ივ. ჯავახიშვილის სახ. თბილისის სახელმწიფო უნივერსიტეტი
ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი

კონსტანტინე შალამბერიძე

BGP პროტოკოლის უსაფრთხოება IPv6-ის ბაზაზე

სამაგისტრო პროგრამა: ინფორმაციული ტექნოლოგიები

სამაგისტრო ნაშრომი შესრულებულია კომპიუტერული მეცნიერებების მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

სამაგისტრო ნაშრომის ხელმძღვანელი
ასისტენტ-პროფესორი: პაპუნა ქარჩავა

თბილისი
2017

ანოტაცია

ამ ნაშრომში ჩვენ განვიხილეთ BGP-ის მარშუტიზაციის პროტოკოლის უსაფრთხოებას IPv6-ის ბაზაზე, რადგან BGP წარმოადგენს ერთადერთ პროტოკოლს საერთაშორისო მარშუტიზაციისთვის და მისი მნიშვნელობა დიდია გლობალურ ინტერნეტში, მაგრამ ისმის კითხვა, რატომ ავირჩიეთ BGP-ის უსაფრთხოება IPv6-ში და არა IPv4-ში, მიზეზი ამისა მდგომარეობს შემდეგში, როგორც ჩვენ ვიცით ყოველდღიურად მატულობს ინტერნეტთან დაკავშირებული მოწყობილობების რაოდენობა, ხოლო IPv4-ის მისამართების რაოდენობა კლებულობს, ამიტომ ადრე თუ გვიან საჭირო გახდება მე-4 ვერსიის პროტოკოლის ჩანაცვლება მე-6 ვერსიით და ამან შესაძლოა პრობლემები გამოიწვიოს გლობალური ინტერნეტის უსაფრთხოების განხრით და ჩვენ უნდა ვიყოთ მზად მომავლისთვის, უნდა შევქმნათ პრობლემის გადაჭრის ძირითადი გზები, რომელიც ამ ინოვაციასთან არის დაკავშირებული და მე ვიმედოვნებ, რომ ეს ნაშრომი იქნება სასარგებლო BGP-ის IPv6-ის პროტოკოლში არსებული საფრთხეების გამკლავებაში.

Abstract

On this work we discussed security threats in bgp ipv6 routing protocol, because bgp is the only protocol, that used in global routing. You may ask, so why we choose ipv6 instead of ipv4, the answer is simple, nowadays internet devices, that need ip addresses are growing and the resources of ipv4 adresses are quickly reduced, so sooner or later we will need to change version 4 internet protocol with newer ipv6 and these may lead us to more problems in global internet and we need to be ready for tomorrow and make the basic solution to reduce problems with this innovation. I hope that this work will be helpful to prevent main security threats in bgp ipv6 routing protocol.

შინაარსი

შესავალი

გამოთვლითი მანქანების გამოჩენის პირველივე დღიდან არ შეწყვეტილა სამუშაოები გაუმჯობესებინათ ის, გაეხადათ უფრო უსაფრთხო და ხელმისაწვდომი ნებისმიერი მსურველისათვის. ტექნოლოგიების სწრაფმა განვითარებამ პერსონალური კომპიუტერები ხელმისაწვდომი გახადა ნებისმიერი ადამიანისათვის. რიგ შემთხვევებში ადამიანებს უკვე აქვთ რამდენიმე პერსონალური კომპიუტერი. ასევე, გამოჩნდა მრავალი ახალი მოწყობილობა, რომელიც მნიშვნელოვან როლს თამაშობს ადამიანის ყოველდღიურ ცხოვრებაში. ძველმა მოწყობილობებმა, რომლებიც იყვნენ პოპულარულები ჰპოვეს განვითარება და შეიძინეს ქსელის გამოყენებით კომუნიკაციის შესაძლებლობა. ადამიანები უკვე დიდი ხნით რჩებიან ქსელში, კომუტირებენ ერთმანეთთან, გეგმავენ საკუთარ დასვენებას და ა.შ.

ქსელში გამოყენებული ყოველი მოწყობილობა კომუნიკაციის შესაძლებლობის მიზნით საჭიროებს იდენტიფიცირებას. მხოლოდ ლოგიკურად იდენტიფიცირებულ მოწყობილობებს შეუძლიათ ქსელის მეშვეობით მონაცემების მიღება/გადაცემა. მოწყობილობათა ლოგიკური იდენტიფიცირების მიზნით გასული საუკუნის 80-იან წლებში IEEE-ს (Institute of Electrical and Electronic Engineers) მიერ შემოღებული იქნა IP (Internet Protocol) პროტოკოლი (მეოთხე ვერსია - IPv4). IPv4 პროტოკოლის დამპროექტებლების მიერ მოწყობილობათა იდენტიფიცირებისათვის გამოყენებული იყო დამისამართების 32-თანრიგა ორობითი სისტემა, რაც იძლეოდა დაახლოებით 4,3 მილიარდი მოწყობილობის დამისამართების შესაძლებლობას.

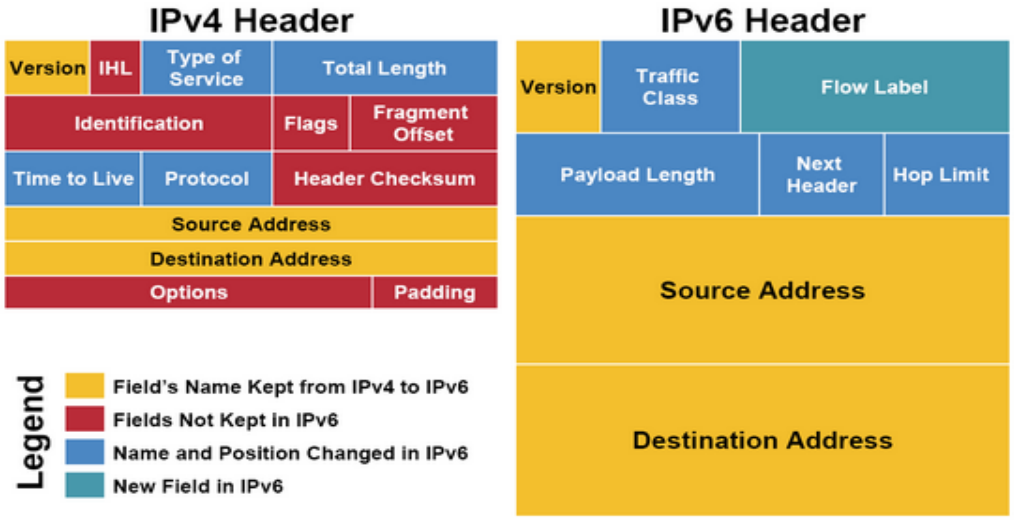
ტექნოლოგიების სწრაფმა განვითარებამ შესაძლებელი გახადა თითქმის ყველა სამომხმარებლო მოწყობილობებისათვის დამატებოდა ქსელში კომუნიკაციის შესაძლებლობა, რაზეც უარი არ თქვეს შესაბამისი მოწყობილობების მწარმოებლებმა (როგორიცაა ტელევიზორები, მაქნანის მაგნიტაფონები და სხვა). უფრო მეტიც ასეთი მოწყობილობების მწარმოებლები საკუთარ პროდუქტის პოპულარიზაციის მიზნით მიმართავენ ამ შესაძლებლობის ჩადებას მასში. სამომხმარებლო მოწყობილობებისათვის ქსელში კომუნიკაციის დამატების შესაძლებლობამ წარმოშვა დამატებით პრობლემა, რომელიც დაკავშირებულია IPv4 პროტოკოლის მიერ მოწყობილობათა დამისამართებისათვის გამოყენებული სივრცეში მისამართების სიმცირესთან. 2016 წლის მონაცემებით ინტერნეტ ქსელთან დაკავშირებული მომხმარებლების რაოდენობამ შეადგინა 3,5 მილიარდი.

IPv4 პროტოკოლის დამპროექტებლები მისი შექმნის პერიოდში ვერც კი იფიქრებდნენ, რომ ინტერნეტი შეიძლებოდა გამხდარიყო ისეთი პოპულარული როგორიც დღესაა. ასევე, რადგანაც ქსელური ტექნოლოგიების შემუშავების საწყის ეტაპზე იგეგმებოდა მისი გამოყენება მხოლოდ სამეცნიერო დაწესებულებებისა და სამთავრობო ორგანიზაციების მიერ გამოყენების მიზნით, ამიტომ ასეთი ტექნოლოგიების შემქმნელები ვერს კი წარმოიდგენდნენ იმ საფრთხეების შესახებ რაც თანამედროვე ქსელებში გამოჩნდა. შესაბამისად რაიმე სახის უსაფრთხოების მექანიზმები არ ყოფილა გათვალისწინებული არც IPv4 პროტოკოლში და არც იმ დროისათვის შემუშავებულ სხვა მრავალ პროტოკოლში. BGP (Border Gateway Protocol) პროტოკოლი წარმოადგენს ერთერთ ასეთ პროტოკოლს. ის შეიქმნს გასული საუკუნის 80-ანი წლების ბოლოს. ეს არის პროტოკოლი, რომელზეც დამყარებულია მთლიანი Internet ქსელი და მისი ნორმალური ფუნქციონირება და ქსელური სერვისების ხელმისაწვდომობა, როგორცაა Web-სერვისები: email, clowd, ფულადი ტრანზაქციები და სხვა. IPv4 პროტოკოლის მსგავსად BGP პროტოკოლშიც არ ყოფილა რაიმე სახის უსაფრთხოების მექანიზმი ჩადებული.

უსაფრთხოებასთან დაკავშირებული სიტუაცია შეცვალა 90-იან წლებში გამოჩენილმა ე.წ. „ჭიამ“ (worm). ჭიას მოჰყვა სხვა დღეისათვის ცნობილი მეთოდები (როგორიცაა ტროიანის ცხენები, malware და სხვა), რომლებიც საფრთხეს უქმნიან ქსელურ კომუნიკაციას და მონაცემების კონფიდენციალურობას. ამ დროიდან მოყოლებული აქტიურად მიმდინარეობს სამუშაოები უსაფრთხოების უზრუნველსაყოფად სხვადასხვა ახალი ტექნოლოგიების შემუშავებისა. შემუშავდა მრავალი ასეთი ტექნოლოგია (როგორიცაა IPSec, VPN, Tunel და სხვა), როგორც დანამატი შესაბამის პროტოკოლზე. ასეთმა ტექნოლოგიებმა გაზარდეს უსაფრთხოების საკითხი, მაგრამ ყოველი ახალი ტექნოლოგიის შემუშავების შემდეგ არ ცხრება არაკეთილმოსურნე მხარის მიერ ახალახალი მეთოდების შემუშავების მცდელობა, რითაც ისინი შეძლებენ უსაფრთხოების გვერდის ავლით მიაღწიონ სასურველ შედეგს.

Internet ქსელის სწრაფმა პოპულარიზაციამ და იმ პერიოდისათვის დაფიქსირებულმა სხვადასხვა სახის პრობლემებმა (არასაკმარისი დამისამართების სივრცე, უსაფრთხოება) IP პროტოკოლის დამპროექტებლებს მისცა ბიძგი შეექმნათ ახალი პროტოკოლი, რომელშიც გათვალისწინებული იქნებოდა IPv4 -სათვის დაფიქსირებული ნაკლოვანებები. შედეგად გამოჩნდა IP პროტოკოლის ახალი ვერსია 6 (IPv6).

IPv6 პროტოკოლში მოწყობილობათა დამისამართებისათვის გამოიყენება 128 თანრიგა ორობითი მნიშვნელობა, რაც გაცილებით მეტი მოწყობილების დამისამართების საშუალებას იძლევა. გარდა ამისა, შეცვლილია პაკეტის თავსართი (ნახ. 1). ახალ თავსართში შემცირებულია ველების რაოდენობა (ამოღებულია ზოგიერთი არააუცილებელი ველი და შემოღებულია ზოგიერთი ახალი ველი). IPv6 პროტოკოლში უსაფრთხოების უზრუნველსაყოფად ჩადებულია IPSec უსაფრთხოების მექანიზმი.



ნახ. 1. განსხვავება IPv4 და IPv6 პაკეტების თავსართებს შორის

IPv6 პროტოკოლს უნდა ჩაენაცვლებინა მისი წინამორბედი, მაგრამ ჯერჯერობით ამის გაკეთება არის შეუძლებელი საჭირო ცვლილებისთვის თანმდევი ფინანსური და მატერიალური დანახარჯების გამო. სახელდობრ, საჭიროა სრულად შეიცვალოს ის ქსელური მოწყობილობები, რომლებსაც არ გააჩნიათ IPv6 პროტოკოლის მხარდაჭერა. ასევე, საჭიროა მოხდეს შესაბამისი პერსონალის გადამზადება. ამ ყველაფერს კი დიდი ფინანსური მხარდაჭერა სჭირდება. რადგანაც IPv6 შიქმნა არსებული ცოდნისა და გამოცდილების გათვალისწინებით, ამიტომ ის წარმოადგენს IPv4-ის ერთადერთ ხანგრძლივ შემცვლელს.

