Georgian Scientists
ქართველი მეცნიერები
Vol. 6 Issue 2, 2024
https://doi.org/10.52340/gs.2024.06.02.11

მონაცემთა გადაცემის ქსელების პროექტირებისა და ოპტიმიზაციის შესახებ

მამუკა ჩხაიძე[1], გიორგი მურჯიკნელი[2]

[1] ასოცირებული პროფესორი, საქართველოს ტექნიკური უნივერსიტეტი. chkhaidzemamuka08@gtu.ge. Orcid-0009-0004-4021-8407; [2] დოქტორანტი, საქართველოს ტექნიკური უნივერსიტეტის სადოქტორო პროგრამა „ციფრული სატელეკომუნიკაციო ტექნოლოგიები“. Orcid-0009-0005-2339-0878

აბსტრაქტი

ნაშრომში განიხილება პრობლემები, როგორიცაა ორი არქიტექტურის გაერთიანება ინფრასტრუქტურებში. წარმოდგენილია MPLS (Multiprotocol Label Switching), VPN (Virtual Private Network) და BSG (Border Gateway Protocol) რისკების ანალიზი, რაც სასრგებლო შეიძლება იყოს თანამედროვე საკვლევი სამყაროსათვის.

საკვანძო სიტყვები: უსაფრთხოება, მასშტაბურობა, ტოპოლოგია, ოპტიმიზაცია

ინტერნეტის განსაკუთრებულ ძლიერ მხარეს მისი უზარმაზარი მასშტაბურობა და მოქნილობა წარმოადგენს, რომელიც საშუალებას იძლევა განთავსდეს უამრავი დანართი.

ნებისმიერი კომპიუტერული ქსელის ფუნდამენტური ამოცანა მდგომარეობს უზრუნველყოს კავშირი მის სასრულ წერტილებს შორის, ანუ სისტემის მართვის მთავარ საშუალებას ავტომატიზირებული ვერიფიკაცია წარმოადგენს.

მონაცემთა გადაცემის მომსახურების გზას აღადგინოს სისტემა მწყობრიდან გამოსვლის შემდეგ მნიშვნელოვანი ასპექტია თანამედროვე და მომავალი IP (Internet Protocol) და სატრანსპორტო ქსელებისთვის.

ამ თვალსაზრისით MPLS წარმოადგენს უახლოეს ტექნოლოგიას, რომ დააკმაყოფილოს გაზრდილი მოთხოვნები გამტარუნარიანობისა და მიერთების შემთხვევაში, რაც საშუალებას იძლევა ამოვხსნათ ისეთი პრობლემები, როგორიცაა მასშტაბურობა და უსაფრთხოება (Previdi, 2000).

საბაზისო არხის მთავარი მოთხოვნაა უზრუნველყოს უსაფრთხოება, საიმედო და თანმიმდევრული კავშირი.

მომსახურების ხარისხის (QoS – Quality of Service) მართვის პოლიტიკის წესი QoS-ის საშუალებით მიღწევადია, დაკავშირებულია კვლევებთან, იძლევა საშუალებას QoS შეეხოს მთელ VPN-ს.

მასშტაბურობის პრობლემა - ასოციაციების ძალზე დიდი სიმრავლე VPN ქსელის მიერ მარტივად წარმოებადია და ადვილად მხარდაჭერილია ინტერნეტით.

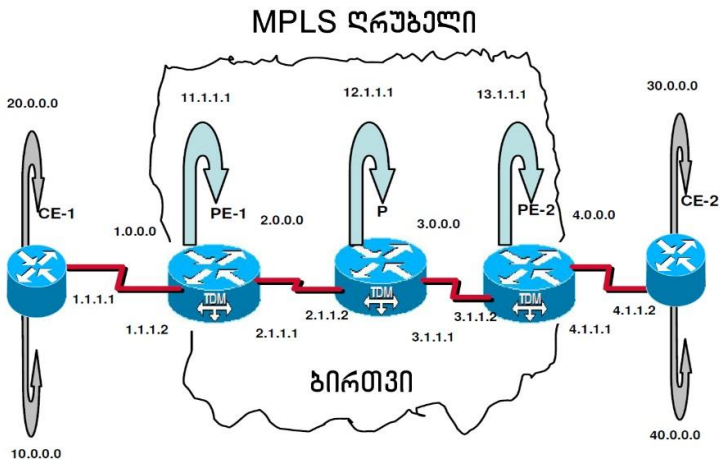
უსაფრთხოების პრობლემა - ბევრი ვირუსი დახეტიალობს VPN სასრულ წერტილებში, რომლებიც იწვევენ არხების უსაფრთხოების დაშლას, დანგრევას.

იმსათვის, რომ დააკმაყოფილოს უსაფრთხოების მოთხოვნა და ეფექტურობა მაგისტრალურ ქსელებში MPLS მიმართულია წარმოადგინოს გაუმჯობესებული მექანიზმები, რომლებიც შეუმსუბუქებენ ინტერნეტ-პროვაიდერებს ადვილად შეისწავლონ და დააკმაყოფილონ სხვადასხვა მოთხოვნები მომსახურებაში მთელ მსოფლიოში (Alawieh B., Ahmed R.E., and Mouftah HT., 2008).

