ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი

აკაკი ნავდარაშვილი

ინფორმაციული ტექნოლოგიები

ნაშრომი შესრულებულია **საინფორმაციო სისტემების მაგისტრის** აკადემიური ხარისხის

მოსაპოვებლად

ipv6-ის ტუნელინგი ipv4-ის გარემოში

თბილისი 2014

სამაგისტრო ნაშრომის ხელმძღვანელი

ლელა მირცხულავა

დოქტორი, ასოცირებული პროფესორი

ანოტაცია

მოცემული სამაგისტრო ნაშრომის მთავარი მიზანია IPv4-დან IPv6-ზე გადასვლის მექანიზმის ეფექტურობის მახასიათებლების წარმოდგენა. შედარება IPv4 და IPv6 ქსელების ეფექტურობის მახასითებლებისა როგორც Windows გარემოში, ასევე Linux-ის პლატფორმაზე. განხორიელებულია IPv4 -ისა და IPv6 პროტოკოლების ტესტირება Windows პლატფორმაზე. წარმოდგენილია საწყისი IPv4 რომ IPv6 პროტოკოლი სტეკის სხვდასხვა ტიპის კონვერტაცია. კვლევების პროცესში გამოყენებულია ორი სახის ტუნელინგი : Router-to-Router ტუნელინგი, Host-to-Host ტუნელინგი.

Annotation

The main objective of this Master's Thesis presents from the performance characteristics of the IPv4 to IPv6-transition mechanism. Comparison of IPv4 and IPv6 networks performance charaqteristics is discussed in both as a Windows environment, as well as the Linux-platform. IPv4 - IPv6 protocol testing is preformed on the Windows platform. Different types From IPv4 to IPv6 protocol stack conversion are presented. Two types of Tunneling: Router-to-Router Tunneling, Host-to-Host Tunneling are used in process of researching

შინაარსი

შესავალი

IPv6 (Internet protocol Version 6) არის შემდეგი თაობის პროტოკოლი ინტერნეტისთვის, რომელმაც უნდა ჩაანცავლოს IPv4 . IPv6 რომელიც ხასიათდება მთელი რიგი უპირატესობებით ვიდრე მიმდინარე IPv4 (Internet Protocol Version 4). ორივე IPv6 და IPv4 პროტოკოლები განსაზღვრავენ ქსელური დონის პროტოკოლს, ანუ თუ როგორ გადაეცემა მონაცემები ერთი კომპიუტერიდან მეორეში ერთი და იმავე პაკეტურ ქსელში, როგორიცაა ინტერნეტი. ამაჟამად ყველაზე მნიშვნელოვანი ამოცანაა მიგრაციის პროცესი IPv4-სა და IPv6-ს შორის . პირველი ნაბიჯები IPv6-ის შემოტანასთან დაკავშირებით: IPv6-ის ფორუმი დაფუძნდა 1999 წელს ივლისში. მისი საერთო მისიაა ასწავლოს ინტერნეტ მომხმარებლებს IPv6-ის უპირატესობები. ხელი შეუწყოს და განახორციელოს ამ პროტოკოლის მსოფლიოში დანერგვას. მას აქვს წევრების სია, რომელიც მოიცავს მწარმოებლებს, წამყვან ტელეკომის ოპერატორებს. ინტერნეტ პროვაიდერებს, საკონსულტაციო კომპანებს და ა.შ.

თავი 1

IP V6

1.1IP V6 -ის შექმნის ისტორია

1980 წლის ბოლოს თვალნათლივ გამოჩნდა აუცილებლობა შექმნილიყო ინტერნეტის სამისამართო სივრცის შენახვის საშუალებები. 1990 წლების დასაწყისში მიუხედავად იმისა რომ დაინერგა უკლასო დამისამართება, ნათელი გახდა რომ ეს საკმარისი არ იყო მისამართების შემცირების აღმოსაფხვრელად და საჭიროა ინტერნეტის ინფრასტრუქტურის შემდგომი ცვალებადობა. 1992 წლების დასაწყისისთვის გაჩნდა რამდენიმე წინადადება და 1992 წლის ბოლოსთვის IETF-მ გამოცახადა კონკურსი. რომ მუსა ჯგუფებისთვის შექმნილიყო შემდეგი თაობის ინტერნეტ პროტოკოლი. 1994 წლის 24 ივლისს IETF-მ დაამტკიცა მედალი pnp, რადგან შეიქმნა pnp-ის რამდენიმე სამუშაო ჯგუფი. 1996 წლისთვის გამოშვებული იყო RFC სერია, რომლებიც განსაზღვრავდნენ ინტერნეტ პროტოკოლს ვერსიას 6.

IETF-მ დაუნიშნა ახალ პროტოკოლს ვერსია 6, რადგან ვერსია 5 დაენიშნა ექსპერიმენტალურ პროტოკოლს, რომელიც გათვალისწინებული იყო აუდიო და ვიდეო გადაცემისთვის.

დღესდღობით IP V6 გამოიყენება მსოფლიოს რამდენიმეათასიან ქსელებში (9000 ქსელში 2012 წლის მაისის მონაცემებით). ამის მიუხედავად ჯერ კიდევ არ გამოიყენება ფართოდ ინტერნეტში, როგორც IP V4. რუსეთში გამოიყენება მხოლოდ ტესტურ რეჟიმში კავშირის რამდენიმე ოპერატორების მიერ და ასევე დომენების რეგისტრატორების მიერ DNS სერვერების მუშაობაში. პროტოკოლი შემუშავებულია IETF-ის მიერ.