უნდა აღინიშნოს რომ, IPv6 პროტოკოლს, ისევე, როგორც თითქმის ყველა სხვა პროტოკოლს გააჩნია უსაფთხოებასთან დაკავშირებული გარკვეული პრობლემები და მისი

პოპულარობის ზრდასთან ერთად იზრდება საფთხეებიც, ამიტომ მნიშვნელოვანია დროულად მოხდეს საფრთხეების დეტექცია, პრევენცია და მათი აღმოფხვრა.

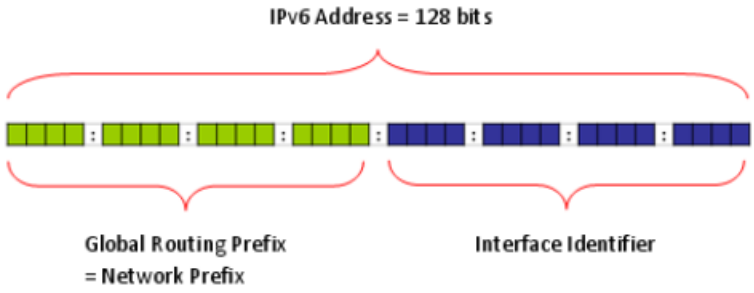
როგორც უკვე აღვნიშნეთ, BGP არის დინამიური მარშრუტიზაციის პროტოკოლი Internet ქსელში რომელზეც დაფუძნებულია მთლიანი Internet ქსელის ნორმალური ფუნქციონირება. როუტერები, რომლებზეც ამუშავებულია BGP პროტოკოლი, მათთვის უკვე ნაცნობ ქსელებზე ინფორმაციას ერთად ერთმანეთთან ცვლიან ამავე ქსელებზე სხვადასხვა სახის ატრიბუტებს. ასეთი ატრიბუტების მეშვეობითაც როუტერები ირჩევენ საუკეთესო გზას დანიშნულების ქსელის მიმართულებით და იყენებენ მათ აქტიური გაცვლის პერიოდში. ერთერთ ასეთ ატრიბუტს წარმოადგეს ავტონომიური სისტემის ნომერზე ინფორმაცია, რომელმაც გამოაგზავნა შესაბამისი მონაცემები. ავტონომიური სისტემის ნომრების მიხედვით როუტერი განსაზღვრავს მათ ადგილმდებარეობას და განსაზღვრავს მარშრუტიზაციის პოლიტიკას. განისაზღვრება შიდა/გარე ავტონომიურ სისტემებს შორის გზის განსაზღვრის პოლიტიკები და აღიწერება მათი ურთიერთქმედების წესები.

რადგანაც როუტერები მასზე ამუშავებული BGP პროტოკოლის ბაზაზე მარშრუტიზაციის ცხრილში შეიცავს დიდი რაოდენობით (რამდენიმე ასეული ათასი) ჩანაწერს, ამიტომ მნიშვნელოვანია ასეთი როუტერები ფუნქციონირებდნენ სრულფასოვნად. მათი მწყობრიდან გამოსვლის შემთხვევაში შეიძლება Internet ქსელმა შეწყვიტოს ფუნქციონირება, რაც დაუშვებელია.

სამაგისტრო ნაშრომი შეეხება IPv6 პროტოკოლის ბაზაზე BGP პროტოკოლის უსაფრთხოების საკითხს. მასში განხილულის BGP პროტოკოლის საფრთხეების ტიპები, მათი აღმოჩენისა და დროული პრევენციის მეთოდები.

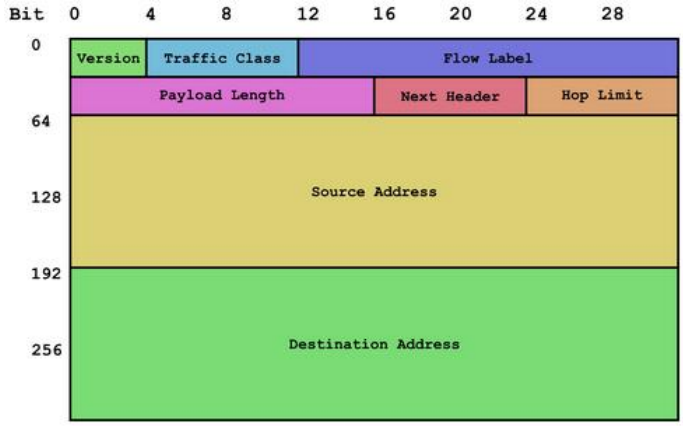
1. IPv6 პროტოკოლი

IPv6 პროტოკოლი (Internet Protocolversion 6) წარმოადგენს ახალ პროტოკოლს როგორც ლოკალურ და გლობალურ ქსელში მოწყობილობათა დამისამართებისათვის. ამ მიზნით მასში გამოიყენება 128 თანრიგა ორობითი მნიშვნელობები (მისამართები, ნახ. 2). შედეგად, მისამართების რაოდენობა 2^{32} -დან (IPv4-ის შემთხვევაში) იზრდება 2^{128} რაოდენობამდე, რაც წარმოადგენს კოლოსალურ მნიშვნელობას.



ნახ. 2. IPv6-ის მისამართის სტრუქტურა

გარდა ამისა IPv6-ში განსაზღვრულია თავსართის ახალი ფორმატი (ნახ. 3). ახალი თავსართი ოპტიმიზირებულია არააუცილებელი და ოფციური ველების გაფართოებულ თავსართში გადატანით. მიუხედავად, IPv6 პროტოკოლისათვის თავსართის გაზრდილი მნიშვნელობისა, ასეთი თავსართის დამუშავება დანიშნულებისაკენ მიმავალ გზაზე განთავსებულ შუამავალ როუტერებზე მოითხოვს პროცესირების ნაკლებ დროს.



ნახ. 3. IPv6-ის პაკეტის ფორმატი.

განვიხილოთ თითოეული ველის ფუნქცია:

Version - ინტერნეტ პროტოკოლის ვერსია, IPv6 შემთხვევაში იწერება მნიშვნელობა 6;

Traffic Class - პაკეტის პრიორიტეტის განმსაზღვრელი;

Flow Label - ნაკადის მარკერი;

Payload Length - დატვირთვის სიგრძე;

Next Header - ახდენს რიგში შემდგომი თავსართის იდენტიფიკაციას;

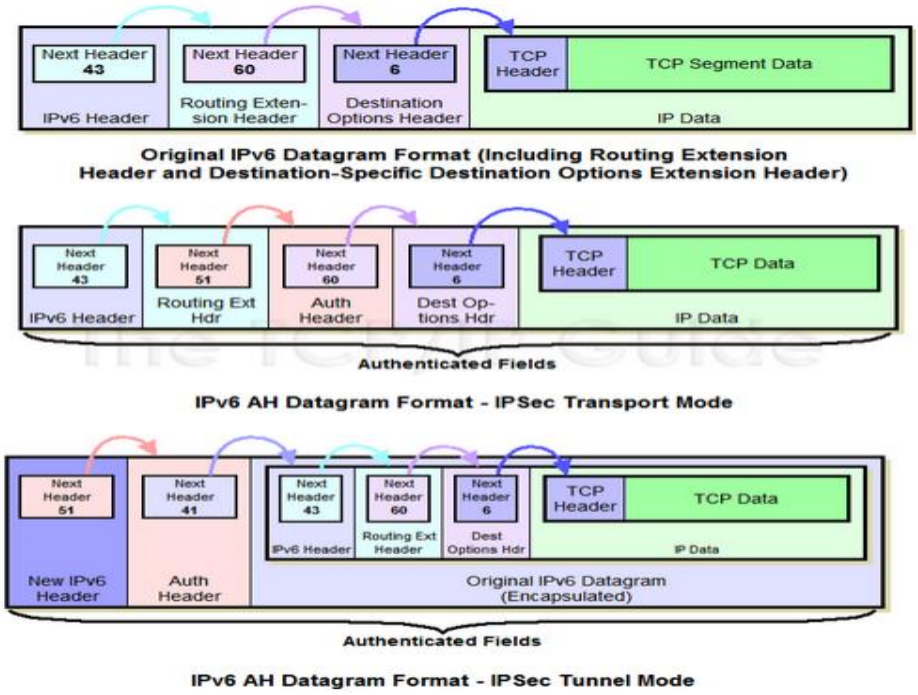
Hop Limit - იგივე TTL რაც IPv4 -ის შემთხვევაში;

Source Address - მონაცემების გამგზავნის მისამართი;

Destination Address - მონაცემების დანიშნილების მისამართი.

უნდა აღინიშნოს, რომ IPv6 -ში გარდა ჩვეულებრივი თავსართისა არსებობს ე.წ. გაფართოებული თავსართი, რომლის მოქმედების ზონა არის ინტერნეტ დონე და ქმნის

თავსართების ერთგვარ ჯაჭვს. ნახ. 4 -ზე ნაჩვენებია გაფართოებული თავსართის სამი მაგალითი. მის ძირითად ფუნქციას წარმოადაგენს სხვადასხვა პროტოკოლების მხარდაჭერა.



ნახ. 4. გაფართოებილი თავსართის ფორმატი

როგორ ცნობილია, შუამავალ მოწყობილობებზე IPv4 პაკეტიდან საჭირო ინფორმაციის მისაღებად ხდებოდა მისი დეკაფსულაცია ტრანსპორტულ დონემდე, რის შემდეგაც ხდებოდა მიღებული ინფორმაციის (რიგ შემთხვევებში არააუცილებელი ველების ჩათვლით) პროცესირება. IPv6 პროტოკოლში გაფართოებული თავსართის მექანიზმის შემოღებით თავიდან აცილებულია მსგავსი აუცილებლობა. კერძოდ, გაფართოებული თავსართების მექანიზმის გამოყენებით აღნიშნული ინფორმაცია (რომელიც ქსელურ დონეზე ემატება პაკეტს) დაჯგუფებულია მსგავსი ფუნქციების მიხედვით სხვადასხვა თავსართებში და მათი პროცესიება (შემოწმება) ხდება იმის მიხედვით თუ რისი გაკეთებაა საჭირო შუამავალ მოწყობილობაზე (მაგალითად, გზის შერჩევა თუ აუთენთიკაცია). ინტერნეტ დონის ინფორმაციის გადანაწილება სხვადასხვა თავსართებში ამცირებს პაკეტის დამუშავების დროს და დატვირთვას პროცესორზე.

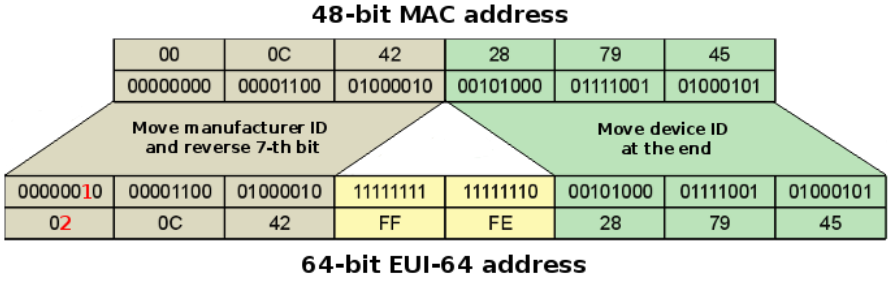
შევნიშნოთ, რომ პროცესირების დროის შემცირება ერთის მხრივ კარგია, მაგრამ მეორეს მხრივ უსაფრთხოების თვალსაზრისით გაფართოებული თავსართი არ არის საკმარისად დაცული ჰაკერული შეტევებისგან. აქ შეიძლება გამოჩნდეს ახალი საფრთხეები, რომლის ანალოგიც IPv4 ქსელში არ არსებობდა.

IPv6-ში სტანდარტული დამისამირათების მეთოდების გარდა დამატებით შემოღებულია დამისამართების ორი ახალი მეთოდი (EUI-64 და SLAAC), რომლის ანალოგი IPv4 ქსელში არ არსებობს. მოკლედ აღვწეროთ თითოეული მეთოდით IPv6 მისამართის დანიშვნის პროცესი.

