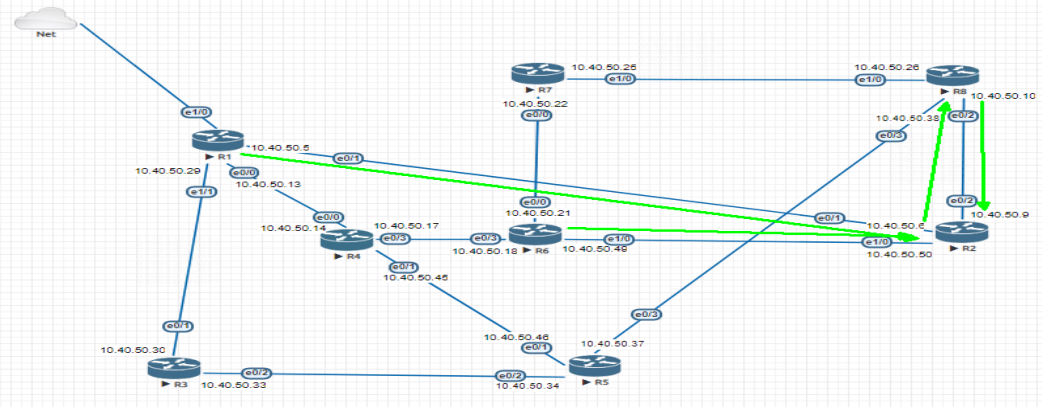
ნახ. 17. R2 და R3 კვანძების პრობლემის დროს vrf VOIP ტრაფიკის გადაადგილება

4. შეტყობინება R2 და R3 მარშრუტიზატორების ცენტრალური პროცესორის ნორმალური დატვირთულობის შესახებ, რომლის მიხედვითაც მე-3 პუნქტში წარმოდგენილი პრობლემის მოგვარების სიმულაციისას NACS-სერვერი იღებს აღნიშნულ შეტყობინებას და ამუშავებს მას (ნახ. 18).

```
R2_LAB 2.2.2.2 High CPU <90%
Listen to new message
finding index by 1.1.1.1CPU_Reset
    2
finding index by 8.8.8.8CPU_Reset
    2
finding index by 6.6.6.6CPU_Reset
    2
we found more then one index and execute config 1.1.1.1CPU_Reset
we found more then one index and execute config 8.8.8.8CPU_Reset
we found more then one index and execute config 6.6.6.6CPU_Reset
R3_LAB 3.3.3.3 High CPU <90%
Listen to new message
finding index by 1.1.1.1CPU_Reset
    1
finding index by 8.8.8.8CPU_Reset
    1
finding index by 6.6.6.6CPU_Reset
    1
we found only one index and execute config 1.1.1.1CPU_Reset
we found only one index and execute config 8.8.8.8CPU_Reset
we found only one index and execute config 6.6.6.6CPU_Reset
```

ნახ. 18. NACS-ის მიერ შეტყობინების მიღება და დამუშავება

CPU-ს გადატვირთულობის პრობლემის მოგვარების შემდგომ R1, R6 და R8-ზე მოიხსნება R2-და R3-ის მარშრუტის შეზღუდვა და vrf VOIP-ტრაფიკი იმოძრავებს OSPF-ით მიღებული უმოკლესი მარშრუტით (ნახ.19).



ნახ. 19. vrf VoIP-ტრაფიკის მოძრაობის სურათი პრობლემის მოხსნის შემდეგ

დასკვნები

ძირითადი შედეგები, რომლებიც მიღებულია სადისერტაციო ნაშრომში, შემდეგია:

1. შეფასებულია VoIP-ქსელების კომპონენტები და უსაფრთხოების რისკები და შემუშავებულია VoIP-უსაფრთხოების მოდელი, რომლის განხორციელება უზრუნველყოფს VoIP-ქსელის მომხმარებელთა ხმოვანი ტრაფიკის ხელმისაწვდომობას, მთლიანობასა და კონფიდენციალობას;