ინტელექტუალური მარშრუტიზაციის მაქსიმალური გამოყენება და სწრაფი კომუტატორები გვთავაზობენ ტექნოლოგიებს, რათა მთლიანად შეივსოს IP სეგმენტის მოცულობა.

მომსახურების მსგავსი დონის მოთხოვნები მარშრუტიზაციის ორგანიზაციის მიზნით იყენებენ ერთიდაიგივე გზა-მარშრუტებს ქსელში, რასაც მივყავართ შეათანხმოს მომსახურების მაღალი დონე ქსელურ ნაკადებთან.

დღესდღეობით MPLS მიდის იმ მიზნისკენ, რომ განავრცოს მთელ არქიტექტურაში (ხერხემალში) პირველ რიგში (Rosen E. and Rekhter Y., 1999).



ნახ.1. ქსელის ტოპოლოგია

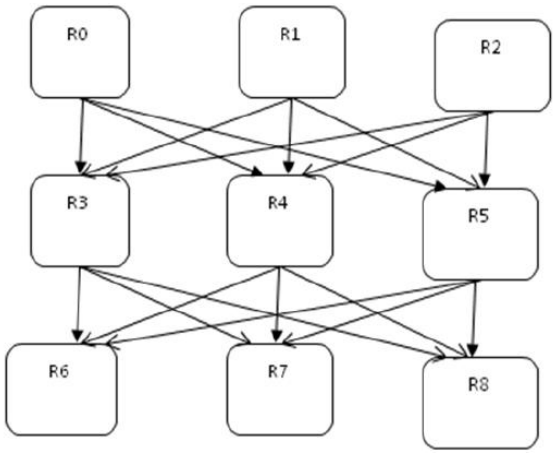
არხის ტოპოლოგია - შემოთავაზებულია სისტემა MPLS არხის ბირთვში რეალიზდება “Danagen” სტიმულატორის საშუალებით, რომელშიც ქსელის ტოპოლოგია შედგება ხუთი მარშრუტიზატორისგან (ნახ.1).

მარშრუტიზატორი რომელიც იღებს გარე ტრაფიკს MPLS VPN-ის კიდეზე გადაამისამართებს მის ბირთვში მარკირების შემდეგ (Ferguson P. and Huston G., 1998).

ერთი ქსელიდან შემოსული და ბირთვში გადამისამართებული ინფორმაცია წარმოადგენს ერთისათვის გასასვლელს, რომელიც შედის ბირთვში და გადაიგზავნება MPLS სისტემის ღრუბლებს იქით.

საბაზისო მარშრუტიზატორი უბრალოდ გადართავს „teg“-ით, რომელიც შესაძლებელს ხდის გაცილებით გაასუმჯობესოს ტრაფიკის გადამისამართება.

სასაზღვრო პროვაიდერის მარშრუტიზატორი ანიჭებს ნიშნულებს მის არელაში დაკავშირებულ ნიშნულებთან საწყისი სასაზღვრო მარშრუტების ქსელში.



ნახ.2. შემოთავაზებული არქიტექტურა

დასკვნა

სტატიაში განხილულია სხვადასხვა აღდგენის მეთოდი სისტემის მწყობრიდან გამოსვლის შემთხვევაში. უპირატესობები და ნაკლოვანებები სხვადასხვა მეთოდების ანალიზის საშუალებით, არხის ტოპოლოგიის არქიტექტურის გათვალისწინებით.

ლიტერატურა

1. Previdi, S. (2000, April). Introduction to MPLS-BGP-VPN. Proceeding of MPLS Forum 2000. Cisco.

2. Alawieh B., Ahmed R.E., and Mouftah HT. (2008, July). Security impacts on establishing MPLS/BGP VPNs. Journal of Security and Communication Networks, Volume 1, No. 4, pp. 269-275.

3. Rosen E. and Rekhter Y. (1999). BGP/MPLS VPNs, RFC 2547.

4. Ferguson P. and Huston G. (1998, September). What is VPN. The Internet Protocol Journal, Volume 1, No. 2.

About projecting and optimization of data transmission networks

Mamuka Chkhaidze[1], Giorgi Murjikneli[2]

[1] Associate Professor, Georgian Technical University. chkhaidzemamuka08@gtu.ge.

Orcid-0009-0004-4021-8407; [2] Doctoral student, Georgian Technical University, doctoral program "Digital Telecommunication Technologies". gurjikneli@gmail.com. Orcid-0009-0005-2339-0878

Abstract:

Problems such as combining two architectures in infrastructures are discussed in the paper. MPLS (Multiprotocol Label Switching), VPN (Virtual Private Network) and BSG (Border Gateway Protocol) risk analysis are presented, which can be beneficial for the modern research world.

Keywords: Security, scalability, topology, optimization