- **სტატიკური მეთოდი**, რომელიც გულისხმობს მოწყობილობისათვის IPv6 მისამართის დანიშვნისათვის ქსელის ადმინისტრატორის აქტიურ ჩართულობას. ამ შემთხვევაში IPv6 მისამართების დუბლირების და სხვა კონფიგურაციის შეცდომებზე პასუხისმგებლობა ეკისრება უშუალოდ ადმინისტრატორს. მცირე ზომის ქსელის

შემთხვევაში IPv6 მისამართის დანიშვნა მოწყობილობისათვის არაა დაკავშირებული რამენაირ სირთულესთან;

- **EUI-64** (Extended Unique Identifier 64), რომელიც არის სტატიკური მეთოდი და მოწყობილობისათვის IPv6 მისამართის გამოყოფას გულისხმობს მისივე MAC (Media Access Control) მისამართზე დაყრდნობით. ამ შემთხვევაში ქსელის ადმინისტრატორისაგან მოითხოვება IPv6 მისამართის ქსელის ნაწილის მითითება (64 ბიტი), ხოლო IPv6 მისამართის მომხმარებლის ნაწილი (64 ბიტი) მიიღება მოწყობილობის MAC მისამართიდან შემდეგი პრინციპის გამოყენებით (ნახ. 5): მოწყობილობის MAC მისამართი (48 ბიტი) იყოფა ორ ტოლ ნაწილად (24-24 ბიტი) და მათ შორის იწერება 16 ბიტი შემდეგი ფიქსირებული ორობითი მნიშვნელობა 1111111111111110 (თექვსმეტობითი მნიშვნელობა FFFE). ამის შემდეგ, თუ მომხმარებლის ნაწილში მეშვიდე (მარცხნიდან) ბიტი აღმოჩნდა 0 -ის ტოლი მისი მნიშვნელობა შეიცვლება 1-ით, ან პირიქით. ამ ფორმით მიღებული IPv6 მისამართი ენიჭება მოწყობილობას. MAC მისამართის უნიკალურობა უზრუნველყოფს ასეთი IPv6 მისამართის უნიკალურობას.



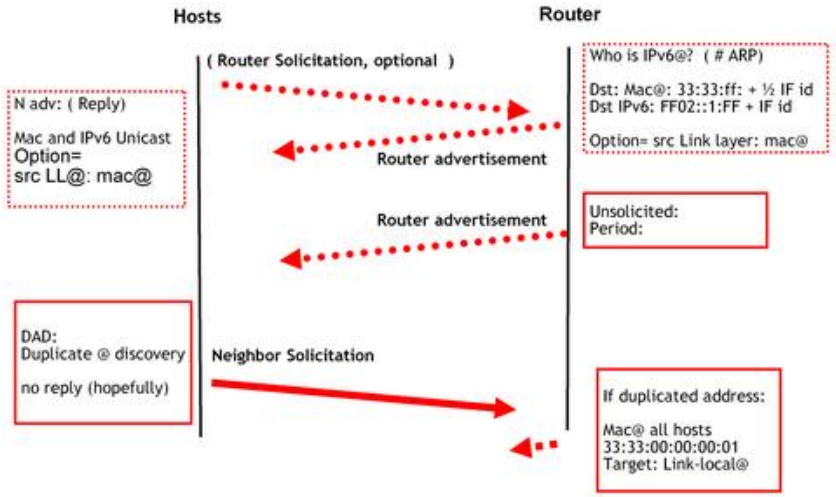
ნახ 5. EUI-64 მეთოდით მიღებილი IPv6 მისამართი

- **DHCP** (Dynamic Host Configuration Protocol), რომელიც არის დინამიური მეთოდი და ის შემოღებული ქსელის ადმინისტრატორის საქმიანობის შემსუბუქების მიზნით. მისი მეშვეობით ქსელში ჩართული ყოველი მოწყობილობა დინამიურად იღებს ქსელში კომუნიკაციისათვის აუცილებელ ყველა პარამეტრს (IPv6 მისამართი, ქსელის პრეფიქსი, gateway, DNS და ა.შ.). მოწყობილობის მიერ კომუნიკაციისათვის აუცილებელი პარამეტრების მიღების პროცესი აღიწერება შემდეგი 4 მოქმედებით (ნახ. 6):
    - **Solicit შეტყობინება.** IPv6 მისამართის საჭიროების მქონე მოწყობილობა (DHCP client) ქსელში აგზავნის DHCP Solicit შეტყობინებას (შეტყობინება იგზავნება multicast მისამართზე). ამ შეტყობინების გაგზავნით მოწყობილობა ცდილობს აღმოაჩინოს შიდა ქსელში ან მოშორებულად გამოყოფილი DHCP server -ი;
    - **Advertise შეტყობინება.** მიღებულ შეტყობინებას DHCP server -ი პასუხობს DHCP Advertise შეტყობინებით, რომელიც შეიძლება იყოს როგორც unicast ისე multicast შეტყობინება. ამ შეტყობინებით DHCP server -ი DHCP client -ს სთავაზობს საკუთარი წყებიდან აღებული კონფიგურაციის პარამეტრების ნაკრებს (IPv6 მისამართი, prefix-ს, DNS-ის მისამართს და ა.შ.);
    - **Request შეტყობინება.** DHCP client -ი DHCP advertise შეტყობინებას პასუხობს DHCP request შეტყობინებით (ეს შეტყობინებაც იგზავნება multicast მისამართზე), რომლითაც DHCP server -ს უდასტურებს მისთვის გამოყოფილი კონფიგურაციის პარამეტრების ნაკრებზე თანხმობას და ელოდება DHCP server -საგან დადასტურების მიღებას;

- **Reply შეტყობინება.** DHCP server -ი მიღებული DHCP request შეტყობინებით ასკვნის, რომ DHCP client -მა მიიღო მის მიერ გამოყოფილი კონფიგურაციის პარამეტრები, წყებიდან იღებს IPv6 მისამართს, იწყებს პარამეტრების გაცემის (lease) დროის ათვლას და DHCP reply შეტყობინებას უგზავნის DHCP client -ს.

ნახ. 6. DHCP მეთოდით IPv6 მისამართის მიღების პროცესი

- **SLAAC** [1] (Stateless Address Autoconfiguration), რომელიც არის დინამიური მეთოდი. ის შემოღებულია IPv6 პროტოკოლის დამპროექტებლების მიერ იმ მიზნით, რომ DHCP (Dynamic Host Configuration Protocol) სერვერის გამოყენების გარეშე შესაძლებელი ყოფილიყო მოწყობილობისათვის IPv6 მისამართის დინამიური გამოყოფა. მისამართის გამოყოფისათვის SLAAC მეთოდის მიერ შეიძლება გამოყენებული იქნას IPv6 მისამართის პირდაპირი გამოყოფის მექანიზმი ან EUI-64 მეთოდი. ეს მეთოდი იძლევა მხოლოდ ქსელს შიგნით კომუნიკაციის შესაძლებლობას, ხოლო მის გარეთ კომუნიკაციისათვის მაინც არსებობს DHCP სერვერის გამოყენების აუცილებლობა. ამ მეთოდის გამოყენებით IPv6 მისამართის მიღება ხდება შემდეგნაირად (ნახ. 7): ქსელში ჩართული მოწყობილობა ქსელში აგზავნის RS (router solicit) შეტყობინებას (multicast მისამართზე), რომლითაც ცდილობს აღმოაჩინოს ქსელში გამოყენებული როუტერი. როუტერი შემოსულ შეტყობინებას პასუხობს RA (router advertisement) შეტყობინებით, რომელიც ასევე იგზავნება multicast მისამართზე. მიღებული RA შეტყობინებიდან მოწყობილობა არკვევს ქსელის მისამართს (Network Prefix) და მისამართის პირდაპირი გამოყოფის ან EUI-64 მეთოდის გამოყენებით აგენერირებს IPv6 მისამართს და საკუთარი თავისათვის.



ნახ. 7. SLAAC მეთოდის გამოყენებით IPv6 მისამართის მიღების პროცესი

[1] შეიძლება ითქვას, რომ ამ მეთოდის ანალოგი IPv4 ქსელში არსებობდა APIPA მეთოდის სახით, მაგრამ ეს მთლად ასეც არაა. APIPA -სგან განსხვავებით SLAAC მეთოდი იძლევა ფუნქციონირებად ქსელს

2. მარშრუტიზაციის პროტოკოლები

ქსელური კომუნიკაციისათვის ერთერთ მნიშვნელოვან მოწყობილობას წარმოადგენს როუტერი (Router). როუტერი ერთმანეთთან აკავშირებს სხვადასხვა ქსელებს და მართავს დანიშნულების ქსელის მიმართულებით მონაცემების გადაცემის პროცესს. მონაცემების (ტრაფიკის) დანიშნულების მიმართულებით გადასაცემად როუტერები იყენებენ ე.წ. მარშრუტიზაციის ცხრილს (Routing Table), რომელშიც ინახება როუტერისთვის ცნობილ ყველა ქსელამდე გზებზე ინფორმაცია. მარშრუტიზაციის განხორციელებისთვის როუტერს უწევს შემდეგი ეტაპების გავლა:

1. როუტერზე ამუშავდება სპეციალური პროგრამა, რომელსაც ეწოდება მარშრუტიზაციის პროტოკოლი (*routing protocols*). ასეთი პროგრამები გამოიყენება ქსელში მეზობელ (ფიზიკურად კაბელური ან ლოგიკურად დაკავშირებული) როუტერებთან მარშრუტიზაციის მონაცემების გასაცვლელად. მარშრუტიზაციის მონაცემების გასაცვლელად როუტერებზე საჭიროა ამუშავებული იქნას ერთიდაიგივე მარშრუტიზაციის პროტოკოლი;
2. მარშრუტიზაციის მიღებული მონაცემებით როუტერები ავსებენ საკუთარ მარშრუტიზაციის ცხრილს;
3. როუტერები ახდენენ საკუთარი მარშრუტიზაციის ცხრილის სკანირებას და იქ არსებული ჩანაწერებიდან დანიშნულების ქსელისკენ მიმავალი გზებიდან ირჩევენ ერთ ან რამდენიმე საუკეთესო შეფასების მქონე გზას;
4. მონაცემების გადაცემისას როუტერი ურთიერთქმედებს იმ მეზობელ როუტერთან, რომელიც განთავსებულია დანიშნულების ქსელის მიმართულების გზაზე.
5. როუტერი საკუთარი მარშრუტიზაციის ცხრილიდან ახდენს იმ ადაპტერის იდენტიფიცირებას, რომელზეც უნდა მოხდეს დანიშნულების მიმართულებით მონაცემების გადაცემა.
6. მონაცემების მიღების შემთხვევაში როუტერი იხედება შესაბამის პაკეტში და იქიდან გებულობს დანიშნულების ქსელის მისამართს. მიღებულ მისამართს ადარებს საკუთარ მარშრუტიზაციის ცხრილში არსებულ ჩანაწერებს და ამის მიხედვით განსაზღვრავს შემდეგ მოქმედებებს. თუ ჩანაწერი მოიძებნა პაკეტი აგრძელებს გზას დანიშნულების ქსელისკენ. წინააღმდეგ შემთხვევაში პაკეტი წყვეტს მოგზაურობას.
7. გარდა ზემოთ ჩამოთვლილი ფუნქციებისა და როუტერი ახდენს დამატებითი ფუნქციების შემოწმებას, როგორციაა პაკეტის სიცოცხლის ხანგრძლივობა (TTL) და მომსახურების ტიპი (TOS). შემოწმების გავლის შემდეგ პაკეტი აგრძელებს მოგზაურობას დანიშნულების ქსელის მიმართულებით.
8. ზემოთ აღწერილი ყოველი მოქმედება მეორდება დანიშნულების ქსელისკენ მიმავალ გზაზე განთავსებულ ყველა როუტერზე

3. მარშრუტიზაციის პროტოკოლები

როგორც უკვე აღვნიშნეთ, როუტერები მონაცემების დანიშნულების მიართულებით გადასაცემად მიმართავენ საკუთარ მარშრუტიზაციის ცხრილს. მარშრუტიზაციის ცხრილი შეიცავს იმ მოშორებულ ქსელებზე ინფორმაციას, რომლებზეც მიმდინარე როუტერს გააჩნია ინფორმაცია. მარშრუტიზაციის ცხრილში ინფორმაცია ამა თუ იმ ქსელზე შეიძლება გამოჩნდეს ორი წესით:

1. **სტატიკური,** როცა ქსელის ადმინისტრატორი გარკვეული ბრძანებათა მიმდევრობით ასწავლის როუტერს ამა თუ იმ ქსელზე ინფორმაციას;
2. **დინამიური,** როდესაც შესაძლებელია როუტერებზე ამუშავებული იქნას რაიმე სპეციფიური პროგრამა, რომელიც ფიზიკურად კაბელური ან ლოგიკურად დაკავშირებულ როუტერებს (ერთიდაიმავე პროგრამის ფარგლებში) აძლევს საშუალებას ერთმანეთთან გაცვალონ მათთვის ნაცნობ ქსელებზე ინფორმაცია.