2. გაანალიზებულია MPLS-ქსელის არქიტექტურა და MPLS-TE-ტექნოლოგია, რომლის საფუძველზეც დადგინდა, რომ MPLS მოქნილი ტექნოლოგიაა, რომელიც უზრუნველყოფს უსაფრთხოებას, პაკეტების დაგვიანების მინიმიზაციასა და მონაცემთა გადაცემას მაღალი სიჩქარით;

3. ნაჩვენებია, რომ MPLS-ქსელის არქიტექტურისა და MPLS-TE-ტექნოლოგიის ერთობლიობა ძირითადად გამოიყენება სერვის-

პროვაიდერების მიერ რეალურ დროში გადაცემული ხმოვანი და ვიდეო-სერვისების გაუმჯობესებული ხარისხით მისაწოდებლად;

4. დადგენილია, რომ MPLS-ის ერთ-ერთი მნიშვნელოვანი ფუნქცია ტრაფიკის ინჟინერინგია (TE), რომელიც მნიშვნელოვან როლს ასრულებს ქსელური დატვირთვის მინიმიზაციისთვის, რესურსების რეზერვაციისთვის, ბალანსირებისა და მართვისთვის და რომლის საშუალებითაც განისაზღვრება მონაცემების უსაფრთხო და ხარისხიანი მარშრუტიზაცია;

5. დამუშავებულია მონაცემთა ნაკადის გვირაბების (Tunnels), ვირტუალური მარშრუტიზაცია-გადამისამართების (VRF) პროტოკოლების ავტომატიზაციის პროგრამულ უზრუნველყოფასთან ინტეგრაციის მეთოდი, რამაც უზრუნველყო ხმისა და ინტერნეტ-ტრაფიკის ერთმანეთისა და გლობალური მარშრუტიზაციის ცხრილიდან იზოლაცია;

6. დამუშავებულია რეალური IP-MPLS-ის ანალოგიური ქსელი ვირტუალურ პროგრამულ EVE-NG-გარემოში, რამაც უზრუნველყო შესაბამისი ალგორითმის მოდელირების, IP-MPLS ქსელის სიმულაციის, ქსელური პრობლემისა და მისი მოგვარების განხორციელების შესაძლებლობა.

7. დასაბუთებულია ქსელის მონიტორინგის პროგრამული უზრუნველყოფის გამოყენებისა და სატესტო გარემოში სიმულაციის შესაძლებლობა;

8. განხორციელებულია ინტერნეტისა და ხმოვანი სიგნალების მონაცემების ერთმანეთისგან იზოლირებისა და ხმოვანი სიგნალის ტრაფიკის წყაროზე დაფუძნებული მარშრუტიზაციის (SR) ოპერაციები;

9. რეალიზებულია ქსელის მონიტორინგის შემუშავებულ სისტემაში მიმდინარე პროცესების ვიზუალიზაციისა და რეალურ დროში დაკვირვების შესაძლებლობა, რამაც უზრუნველყო მონიტორინგის სისტემის მოქნილობა და მისი ეფექტურობის გაუმჯობესება.

10. შემუშავებულია გადაცემის პაკეტური საკომუტაციო ქსელის მართვის, მონიტორინგისა და ინტელექტუალური გადაწყვეტილებების მიმღები სისტემა, რომელიც ქსელში დაფიქსირებული პრობლემების დროს პროგრამული ალგორითმების დახმარებით გადაწყვეტს ქსელური მოწყობილობების კონფიგურაციის ოპტიმიზაციის ამოცანას და დაახარისხებს შესრულებულ ქმედებებს.

დისერტაციის თემაზე გამოქვეყნებული შრომები

1. Irakli Jorjadze. Analysis of Security issues in VoIP (Voice over IP Protocol) Technology and Development of a Security Model. Gtu and Unifg 1ST joint R&D International Conference “Dynamics and Recent Trends of Vary Industries In EU and Georgia: ICTS Adoption in Supply Chain Management”. © Publishing House “Technical University”, 2018, 17-19 October, Tbilisi, Georgia, pp. 52-55.
2. აბულაძე ვ., ხუნწარია ჯ., ჯორჯაძე ი., გიორგაძე გ. ხმოვანი სიგნალის გადაცემის ქსელის უსაფრთხოების მოდელი. “ენერგია”, 2019, №1(89), გვ. 90-95.
3. აბულაძე ვ., ხუნწარია ჯ., ჯორჯაძე ი., გიორგაძე გ. MPLS ქსელში მონაცემთა ნაკადის ავტომატური მართვის მოდელი. “მართვის ავტომატიზებული სისტემები”, 2019, №1(28), გვ. 106-111.
4. გიორგაძე გ., ჯორჯაძე ი., აბულაძე ვ., ხუნწარია ჯ. მეოთხე თაობის რადიო ქსელის დატვირთვისა და გამტარუნარიანობის ანალიზი. “მართვის ავტომატიზებული სისტემები”, 2019, №1(28), გვ. 112-117.

Resume

The work includes the results of the theoretical and experimental research on the Dissertation topic "Elimination of problems related to the transmission of voice signals with data transmission networks and the elaboration of appropriate protection mechanisms".

The modern telecommunication providers networks are complex and offer users a variety of services that provide various technologies and protocols in the provider's network

The demand for multimedia applications in the internet network has increased the frequency and demands of data transfer in recent years. Providing users with the best quality services is associated with many problems such as delay in packets, loss of them, change of time intervals between the packets, etc. For solving these problems, technology can be used as a Multi-protocol Label Switching protocol (MPLS), which ensures safety of transmitted packets, minimizing their time of delay and transmission at high speed.

Therefore, MPLS-networks use the switching method instead of standard routing, and they do not replace the existing IP-networks, but in combination with them to provide improved quality of services and to manage the suitable environment. MPLS's important function is Traffic Engineering (TE), which plays an important role in minimizing network loads, resource surveillance, traffic balance and management. The network performance efficiency is evaluated by considering certain network parameters, most of which are the delay, the packet delay variation (jitter) and the packet loss (packet loss). With the MPLS-TE quality of service (QoS), it is possible to improve network efficiency. That is why MPLS-TE can provide data safe and quality routing. network traffic, a large volume of existence and the unexpected problems arising, such as the physical link damage , the network of hacker attacks, and in such variety, such as the distributed denial-of-service (DdoS), At the same time, data transfer channels increase the traffic to critical levels and often fill the bandwidth limit. For this it is necessary to manage the network data stream, which is also appropriate for routers, switches, and other hardware problems. In such cases, instant change of routing configuration should be performed. In case of network engagement, this process requires a lot of time and it leads to increasing the likelihood of mechanical errors.

Therefore, Multi-protocol Label Switching (MPLS) is a flexible technology that provides security, minimizing delay of network data packets and high data transmission. It is mainly used by service providers and is the ideal way to deliver real-time voice and video services. VoIP over Internet Protocol (VoIP) is the ultimate product of many protocols, and with its development it is necessary to develop the integrity and confidentiality issues of its components.

Experience shows that optimal routing of traffic in the service provider's network is associated with many problems, as the providers have channels with high bandwidth transfers, increasing the capacity of these channels or adding them to big finances. Therefore providers are forced to use the resources available on their

network, which can not be done using standard internal routing protocols. At this time specialists refer to traffic engineering (MPLS-TE), which is almost excluded from the service provider's Internet-network.

However, as indicated in the use of MPLS-TE, the network is not insured from some kind of problem that has been developed the NACS system with adaptive algorithms to resolve the problem of networking devices and optimize the configuration of network devices. In addition, it will be possible to visualize these processes and monitor them in real time.

In this work the process of integration of data flow tunnels (Tunnels), Virtual Routing and Forwarding (VRF) protocol automation software is developed, which ensured isolation from the Internet and Internet traffic between each other and from the Global Routing Table.

The work has also developed, so called NACS-system logic scheme of the so-called network configuration, developed by the relevant software code, its implementation technique and the ability to integrate with the monitoring system. With the development of a similar network of real IP-MPLS in virtual software EVE-NG environments, modeling of algorithm, IP-MPLS-network simulation and solving network problems.