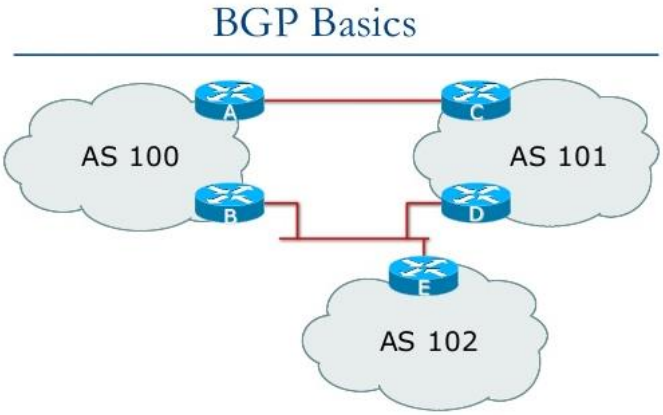
დინამიური მარშრუტიზაციის პროტოკოლები იყოფიან ორ ნაწილად: IGP (Interior Gateway Protocol) და EGP (Exterior Gateway Protocol) პროტოკოლებად.

IGP პროტოკოლები გამოიყენებიან ორგანიზაციის ქსელს შიგნით საქმიანობისთვის. ასეთ მარშრუტიზაციის პროტოკოლებს წარმოადგენენ: RIP, EIGRP, IS-IS და OSPF.

EGP პროტოკოლები შემუშავებული იქნა მარშრუტიზაციის გაზრდილი ცხრილების სამართავად და ასევე, მარშრუტიზაციის დომენების სხვადასხვა ადმინისტრაციულ ერთეულებად დაყოფის გზით Internet ქსელის სტრუქტურირების ამაღლების მიზნით. ასეთ ადმინისტრაციულ ერთეულებს **ავტონომიური სისტემა** (autonomous systems — AS) ეწოდებათ. მიმდინარე დროისათვის Internet ქსელში საერთაშორისო მარშრუტიზაციისათვის გამოყენებულ ერთადერთ პროტოკოლს წარმოადგენს BGP-4.

4. ავტონომიური სისტემა

ავტონომიური სისტემა (autonomous system - AS) ეს არის როუტერების ნაკრები, რომელთაც გააჩნიათ მარშრუტიზაციის ერთიდაიგივე წესი, იმართება ერთიდაიგივე ტექნიკური ჯგუფის მიერ და გამოიყენება ერთერთი ან რამდენიმე IGP პროტოკოლებიდან. სხვა დანარჩენი ქსელის მიერ AS აღიქმება, როგორც ცალკეული ელემენტი და ერთი მთლიანი. უნიკალური AS ნომერი ორგანიზაციას ენიჭება Internet ქსელის სერვისის პროვაიდერის მიერ. სხვადასხვა AS სისტემებს შორის ხორციელდება გარე მარშრუტიზაციის პროტოკოლის მიერ, როგორიცაა BGPv4 (ნახ. 8).



ნახ. 8. BGP პროტოკოლის მეშვეობით ავტონომიური სისტემების დაკავშირება

ბუნებრივად ისმის კითხვა: იქნებ სჯობდა Internet ქსელის დატოვება AS სისტემებად დაყოფის გარეშე. ამ შემთხვევაში, არ იარსებებდა მარშრუტიზაციის პროტოკოლების EGP და IGP პროტოკოლებად დაყოფის აუცილებლობა და შესაბამის ქსელში მარშრუტიზაციისთვის შესაძლებელი იქნეოდა ისეთი პროტოკოლების გამოყენება, როგორიცაა OSPF ან IS-IS?

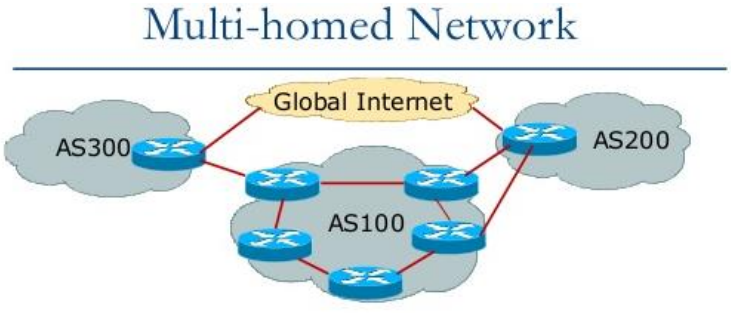
Internet ქსელის დაყოფა შედარებით პატარა ქსელებად, ცალკეულ AS სისტემებად იძლევა იმ უპირატესობას, რომ თითოეულ AS სისტემაში შესაძლებელია რეალიზებული იქნას მარშრუტიზაციის საკუთარი წესების ნაკრები, რომელიც იქნება უნიკალური მახასიათებელი ამავე AS სისტემისთვის და იძლევა სხვა ქსელებისათვის შეთავაზებული მომსახურეობების აღწერის შესაძლებლობებს. ამ შემთხვევაში ყველა AS სისტემას შეუძლია აამუშაოს საკუთარი ნაკრები IGP პროტოკოლებისა მიუხედავად იმისა, რომელ IGP პროტოკოლებს იყენებენ სხვა AS სისტემები.

AS სისტემა შეიძლება დაკონფიგურირებული იქნას როგორც:

1. Stub ან single-homed, როსედაც ორგანიზაციიდან გამომავალი მონაცემები ნებისმიერი მიმართულებით გადაცემისთვის საჭიროებს ერთიდაიმავე წერტილის (როუტერის) გავლას;

ნახ. 9. Stub ქსელი

2. Multi-homed non-transit, როდესაც ორგანიზაციიდან გამომავალი მონაცემები შესაძლებელია გადაიცეს სხვადასხვა წერტილიდან (ორგანიზაცის დაკავშირებულია Internet ქსელის რამდენიმე პროვაიდერთან). ამ შემთხვევაში შეზღუდულია დანიშნულების ქსელისკენ მიმავალი მონაცემების გატარება მიმდინარე AS სისტემაში.
3. Multi-homed transit, როდესაც ორგანიზაციიდან გამომავალი მონაცემები შესაძლებელია გადაიცეს სხვადასხვა წერტილიდან (ორგანიზაცის დაკავშირებულია Internet ქსელის რამდენიმე პროვაიდერთან). ამ შემთხვევაში არ იზღუდება დანიშნულების ქსელისკენ მიმავალი მონაცემების გატარება მიმდინარე AS სისტემაში.



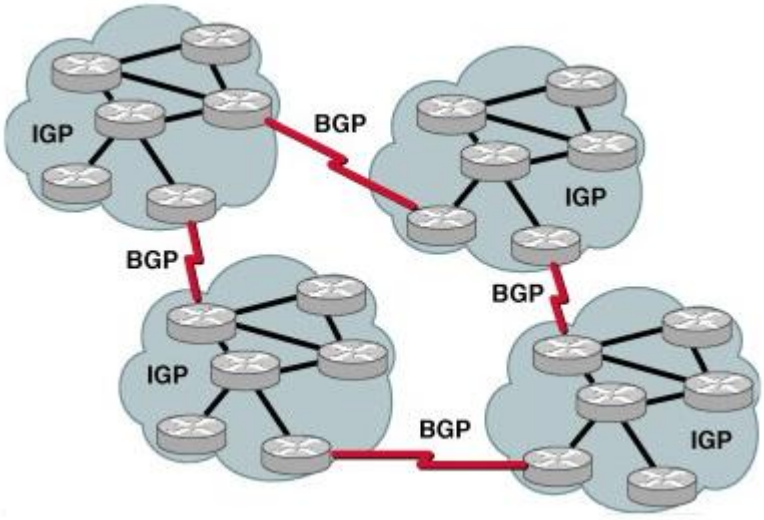
ნახ. 10. Multi-homed ქსელი

5. BGP პროტოკოლი

როგორც უკვე არაერთხელ აღვნიშნეთ BGP (Border Gateway Protocol) პროტოკოლი გამოიყენება სხადასხვა AS სისტემებს შორის მონაცემების გადაადგილებისთვის. BGP პროტოკოლი (ვერსია 1) შეიქმნს გასული საუკუნის 80-ანი წლების ბოლოს (1989 წ.). მისი შექმნის მომენტიდან მან განიცადა მრავალი ცვლილება. დღეისათვის BGP პროტოკოლის დეფაქტო სტანდარტად აღიარებულია პროტოკოლის მეოთხე ვერსია (BGPv4), რომელსაც გააჩნია ქსელების აგრეგირების (გაერთიანების), CIDR (classless interdomain routing - არა კლასობრივი დომენთაშორისი მარშრუტიზაცია) ტექნოლოგიის და ე.წ. superset-ის კონცეფციის მხარდაჭერა.

BGP პროტოკოლი არ უყენებს რაიმე სახის მოთხოვნებს AS სისტემებს მათ შიგნით გამოყენებულ ქსელურ ტოპოლოგიასთან მიმართებაში. მისი მუშაობის პრინციპი გულისხმობს, რომ AS სისტემის შიგნით გამოყენებულია IGP პროტოკოლები.

BGP პროტოკოლი სხვადასხვა AS სისტემის როუტერებისგან მიღებული მარშრუტიზაციის ინფორმაციის საფუძველზე ადგენს შესაბამის გრაფს და AS სისტემებს შორის კავშირებს. ასეთ გრაფს ხანდახან უწოდებენ მარშრუტიზაციის ხეს. თუ BGP პროტოკოლის მხრიდან განვიხილავთ Internet ქსელს (ნახ. 11), ეს იქნება გრაფი, რომელიც შედგება ავტონომიური სისტემებისგან, სადაც ყოველ AS-ს შეესაბამება უნიკალური ნომერი. ორ AS სისტემას შორის გადებული მონაკვეთი (წითელი ხაზი ნახაზზე) წარმოადგენს გზას ამ სისტემებს შორის, ხოლო ერთი AS სისტემიდან მეორემდე გადასვლების ერთობლიობაზე ინფორმაცია ქმნის სრულ გზას ამ AS სისტემებს შორის. BGP პროტოკოლი აქტიურად იყენებს ამ ინფორმაციას დანიშნულების მიმართულებით მონაცემთა გადაცემის საჭიროებისას.



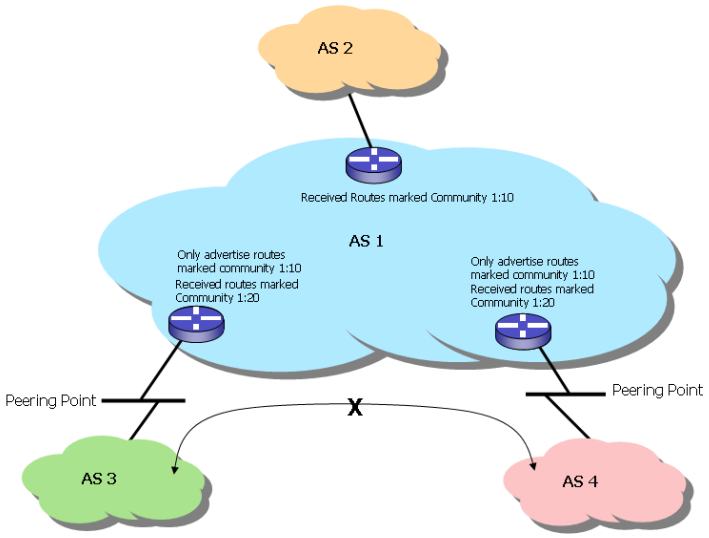
ნახ. 11. BGP ქსელის მაგალითი

BGP პროტოკოლი შეიძლება დაიყოს როგორც EBGP (External BGP), რომელიც გამოიყენება ავტონომიურ სისტემებს შორის, და IBGP (Internal BGP), რომელიც გამოიყენება ავტონომიური სისტემის შიგნით. ავტონომიური სისტემის შიგნით IBGP პროტოკოლის გამოყენება საჭიროა კომპლექსური ქსელის არსებობის შემთხვევაში, ვინაიდან ის იძლევა უკეთესი მასშტაბირებადობის შესაძლებლობას. ტექნოლოგიური განვითარების პარალელურად განვითარდა BGP პროტოკოლი და მან შეიძინა მულტი-პროტოკოლის გაფართოება (RFC 4760), რაც ნიშნავს, რომ მას შეუძლია დაკონფიგურირდეს როგორც IPv4 ისე IPv6 პროტოკოლის შემთხვევაში და გადასცეს ნებისმიერი სახის მარშრუტირებადი ინფორმაცია.

BGP წარმოადგენს ე.წ. path vector-ს (გზის ვექტორი) და გამოიყენება AS სისტემებს შორის გზებზე ინფორმაციის გაცვლისთვის. ტერმინი path vector-ი გამომდინარეობს BGP პროტოკოლის მოქმედებიდან: გზაზე ინფორმაცია შეიცავს იმ AS სისტემების ნომრების მიმდევრობას, რომელთა გავლაც დასჭირდა პაკეტს ქსელის მითითებული პრეფიქსით.

BGP პროტოკოლი მონაცემთა ტრანსპორტირებისთვის იყენებს TCP (პორტის ნომრით 179) პროტოკოლს. შესაბამისად, ამ შემთხვევაში, მთელი პასუხისმგებლობა მონაცემების გარანტირებულ გადაცემაზე ეკისრება TCP პროტოკოლს და არ არსებობს გადაცემის გარანტირებულობის მიზნით BGP პროტოკოლისთვის რაიმე მექანიზმების ამუშავებისა.

როუტრებს, რომლებზეც ამუშავებულია BGP პროტოკოლი ხშირად უწოდებენ BGP speaker-ს. ორ BGP speaker-ს, რომლებიც მონაცემთა გაცვლის მიზნით ერთმანეთს უკავშირდება TCP პროტოკოლის მეშვეობით, უწოდებენ მეზობლებს (neighbor) ან peer-ს (ნახ. 12). მეზობელი როუტერები კომუნიკაციის დაწყებამდე ერთმანეთთან ცვლიან შეტყობინებებს დაკავშირების პარამეტრების განსაზღვრის მიზნით. ასეთი შეტყობინება ემსახურება ისეთ პარამეტრებზე შეთანხმებას, როგორიცაა მაგალითად, BGP პროტოკოლის ვერსიის ნომერი და სხვა.



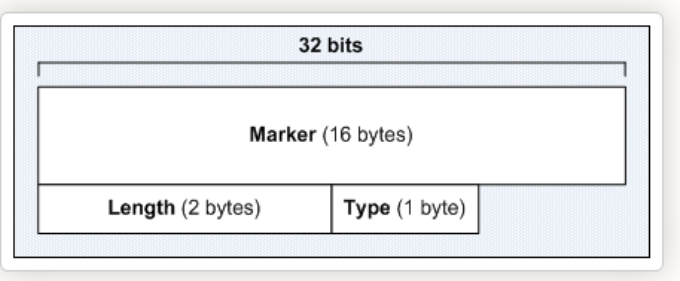
ნახ. 12. ავტონომიური სისტემების დაკავშირება

5.1. BGP შეტყობინების ფორმატი

BGP შეტყობინების თავსართი შედგება სამი ველისაგან (ნახ. 13). ესენია:

1. Marker-ი (16 ბაიტი), რომელიც გამოიყენება შემომავალი BGP შეტყობინების აუთენთიკაციის მიზნით ან ორ მეზობელს შორის სინქრონიზაციის დეტექტირებისთვის. ეს ველი შეიძლება იყოს 2 ფორმატის:
   - თუ გაგზავნილია OPEN ტიპის შეტყობინება ან მასში არაა აუთენთიკაციაზე ინფორმაცია, მაშინ მარკერის ველი ყველა პოზიციაზე დაყენებულია მნიშვნელობაზე 1-ი;
   - სხვა შემთხვევაში მარკერის ველის მნიშვნელობა გამოითვლება აუთენთიკაციის გამოყენებული მექანიზმის შესაბამისად.
2. თავსართის სიგრძე (Length, 2 ბაიტი), რომელიც გამოიყენება BGP შეტყობინების მთლიანი მოცულობის მისათითებლად. მისი მინიმალური მნიშვნელობა შეიძლება იყოს 19 (16+2+1) ბაიტი, ან 4096 ბაიტი;

3. ტიპი (type, 1 ბაიტი), რომელიც განსაზღვრავს BGP შეტყობინების ტიპს. BGP შეტყობინება შეიძლება იყოს შემდეგი ტიპის:
   - OPEN (კავშირის გახსნის)
   - UPDATE (მარშრუტიზაციის ინფორმაციის განახლების)
   - NOTIFICATION (შეცდომაზე ინფორმირების)
   - KEEPALIVE (კავშირის მდგომარეობის შემოწმების)



ნახ. 13. BGP შეტყობინების ფორმატი

6. საფრთხეები BGP სესიისათვის

მრავალი სხვა პროტოკოლის მსგავსად BGP პროტოკოლი შეიქმნა დიდი ხნით ადრე სანამ უსაფრთხოების საკითხი გახდებოდა აქტუალური ქსელური კომუნიკაციისათვის, სახელდობრ, Internet ქსელისთვის. შესაბამისად, მას არ გააჩნია უსაფრთხოების ჩაშენებული მექანიზმი. BGP პროტოკოლს უსაფრთხოების გაზრდის მიზნით შემუშავებული იქნა მრავალი ტექნოლოგია, რომლებიც წარმოადგენენ პროტოკოლის შესაძლებლობების გაფართოებას. მიუხედავად ამისა, BGP პროტოკოლს შეიძლება გააჩნდეს სუსტი წერტილები და საჭიროა ასეთი სუსტი წერტილების დროულად აღმოჩენა და აღმოფხვრა რათა არაკეთილმოსურნე მხარემ არ გამოიყენოს ეს სუსტი წერტილები ცუდი განზრახვისთვის.

BGP პროტოკოლისათვის საფრთხის შემცველი საქმიანობა შესაძლებელია განხორციელებული იქნას, როგორც ორგანიზაციის ქსელში ისე მის გარეთ. თითოეული მათგანი საჭიროებს პრობლემის იდენტიფიცირებისა და მისი აღმოფხვრის განსხვავებულ მიდგომასა და მეთოდების გამოყენებას.

BGP პროტოკოლზე შეტევის განხორციელებისას ერთერთ მნიშვნელოვან პრობლემას წარმოადგენს Internet-ის კრიტიკულ ნაწილებს შორის კავშირის დაკარგვა. პრობლემას ამ შემთხვევაში წარმოადგენს ის, რომ შეუძლებელი Web-ზე წვდომა და ვერ იფუნქციონირებს ვერცერთი Web-სერვისი (როგორიცაა, email-ი, e-commerce-ი და სხვა). ვინაიდან ბიზნესი საქმიანობის განმახორციელებელი ორგანიზაციები აქტიურად იყენებენ Internet ქსელს ფულადი ტრანზაქციებისათვის, ამიტომ შესაბამისი სერვისის გათიშვამ შეიძლება გამოიწვიოს ეკონომიკური კრიზისი.

მეორე მნიშვნელოვან პრობლემას წარმოადგენს მონაცემების კონფიდენციალურობა. კონფიდენციალურობის პრობლემა შეიძლება გამოწვეული იყოს შერეული მარშრუტიზაციის პაკეტებით. რაც ნიშნავს, კონფიდნციალურობის დარღვევის მიზნით არაკეთილმოსურნე მხარე (ე.წ. eavesdropper-ი) ცდილობს მოახდინოს პაკატების გადაცემა დანიშნულების

მიმართულებით საკუთარი მოწყობილობის გავლით. ამ მიზნით ის შესაბამის BGP როუტერს უგზავნის „ცრუ“ ინფორმაცია იმის თაობაზე, რომ დანიშნულების ქსელი მიღწევადია მისი მოწყობილობის გავლით. თუ eavesdropper-მა მიაღწია საკუთარ მიზანს, მაშინ მას შეუძლია განახორციელოს გადაცემული პაკეტების მონიტორინგი, საიდანაც ნებისმიერი ინფორმაციის მიღება არის შესაძლებელი.

BGP პროტოკოლზე შეტევები შეიძლება დაიყოს ორ ტიპად:

- სტანდარტული მეთოდები, რომლებიც ცნობილია სამომხმარებლო მოწყობილობებთან მიმართებაში.
- არასტანდარტული მეთოდები, რომლებიც გამოიყენებიან უშუალოდ პროტოკოლზე შეტევის მიზნით.

ცალცალკე განვიხილოთ ორივე მათგანი.

6.1. სტანდარტული შეტევები BGP პროტოკოლზე

BGP პროტოკოლზე სტანდარტული წარმოადგენს ისეთივე მეთოდებს რაც სამომხმარებლო სისტემებისთვის ცნობილი მეთოდებია. ასეთი შეტევებს წარმოადგენენ:

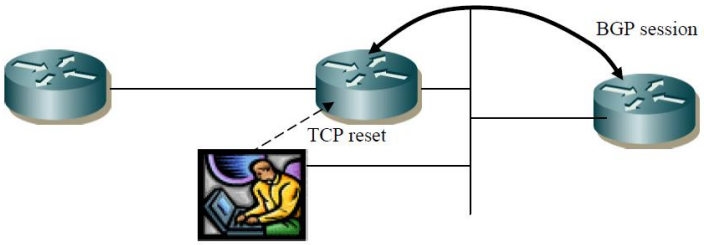
- Denial of service - ამ შემთხვევაში როუტერზე შემოდის დიდი რაოდენობით პაკეტი. პაკეტების დიდი რაოდენობით გაგზავნა მიამართულია როუტერი გახადონ ქმედუუნარო.
- არაავტორიზირებული წვდომა (Unauthorized access), შეიძლება დაფიქსირდეს როცა როუტერზე გამოიყენება ე.წ. default პაროლი.
- Eavesdropping -ი შეიძლება განხორციელებული იქნას პაკეტის მიერ გასვლელ გზაზე ნებისმიერ როუტერზე.
- პაკეტის მანიპულაციის მეთოდი, რომელიც შეიძლება მოიცავდეს წვდომის მიღების მიზნით ცრუ IP მისამართის გამოყენება ან მარშრუტიზაციის ცხრილში ცრუ გზის ჩაწერის მინზით.

6.2. არასტანდარტული შეტევები BGP პროტოკოლზე

ქვემოთ ჩამოთვლილი შეტევები, რომლებიც გულისხმობს მოტყუებას და სესიის მოპარვას, წარმოადგენენ TCP/IP პროტოკოლისათვის დამახასიათებელ შეტევებს, მაშინ როცა გზის მანიპულირების შეტევები დამახასიათებელია BGP ან როუტინგ პროტოკოლისთვის. რადგანაც BGP პროტოკოლი იყენებს TCP/IP სტეკს, ამიტომ TCP/IP -სთვის ცნობილი შეტევები შეიძლება გამოჩნდეს BGP პროტოკოლის შემთხვევაშიც.

არასტანდარტული შეტევების ჩამონათვალს შეიძლება მივაკუთვნთ:

- **Peer Spoofing და TCP Resets** - რომელიც დამახასიათებელია ყველა ქსელური პროტოკოლისათვის. Spoofing (მოტყუება) გულისხმობს მოდიფიცირებული პაკეტის გატარებას, რომელიც გამოიყენება გარკვეული მიზნის მისაღწევად. Peer Spoofing -ის სპეციალურ შემთხვევას წარმოადგენს TCP Resets სახელით ცნობილი შეტევა, რომელიც გულისხმობს ორ BGP პაკეტს შორის TCP RESET შეტყობინების ჩართვას (ნახ. 14). BGP შეტყობინება გადამისამართებული იქნება მესამე მხარესთან, რომელსაც ქსელის მონიტორინგის შედეგად შეეძლება გაიგოს მრავალი კონფიდენციალური ინფორმაცია.



ნახ. 14. TCP Resets-ის მაგალითი

- **TCP Resets ICMP პროტოკოლის გამოყენებით.** ICMP (Internet Control Message Protocol) პროტოკოლი შეიძლება გამოყენებული იქნას კავშირის გადამისამართებისთვის. ასეთი შეტევის რეალიზება შეუძლება იყოს უფრო ადვილი ვიდრე წინ დასახელებული მეთოდისა.
- **სესიის მოპარვა (Session Hijacking).** შეტევის ეს სახეც წააგავს წინ განხილულ ორ მეთოდს. ამ შემთხვევაში არაკეთილმოსურნე მხარე გარკვეული სახით შეიძლება იყოს „მასკირებული“ როგორც BGP სესიის თანამონაწილე.
- **გზისს ცვლილება.** შეტევის ეს მეთოდი მიმართულია შეცვალოს განმეორებადი გზები მარშრუტიზაციის ცხრილში. გზების ასეთი ცვლილებები ქმნის დამატებით პრობლემებს იქიდან გამომდინარე, რომ ყოველი ცვლილება აუცილებლად უნდა იქნას ასახული სხვა როუტერებზეც, რაც იწვევს ქსელის გარკვეული დროით დაყოვნებას.

7. BGP სესიების უსაფრთხოება

BGP პროტოკოლის უსაფრთხოების მიზნით შემუშავებულმა მრავალმა მეთოდმა, რომლებიც წარმოადგენენ პროტოკოლისთვის დანამატს, საკმარისად გაზარდეს პროტოკოლის უსაფრთხოების საკითხი. მაგალითად, მარშრუტიზაციის ცხრილში ჩანაწერის ცვალებადობის შემოწმების და შემავალი/გამავალი ტრაფიკის გაფილტვრის პოლიტიკამ BGP პროტოკოლი გახადა უფრო სტაბილური და უსაფრთხო. გარდა ამისა, CIDR (classless interdomain routing) ტექნოლოგიის გამოყენება იძლევა BGP პრეფიქსების დამუშავების პროცესის გაუმჯობესების შესაძლებლობას, რაც უზრუნველყოფს დაცვის შემდეგ ეტაპს მარშრუტიზაციის ცხრილში შემთხვევითი ან ზიანის მატარებელი ინფორმაციის გაჩენას.

რადგანაც BGP პროტოკოლი წარმოადგენს ცენტრალური მნიშვნელობის პროტოკოლს მთლიანი Internet ქსელისათვის, ამიტომ ის წარმოადგენს სამიზნეს არაკეთილმოსურნე მხარისათვის. BGP პროტოკოლის უსაფრთხოების დარღვევა ნიშნავს Internet ქსელის ფუნქციონირების დარღვევას და შესაბამისად სერვისები, რომელთა გავრცელებაც ხდება Internet ქსელის მეშვეობით მიუწვდომელი იქნება ნებისმიერი ადამიანისათვის. ამიტომ მნიშვნელოვანია BGP პროტოკოლის უსაფრთხოების დაცვა. RFC 4272 დოკუმენტში “BGP Security Vulnerabilities Analysis” მოყვანილია BGP პროტოკოლის სუსტი მხარეები, რომელთა გათვალისწინებაც სჭირდებათ სერვისის პროვაიდერებს. შესაბამისად მნიშვნელოვანია BGP პროტოკოლის უსაფრთხოების დაცვისათვის ყურადღება გამახვილებული იყოს შემდეგ საკითხებზე:

- Authentication (აუთენთიკაცია);
- Confidentiality (კონფიდენციალურობა);
- Integrity (მთლიანობა);

- Availability (ხელმისაწვდომობა).

სტანდარტულად არსებობს რამდენიმე მეთოდი BGP სესიის უსაფრთხოების უზრუნველსაყოფად. ესენია:

- პირდაპირ დაკონფიგურებული BGP-ის კვანძები;
- BGP სესიის საერთო გასაღების გამოყენება;
- IPsec ტუნელის გამოყენება;
- Loopback მისამართების გამოყენება BGP peer-ებზე;
- TTL-ის(Time To Live) კონტროლი BGP-ის პაკეტებზე;
- კვანძთან დაკავშირებული ინტერფეისის გაფილტვრა;
- Link-local-ის გამოყენება კვანძების შეერთებაში;
- გრძელი AS გზის არიდება;
- მიღებული პრეფიქსების რაოდენობის ლიმიტერება;
- კერძო ავტონომიური სისტემების განახლების აკრძალვა;
- IGP-ის უსაფრთხოების უზრუნველყოფა;
- BGPის კვანძებს შორის უსაფრთხო კომუნიკაციის უზრუნველყოფა.

7.1. პირდაპირ დაკონფიგურირებული BGP-ის კვანძები

ერთ-ერთი ტექნიკა, რომელიც გამოიყენება BGP სესიების უსაფრთხოებისთვის წარმოადგენს კონცეპციას, სადაც BGP სესიის კონფიგურაცია უნდა მოხდეს როუტერის თითოეულ შემაერთებელ კვანძზე. ამრიგად, როუტერის მიერ აღარ მოხდება კვანძების შეერთება და ახალი სესიის დაწყება, რადგან სხვა როუტერს არ ექნება შესაბამისი კონფიგურაცია გაწერილი. იმისთვის, რომ დაიწყოს სესია მეორე როუტერთან საჭიროა თანხმობა ორივე კვანძის შეერთების დროს და შესაბამისი BGP-ის პარამეტრების გაწერა. BGP-ის სესია არ დამყარდება, თუ მხოლოდ ერთ როუტერზეა გაწერილი კონფიგურაცია, რადგან საჭიროა მთელი რიგი კონფიგურაციების გაწერა ორივე მხარეს კომუნიკაცის განსახორციელებლად. BGP-ის კომუნიკაცია ხორციელდება TCP პროტოკოლის მეშვეობით, რომელიც იყენებს 179 პორტს, ამრიგად მას გააჩნია რაღაც თანდართული უსაფრთხოების მექანიზმები, რადგან TCP არის შეერთებაზე ორიენტირებული პროტოკოლი.

ის გარემოება, რომ BGP არის stateful transport layer მარშუტიზაციის პროტოკოლი მასში არსებობს უსაფრთხოების რაღაც დონე, მაგრამ ეს წარმოადგენს ასევე მის სისუსტეს. თავდამსხმელებს შეუძლიათ მოიპარონ BGP-ს პაკეტები და გააგზავნონ პირდაპირ BGP-ის როუტერთან, ან შეუძლიათ შეტევის განხორციელება პირდაპირ TCP-ის სესიაზე ორი როუტერის დამაკვშირებელ კვანძებზე.

ამ პრობლემის გადაწყვეტა შესაძლებელია BGP-ის იმპლემენტაციის დროს გამოვიყენოთ მძლავრი მიმდევრობის რიცხვის რანდომიზაცია. ამრიგად, მიდევრობის შემდგომი რიცხვის გაგება წარმოუდგენელი იქნება.

7.2. BGP სესიის საერთო გასაღების გამოყენება

ყვლაზე ფართოდ გავრცელებული მეთოდი BGP-ის კომუნიკაციის უსაფრთხოებისათვის წარმოადგენს საერთო გასაღების გამოყენება. ეს მეთოდი იყენებს შეტყობინების კლასიფიცირების MD5 ალგორითმს, რომელიც ჩართულია BGP პაკეტში. ეს კრებული ამატებს იდენტიფიცირებას BGP-ში და გამოიყენება თავდამსხმელებისაგან დასაცავად, რომ არ მოხდეს BGP-ის კვანძების გატეხვა და პაკეტების მოპარვა.

მიუხედავად იმისა, რომ ეს წარმოადგენს საუკეთესო მეთოდს თავდაცვისათვის, თითოეული კვანძების სესიაზე საჭიროა სხვადასხვა გასაღების გამოყენება, რაც დაკავშირებულია შენახვის სირთულესთან. არაგონივრული იქნება ერთი და იმავე გასაღების გამოყენება სხვადასხვა კვანძის შეერთებაზე, რადგან ამ შემთხვევაში თავდამსხმელის მიერ გასაღების გაგება საფრთხის ქვეშ აყენებს მთლიან სისტემას. პრობლემას წარმოადგენს დიდი რაოდენობის გასაღებების შენახვა და ამისთვის უნდა გამოვიყენოთ ცენტრალიზებული სისტემა, სადაც შესაძლებელი იქნება ყველა ორგანიზაციის გასაღებების შენახვა. Cisco-ს როუტერზე, პაროლის კონფიგურირება ხდება მეზობელი როუტერის კონფიგურაციის გაწერის პროცესში. BGP-ის კვანძზე md5 იდენტიფიკაციის ჩართვა შესაძლებელია შემდეგი ბრძანების გამოყენებით:

Neighbor neighbor-ipv6-address password P@ssw0rd

7.3. IPSec ტუნელის გამოყენება

IPSec წარმოადგენს მძლავრ მეთოდს BGP-ის კვანძების უსაფრთხოებისთვის. ის იცავს განახლებების ერთიანობას და ეხმარება DoS (Denial of Service) შეტევების თავიდან არიდებაში, რომელთა სამიზნესაც წარმოადგენენ BGP-ის კვანძები. IPsec კავშირის გამოყენებას შეუძლია დამატებით გადატვირთოს როუტერი და მოითხოვოს უფრო მეტი პროცესორის გამოთვლითი რესურსი. გარდა ამისა, IPSec ტუნელი შესაძლებელია გამოყენებული იქნას როგორც მარშრუტებზე ინფორმაციის გაგზავნისათვის, ასევე კვანძებს შორის სხვა ტრაფიკის გაგზავნისთვის. ეს განაპირობებს პაკეტების მნიშვნელოვნად გაზრდას მოცულობაში და უარყოფითად იმოქმედებს გამტარუნარიანობის მახასიათებლებზე. მიუხედავად იმისა, რომ IPSec უსაფრთხო მეთოდია, მისი გამოყენება ფართოდ არ ხდება.

თავდამსხმელმა თუ გაიგო, რომ მარშუტიზატორი იყენებს იდენტიფიკაციას, მას მარტივად შეუძლია შექმნას ათასობით ყალბი პაკეტი იდენტიფიკაციის არასწორი პარამეტრებით და გაუგზავნოს როუტერს. ეს როუტერში გამოიწვევს იმას, რომ მას მოუხდება ამ ყალბი პაკეტების დამუშავება. მიუხედავად იმისა, რომ ამ პაკეტების უარყოფა სწრაფად მოხდება ეს გამოიწვევს როუტერის რესურსების გადატვირთვას, რასაც მოჰყვება ნამდვილი მონაცემების დაყოვნება. შედეგად მივიღებთ არასტაბილურ სისტემას და შესაძლოა მოხდეს როუტერის გათიშვა. ამრიგად, თავდამსხმელი მიაღწევს თავის შედეგს. ამ მაგალითმა ნათლად დაგვანახა, რომ BGP კავშირებში იდენტიფიკაცია შეუძლებელია იყოს ერთადერთი უსაფრთხო მეთოდი.

7.4. Loopback მისამართების გამოყენება BGP-ის კვანძებზე

Loopback მისამართის გამოყენებით თავდამსხმელისთვის რთულია გაიგოს საწყისი მისამართი TCP-ის 179 პორტის კვანძების შეერთებაში, რადგან ვერ მოხერხდება IP მისამართის გაგება traceroute-ის გამოყენებით. ეს გამოწვეულია იმით, რომ Loopback წარმოადგენს ლოგიკურ მისამართს და მისი დაკავშირება BGP-ს კვანძებთან ხდის მას ნაკლებად დამოკიდებულს ფიზიკურ კავშირზე და მოითხოვს IGP-ს (Interior Gateway Protocol). Loopback ინტეფეისების უპირატესობას წარმოადგენს ის, რომ ისინი ყოველთვის ჩართულებია არიან და წარმოადგენენ სტაბილურ ინტერფეისს როუტერისთვის. კვანძების დაკავშირება Loopback-ის მისამართების გამოყენებით ძირითადად ხდება IBGP-ის კვანძებში, ვიდრე EBGP-ში, რადგან ის დამოკიდებული IGP-ზე. EBGP კვანძები ხშირად იყენებენ პირდაპირ დაკავშირებულ IP მისამართებს თითოეულ ბოლოზე ფიზიკური ლინკის, მაგრამ მისი აღმოჩენა ადვილად ხდება თავდამსხმელის მიერ.

7.5. TTL-ის კონტროლი BGP-ის პაკეტებზე

BGP პროტოკოლის უსაფრთხოებისთვის შემდეგი მეთოდი გულისხმობს IP პროტოკოლის თავსართით გადაცემული TTL-ის (Time To Live) მნიშვნელობის კონტროლს. EBGP როუტერები აგზავნიან პაკეტებს TTL-ის მნიშვნელობით 255 და იღებენ პაკეტებს TTL-ის 0-ზე მეტი ან ტოლი მნიშვნელობით. პრობლემას წარმოადგენს EBGP როუტერებს შეუძლიათ მიიღონ მოშორებული ქსელიდან მოსული პაკეტები. თუ როუტერები დაკონფიგურირებული იქნებიან იმ ფორმით, რომ მათ შეძლონ პაკეტების მიღება, მხოლოდ პირდაპირ დაკავშირებული როუტერიდან, მაშინ უსაფრთხოების გარკვეული დონე იქნება მიღწეული. IBGP პროტოკოლისთვის მსგავსი მიდგომის გამოყენების აუცილებლობა არ არსებობს იქიდან გამომდინარე, რომ ამ შემთხვევაში შესაბამისი როუტერთან დაკავშირებულია მრავალი ფიზიკური კვანძი.

EBGP კვანძებზე უსაფრთხოების უზრუნველსაყოფად IETF (Internet Engineering Task Force - ინტერნეტ ინჟინრების სპეციალური ჯგუფი) ჯგუფმა შეიმუშავა BGP TTL Security Hack (BTSH) მექანიზმი, რომელიც ასევე ცნობილია სახელით Generalized TTL-based Security Mechanism (GTSM - განზოგადოებულ TTL-ზე დაფუძნებული უსაფრთხოების მექანიზმი, RFC 3682). ამ მექანიზმის მიხედვით ურთიერთქმედი EBGP როუტერებს TCP 179 პორტზე ეგზავნება პაკეტი TTL -ის მნიშვნელობით 255. პაკეტის მიმღები ყოველი როუტერი 1-ით ამცირებს TTL-ის მნიშვნელობას. შესაბამისად როუტერი იტოვებს პაკეტს შემდგომი დამუშავებისთვის, თუ პაკეტისათვის TTL-ის მნიშვნელობა 254 (შემცირების შედეგად) ან მეტია (შემცირებამდე). ეს შესაძლებელს ხდის EBGP-ს კვანძებმა მიიღონ პაკეტები მხოლოდ მასთან პირდაპირ დაკავშირებული როუტერებისაგან. თუ იქნება გამოყენებული მოშორებული კვანძი (რიომელიც განთავსებულია 2 ან მეტი როუტერის იქით), მაშინ მოხდება ასეთი პაკეტის უარყოფა რადგანაც ამ შემთხვევაში TTL-ის მნიშვნელობა იქნება ნაკლები 254-ზე. შესაბამისი კონფიგურაცია უნდა იყოს გაწერილი ურთიერთქმედ ორივე EBGP როუტერზე. შესაბამისი კონფიგურაციის გაკეთება შესაძლებელია შემდეგი ბრძანებით:

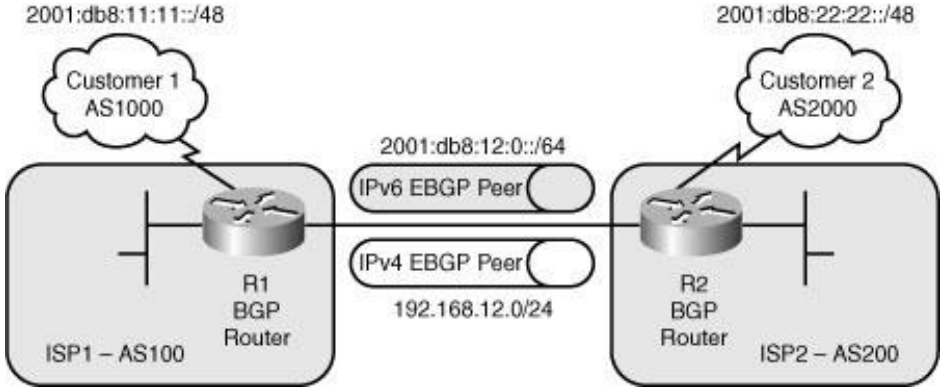
Neighbor neighbor-ipv6-address ttl-security hops 1

BTSH იძლევა BGP პროტოკოლზე თავდასხმების აცილების შესაძლებლობას, მაგრამ ის არ წარმოადგენს სრულყოფილ გადაწყვეტას უსაფრთხოების უზრუნველსაყოფად. მაგალითისათვის, BTSH-ს გამოყენება შეუძლებელია IBGP-ის სესიაზე. უნდა აღინიშნოს,

შემუშავებული იქნა TTL-Hack-ის რამდენიმე ძლიერი სტრატეგია. md5 პაროლები და TTL-ის შემოწმება ტვირთავს როუტერის პროცესორს, რამაც შეიძება მონაცემების გადაცემის დაყოვნება გამოიწვიოს. აღნიშნული მიდგომა შეიძლება იძლეოდეს ძლიერ თავდაცვით მექანიზმს თუკი მისი რეალიზება როუტერზე შესაძლებელი იქნება აპარატურულ დონეზე.

IPv6 EBGP როუტერზე ამ მეთოდებიდან რამდენიმე მეთოდის ერთდროულად დაკონფიგურირების შემთხვევაში როუტერი გახდება შედარებით უსაფრთხო. ქვემოთ მოყვანილია ნახ. 15-ზე ნაჩვენები ISP-ს ორი ურთიერთდაკავშირებული IPv6 EBGP როუტერის კონფიგურაცია. ორივე მათგანს გააჩნია თავიანთ მომხმარებლებთან კავშირი და ასევე backbone დაკავშირებები. როუტერების კავშირი მოხდება ორივე პროტოკოლით IPv4 და IPv6.

კონფიგურაციაზე ნაჩვენებია ISP1 პროვაიდერის R1 როუტერის კონფიგურაცია, რომელიც Serial 1/0 ადაპტერით უკავშირდება R2 როუტერს. ორივე დაკავშირებულ კვანძზე TTL-ის მნიშვნელობა IPv6 პროტოკოლის თავსართში დაყენებულია 254 მნიშვნელობაზე. მრავალპროტოკოლური BGP კონფიგურაცია იყენებს TTL-Hack-ს და განსხვავებულ პაროლებს IPv4 და IPv6 პროტოკოლებისათვის. R1 როუტერი მომხმარებელს უკავშირდება Serial 1/1 ადაპტერით. ის ახდენს მონაცემების გაფილტვრას, იმ მიზნით, რომ იცოდეს რა ქსელები ისწავლა მომხმარებლისგან და რა ისწავლა დაკავშირებული ISP2 პროვაიდერისაგან. ის მომხმარებლისგან იღებს IP მისამართიდან /48 პრეფიქსს და კომუნიკაციის საშუალებას აძლევს მხოლოდ შესაბამისი IP მისამართის მქონე მომხმარებლებს. პროვაიდერებს შორის გამოიყენება უფრო სპეციფიური პრეფიქსი ვიდრე მომხმარებლებთან და დაკავშირებას ანხორციელებს Toredo და 6to4 როუტერებს შორის.



ნახ. 15. IPv6 EBGP ურთიერთდაკავშირებული როუტერები

EBGP როუტერის კონფიგურაცია:

```
hostname R1
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 ipv6 address 2001:DB8::1:1:1:1/128
!
interface FastEthernet0/0
 ip address 2.2.2.1 255.255.255.0
 ipv6 address 2001:DB8:100::1/64
!
interface Serial1/0
 description ISP interconnect
```

```
 ip address 192.168.12.1 255.255.255.0
 ip access-group 100 in
 ipv6 address 2001:DB8:12::1/64
 ipv6 traffic-filter ALLOWBGP in
!
interface Serial1/1
 description Customer 1
 ip address 1.1.0.1 255.255.255.0
 ipv6 address 2001:DB8:1:1::1/64
!
router bgp 100
 bgp router-id 1.1.1.1
 no bgp fast-external-fallover
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 bgp maxas-limit 50
 neighbor 1.1.0.11 remote-as 1000
 neighbor 1.1.0.11 ttl-security hops 1
 neighbor 1.1.0.11 password cisco321
 neighbor 2001:DB8:1:1::11 remote-as 1000
 neighbor 2001:DB8:1:1::11 ttl-security hops 1
 neighbor 2001:DB8:1:1::11 password cisco123
 neighbor 2001:DB8:12::2 remote-as 200
 neighbor 2001:DB8:12::2 ttl-security hops 1
 neighbor 2001:DB8:12::2 password cisco123
 neighbor 192.168.12.2 remote-as 200
 neighbor 192.168.12.2 ttl-security hops 1
 neighbor 192.168.12.2 password cisco321
!
 address-family ipv4
 neighbor 1.1.0.11 activate
 neighbor 1.1.0.11 maximum-prefix 250000
 no neighbor 2001:DB8:1:1::11 activate
 no neighbor 2001:DB8:12::2 activate
 neighbor 192.168.12.2 activate
 neighbor 192.168.12.2 maximum-prefix 250000
 no auto-summary
 no synchronization
 network 1.1.0.0 mask 255.255.255.0
 exit-address-family
!
```

```
 address-family ipv6
    neighbor 2001:DB8:1:1::11 activate
    neighbor 2001:DB8:1:1::11 remove-private-as
    neighbor 2001:DB8:1:1::11 prefix-list FILTERV6CUSTIN in
    neighbor 2001:DB8:1:1::11 maximum-prefix 250000
    neighbor 2001:DB8:12::2 activate
    neighbor 2001:DB8:12::2 remove-private-as
    neighbor 2001:DB8:12::2 prefix-list FILTERV6ISPIN in
    neighbor 2001:DB8:12::2 prefix-list FILTERV6ISPOUT out
    neighbor 2001:DB8:12::2 maximum-prefix 250000
    network 2001:DB8:1::/48
    network 2001:DB8:1:1::/64
    no synchronization
    exit-address-family
!
access-list 100 permit tcp host 192.168.12.2 host 192.168.12.1 eq bgp
access-list 100 deny   tcp any any eq bgp
access-list 100 permit ip any any
!
ipv6 route 2001:DB8:1::/48 Null0
!
ipv6 prefix-list FILTERV6CUSTIN seq 10 permit 2001:DB8:11::/48
ipv6 prefix-list FILTERV6CUSTIN seq 20 deny ::/0 le 128
!
ipv6 prefix-list FILTERV6ISPIN seq 10 deny 2001:DB8:1::/48
ipv6 prefix-list FILTERV6ISPIN seq 20 permit 2001:DB8::/32 le 64
ipv6 prefix-list FILTERV6ISPIN seq 30 permit 2002::/16
ipv6 prefix-list FILTERV6ISPIN seq 40 permit 2001::/32
ipv6 prefix-list FILTERV6ISPIN seq 50 deny ::/0 le 128
!
ipv6 prefix-list FILTERV6ISPOUT seq 10 deny 2001:DB8::/32 ge 49
ipv6 prefix-list FILTERV6ISPOUT seq 20 permit ::/0 le 128
!
ipv6 access-list ALLOWBGP
    permit tcp host 2001:DB8:12::2 host 2001:DB8:12::1 eq bgp
    deny tcp any any eq bgp
    permit ipv6 any any
```

7.6. კვანძთან დაკავშირებული ინტერფეისის გაფილტვრა

უსაფრთხოების უზრუნველყოფის საუკეთესო გამოსავალს წარმოადგენს იმ ადაპტერის გაფილტვრა, რომელიც ახდენს BGP პროტოკოლის მეშვეობით დაკავშირებულ კვანძებს შორის კომუნიკაციას. იმისთვის, რომ ნება დართული იყოს IPv6-ის ტრაფიკის გადაცემა, საჭიროა TCP 179 პორტის იყოს გახსნილი დაკავშირებულ როუტერებს შორის BGP-ის პაკეტების გადასაცემად. ასეთი კომუნიკაციისთვის ორივე როუტერს უნდა ქონდეს ACL ჩამონათვალში TCP 179 პორტზე შესაბამისი მონაცემების მიღების საშუალება წინასწარ განსაზღვრული IP მისამართებისთვის. Serial 1/0 ინტერფეისი გააჩნია IPv4-ზე access list, ხოლო IPv6-ზე traffic filter, რომელთა საშუალებითაც მხოლოდ BGP-ის კომუნიკაციაა შესაძლებელი R2-ის კვანძზე.

შევნიშნოთ, რომ ISP-ები მიმართავენ განსხვავებული მეთოდის გამოყენებას, რომელიც ცნობილია ინფრასტრუქტურული ACL-ი (iACL - infrastructure ACL) სახელით. IACL განთავსებულია ადმინისტრაციული დომეინის საზღვარზე და მის ფუნქციაში შედის პრევენცია მოახდინოს გარედან შემოსული პაკეტის, რომლის დანიშნულებასაც წარმოადგენს როუტერის მისამართი (ფიზიკური ან ლოგიკური). ერთადერთი ტრაფიკი რომელიც ნებადართულია ეს არის BGP-ის კვანძებს შორის. ამ Iacl-ის გამოყენება და განთავსება მარტივია.

7.7. Link-local-ის გამოყენება კვანძების შეერთებაში

ჩვენ უკვე განვიხილეთ BGP-ის კვანძების უსაფრთხოება unicast მისამართების გამოყენებით. ეხლა განვიხილოთ უსაფრთხოება link-local მისამართების გამოყენებით, რომელსაც გააჩნია როგორც დადებითი, ასევე უარყოფითი მხარეები. Link-local მისამართების კონცეფცია მდგომარეობს შემდეგში, რომ თავდამსხმელს არ ექნება შესაძლებლობა დაამყაროს სესია როუტერებთან და არ ექნება შესაძლებლობა გაიგოს ipv6-ის მისამართები. როდესაც ვიყენებთ link-local მისამართებს. BGP-ს კვანძებზე ჩვენ აუცილებლად სწორად უნდა დავაკონფიგურიროთ მისამართი მეზობლის როუტერზე, რადგან link-local -ზე არ გამოიყენება DNS და ჩვენ ხელით გვიწევს მისი გაწერა, ამიტომ შეცდომის დაშვების ალბათობა გაზრდილია და შეიძლება დასჭირდეს გარკვეული დრო მის გასწორებას.

ასევე გასათვალისწინებელია, რომ როუტერის link-local მისამართების გაზიარება შეიძლება მოხდეს უამრავ ინტერფეისზე. ამიტომ, საჭიროა როუტერის კონფიგურაცია მეზობლის link-local მისამართზე და შესაბამისი ინტერფეისის განსაზღვრა პირდაპირ დაკავშირებულ კვანძზე. არსებოს ორი გზა ამისთვის. ადრინდელ პროგრამულ ვერსიებში, ჩვენ უნდა განგვესაზღვრა ინტერფეისის იდენტიფიკატორი და შემდგომ გაგვეწერა link-local მისამართი. უფრო ახალი მეთოდი იყენებს update-source მეზობლის პარამეტრს, რომ განსაზღვროს ინტერფეისი. შემდგომი მაგალითი გვიჩვენებს თუ როგორ ხდება მისი კონფიგურაცია.

```
hostname R1
!
```

```
interface Serial1/0
    description ISP interconnect
    ipv6 address 2001:DB8:12::1/64
    ipv6 traffic-filter ALLOWBGP in
!
router bgp 100
    bgp router-id 1.1.1.1
    neighbor FE80::C801:15FF:FE44:0 remote-as 200
    neighbor FE80::C801:15FF:FE44:0 ttl-security hops 1
    neighbor FE80::C801:15FF:FE44:0 password cisco123
    neighbor FE80::C801:15FF:FE44:0 update-source Serial1/0
 !
 address-family ipv4
    no neighbor FE80::C801:15FF:FE44:0 activate
    exit-address-family
 !
 address-family ipv6
    neighbor FE80::C801:15FF:FE44:0 activate
    neighbor FE80::C801:15FF:FE44:0 prefix-list FILTERV6ISPIN in
    neighbor FE80::C801:15FF:FE44:0 prefix-list FILTERV6ISPOUT out
    neighbor FE80::C801:15FF:FE44:0 route-map SETNEXTHOP out
    neighbor FE80::C801:15FF:FE44:0 maximum-prefix 250000
    network 2001:DB8:1::/48
    network 2001:DB8:1:1::/64
    no synchronization
    exit-address-family
!
route-map SETNEXTHOP permit 10
     set ipv6 next-hop 2001:DB8:12::1
!
ipv6 access-list ALLOWBGP
    permit tcp host FE80::C801:15FF:FE44:0 host FE80::C800:15FF:FE44:0 eq bgp
    deny tcp any any eq bgp
    permit ipv6 any any
```

ამ მაგალითში EBGP-ის მეზობლის კონფიგურაცია მოხდა link-local მისამართით. ტრაფიკის ფილტრი ALLOWBGP კომუნიკაციის ნებართვას აძლევს კვანძებს. ინტერფეისის სახელი/რიცხვი საჭიროა დაემატოს link-local მეზობლის ბრძანებას, რადგან არ არის აუცილებელი, რომ მისამართები იყოს უნიკალური თითოეული როუტერის ინტერფეისზე. ეს მაგალითი იყენებს update-source მეთოდს ინტერფეისის კონფიგურაციისთვის კვანძების შეერთების სესიაში. ინტერფეისი რომელიც გამოიყენება შეერთებაში არის ფიზიკური სერიალული ინტერფეისი, რომელსაც ორივე როუტერი იყენებს. ამან შეიძლება გამოიწვიოს დაბნეულობა, რადგან ბევრი როუტერის ინტერფეისი იყენებს ერთსა და იმავე link-local მისამართს.

დასკვნა

ზემოთ განხილულ თემაში ჩვენ წარმოვადგინეთ ინტერნეტში არსებული მარშუტიზაციის პროტოკოლების უსაფრთხოებისათვის საჭირო მექანიზმები, კერძოდ განვიხილეთ BGP-ის უსაფრთხოება IPv6-ის ბაზაზე, თუ როგორ იყენებს როუტერი ინტერნეტ კომუნიკაციაში მარშუტიზაციის პროტოკოლებს ე.წ. Routing Table-ს გადასაცემად სხვა როუტერებისათვის, სადაც შენახულია როუტერისთვის ცნობილ ყველა ქსელამდე გზა, ხოლო BGP წარმოადგენს ერთადერთ პროტოკოლს საერთაშორისო მარშუტიზაციისთვის. ნაშრომში განხილულია, როგორც სტანდარტული, ასევე არასტანდარტული შეტევები მარშუტიზაციის პროტოკოლზე. სტანდარტულ შეტევებში გაერთიანებულია: Denial of service (Dos), არაავტორიზებული წვდომა, Eavesdropping და ასევე პაკეტის მანიპულაციის მეთოდი, რომლის დროსაც გამოიყენება ცრუ IP, ხოლო არასტანდარტულ შეტევებში: Peer spoofing და TCP Resets, სესიის მოპარვა(Session Hijacking) და გზების ცვლილება მარშუტიზაციის ცხრილში. ამ ტიპის შეტევების თავიდან ასაცილებლად ყურადღება უნდა გამახვილდეს შემდეგ საკითხებზე: აუთენტიფიკაციაზე, კონფიდენციალურობაზე, მთლიანობაზე და ხელმისაწვდომობაზე. ამისთვის უნდა გამოვიყენოთ რამდენიმე მეთოდი სესიის უსაფრთხოებისთვის. ესენია: BGP-ის კვანძების პირდაპირი კონფიგურაცია, სესიის საერთო გასაღების გამოყენება, IPsec ტუნელის გამოყენება, Loopback მისამართების გამოყენება peer-ებზე, TTL-ის კონტროლი BGP პაკეტებზე, კვანძთან დაკავშირებული ინტერფეისის გაფილტვრა, Link-Local-ის გამოყენება კვანძებზე.

პირველ რიგში უნდა მოხდეს BGP-ის კვანძების პირდაპირ დაკონფიგურირება თითოეულ შემაერთებელ კვანძზე, რადგან როუტერზე აღარ მოხდეს ახალი სესიის დაწყება და სხვა როუტერს დასაკავშირებლად დასჭირდება თანხმობა მეორე კვანძის, რომელიც პირდაპირ არის გაწერილი, ამრიგად როუტერს კავშირის დასამყარებლად მთელი რიგი კონფიგურაციის გაწერა მოუწევს. ასევე საერთო გასაღების გამოყენება სესიის დროს წარმოადგენს ეფექტურ მეთოდს თავდამსხმელებისგან დასაცავად, რომ არ მოხდეს კვანძებში არაავტორიზებული შეღწევა და პაკეტების მოპარვა. Denial of service (Dos) შეტევების დროს BGP-ის კვანძებში საჭიროა IPSec-ის გამოყენება, ამგვარი შეტევების თავიდან აცილებისთვის. IPsec ტუნელი შესაძლებელია გამოყენებული იქნას როგროც მარშუტებზე ინფორმაციის გასაგზავნად, ასევე კვანძებს შორის სხვა ტრაფიკის გადასაცემად. ასევე Loopback მისამართების გამოყენება კვანძებზე დაგვეხმარება მისამართის დამალვაში, რადგან ვერ მოხერხდება თავდამსხმელი მიერ მისი გაგება traceroute-ის გამოყენებით. TTL-ის კონტროლი BGP-ის პაკეტებზე დაგვეხმარება თავიდან ავიცილოთ დაშორებული ქსელებიდან პაკეტების მიღება და შევძლებთ მხოლოდ დაკავშირებული კვანძებიდან პაკეტების მიღებას. კვანძთან დაკავშირებული ინტერფეისის გაფილტვრის დროს უნდა მოხდეს შესაბამისი ACL-ების გაწერა დაკავშირებულ როუტერბზე და ამით მოხდება თავდაცვითი მექანიზმის ამუშავება არაავტორიზებული შეღწევებისგან თავის დასაცავად. Link-local-ის გამოყენება, როგორც loopback-ის მაგალითში შესაძლებელს გახდის როუტერის მისამართის დამალვას თავდამსხმელისგან, მაგრამ მას გააჩნია ასევე უარყოფითი მხარე, რადგან Link-local-ს არ გააჩნია DNS და ჩვენ ხელით გვიწევს მისი გაწერა, რაც შეცდომის დაშვების ალბათობას ზრდის. ამრიგად, BGP-ის მარშუტიზაციის პროტოკოლში არსებული საფრთხეები დაკავშირებულია მის კვანძებს შორის წამოებულ შეტევებში, როგორიცაა DoS შეტევები, სადაც

ხდება ათასობით ყალბი პაკეტის შექმნა და როუტერისთვის გაგზავნა, რათა მოხდეს ამ პაკეტების დამუშავება, რაც გამოიწვევს მის გადატვირთვას და მივიღებთ არასტაბილურ სისტემას, ასევე BGP-ის კვანძებში არაავტორიზებული შეღწევა და პაკეტების მოპარვა, სისტემის მთლიანობის დარღვევა და თავდამსხმელის მიერ როუტერის რესურსებთან დაკავშირება. ამ საფრთხეების პრევენციისთვის საჭიროა ზემოთ განხილული უსაფრთხოების მექანიზმების გამოყენება, რაც დაგვეხმარება მეტად უსაფრთხო გავხადოთ ინტერნეტი მომავალში.

გამოყენებული ლიტერატურა

1. Vyncke E., Hogg Sc., IPv6 Internet Security for Your Network, Cisco press 2009.
2. Rekhter,, Y., Li,, T., and S. Hares,, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, 2006, <http://www.rfc-editor.org/info/rfc4271>.
3. Gill, V., Heasley, J., Meyer, D., Savola,, P., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, 2007, <http://www.rfc-editor.org/info/rfc5082>.
4. Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, 2010, <http://www.rfc-editor.org/info/rfc5925>.
5. Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, 1998, <http://www.rfc-editor.org/info/rfc2385>.
6. Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2827, 2000, <http://www.rfc-editor.org/info/rfc2827>.
7. Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, 2012, <http://www.rfc-editor.org/info/rfc6480>.
8. Hilliard, N. and D. Freedman, "A Discard Prefix for IPv6", RFC 6666, 2012, <http://www.rfc-editor.org/info/rfc6666>.
9. Jethanandani, M., Patel, K., and L. Zheng, "Analysis of BGP, LDP, PCEP, and MSDP Issues According to the Keying and Authentication for Routing Protocols (KARP) Design Guide", RFC 6952, 2013, <http://www.rfc-editor.org/info/rfc6952>.
10. Bush, R., "Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)", RFC 7115, 2014, <http://www.rfc-editor.org/info/rfc7115>.
11. Kent, S. and A. Chi, "Threat Model for BGP Path Security", RFC 7132, 2014, <http://www.rfc-editor.org/info/rfc7132>.
12. Jasinska, E., Hilliard, N., Raszuk, R., and N. Bakker, "Internet Exchange Route Server", Work in Progress, draft-ietf-idr-ix-bgp-route-server-06, 2014.
13. Smith, P. and R. Evans, "RIPE-532 - RIPE Routing Working Group Recommendations on IPv6 Route Aggregation", 2011.
14. Smith, P., Bush, R., Kuhne, M., Pelsser, C., Maennel, O., Patel, K., Mohapatra, P., and R. Evans, "RIPE-580 – RIPE Routing Working Group Recommendations On Route-flap Damping", 2013.
15. IANA, "IANA IPv6 Special-Purpose Address Registry", <http://www.iana.org/assignments/iana-ipv6-special-registry>.
16. IANA, "Internet Protocol Version 6 Address Space", <http://www.iana.org/assignments/ipv6-address-space>.
17. Bellovin, S., Bush, R., and D. Ward, "Security Requirements for BGP Path Validation", RFC 7353, August 2014, <http://www.rfc-editor.org/info/rfc7353>.
18. Durand J., Pepelnjak I. BGP Operations and Security, RFC 7454 https://tools.ietf.org/html/rfc7454 , 2015