მას შემდეგ, რაც შეივსება IP V4-ის საინფორმაციო სივრცე, IP V6 და IP V4 გამოიყენება პარარელურად. მაგრამ თანდათანობით IP V6-ის ტრაფიკის წილი გაიზრდება IP V4-თან შედარებით.

რა არის ipv6?

ipv6 ანუ ინტერნეტ პროტოკოლის მე–6 უახლესი ვერსია, რომელიც მიზნად ისახავს უკვე არსებული მე–4 ვერსიის (ipv4) გაუმჯობესებას. ორივე, ipv6 და ipv4 მუშაობენ ქსელურ დონეზე და რა მონაცემები იგზავნება ერთი კომპიუტერიდან სხვა კომპიუტერზე. ყველა

პაკეტი იგზავნება ქსელით. ipv6 შეიცავს მისამართებს და აკონტროლებს პაკეტებით გადაცემულ ინფორმაციას ახალი თაობის ინტერნეტში.

ipv6 არის დოკუმენტირებული RFCs (მოთხოვნების კომენტარი) დაწყებული RFC 2460. მიუხედავად იმისა რომ ipv6 არის ipv4–ის შენდგომი ვერსია, ორივე პროტოკოლი აგრძელებს მონაცემებზე ორიენტირებას ინტერნეტში..

რატომipv6?

Ipv4–ის მთავარი პრობლემაა ის,რომ მისი მისამართების დაკავშირება კომპიუტერთან ამოწურვადია. Ipv6 აქვს ძალიან დიდი მისამართების სივრცე და შდგება 128 ბიტისგან, ხოლო ipv4 32 ბიტისგან.

Ipv4 უზრუნველყოფს 2^{32} მისამართებს, რომელიც 4 მილიარდია, ხოლო ipv6 2^{128} ეს კი უდრის 340 ტრილიონს. მისამართების სიმრავლე კი აღმოფხვრის NET –ში ქსელურ პრობლემებს(როგორიცაა მრავალჯერადი ჰოსტის უკან IP მისამართების გამოყენება) ახალი თაობის ინტერნეტში.

1.2 QOS.(მომსახურების ხარისხი)

Ipv6 აუმჯობესებს მომსახურების ხარისხს. ეს არის რამდენიმე ახალი განცხადება, როგორიცაა ip ტელეფონის, ვიდეო/აუდიო, ინტელექტუალური თამაშები და ეკომერცია. Ipv6 უზრუნველყოფს Qos, მთელი რიგი მოთხოვნების მიწოდების გარანტიას ქსელში მოძრაობისას მონაცემების, შეტყობინებების ან სიჩქარის დაკარგვას.

მობილური ipv6

ეს ფუნქცია უზრუნველყოფს სატრანსპორტო ფენის მხარდაჭერას და საშუალებას აძლევს კომპიუტერს ან ჰოსტს მიუწვდომელი დარჩეს მიუხედავად მისი მდებარეობისა ipv6 ქსელში. მობილური ipv6–ის დახმარებით მიუხედავად ცვლილებისა ადგილებსა და მისამართებში, იგი ინარჩუნებს კომუნიკაციას კვანძებში. აქედან გამომდინარე კვანძების დაკავშირება კეთდება კონკრეტული მისამართებით, რომელიც მინიჭებული აქვს მობილურ კვანძს და რომლის მეშვეობითაც მობილური კვანძები ყოველთვის მიუწვდომელია. ეს ფუნქცია დოკუმენტირებულია REC 3775.

სხვა მნიშვნელოვანი ფუნქციები ipv6–ში.

stateless Auto-reconfiguration of Hosts (არამდგრადი ჰოსტების ავტო რეკონფიგურაცია)–ეს ფუნქცია საშუალებას იძლევა ipv6–ში ჰოსტი ავტომატურად უკავშირდებოდეს მარშუტს ipv6 ქსელში.

Network(ქსელური დონის უზრუნველყოფა) ipv6 ახორციელებს ქსელური დონის შიფრირებას და ავტორიზაციას Ipsecის საშუალებით. უპირატესობები: 1.გაზრდილი მომსახურების სივრცე, 2.უფრო ეფექტური მარშუტიზაცია, 3.შემცირებული მართვის მოთხოვნა, 3.გაუმჯობესებული მეთოდების შეცვლა ISP, 4.უკეთესი მობილობის მხარდაჭერა, 5.Multi-homing, 6.უსაფრთხოება.

1.3 რა არის მობილური IPv6?

მობილური IPv6 არის IETF სტანდარტი, რომელმაც დაამატა მარშუტიზაციის შესაძლებლობები მობილურ კვანძებს IPv6 ქსელში, RFC 3775 აქვს ეს სტანდარტი აღწერილი დეტალურად. ძირითადი უპირატესობა ამ სტანდარტის არის ის რომ მობილური კვანძები (როგორც RFC 3775 კვანძი) არის შეცვლილი point of attachment დანართი მათი IP მისამართის გარეშე, ეს საშუალებას აძლევს მობილურ მოწყობილობებს გადავიდნენ ერთი ქსელიდან სხვაზე და კვლავ გაიზარდოს არსებული კვანძები. მობილური IPv6 გამოყენება აუცილებელია, იმიტომ რომ მობილური კვან|ძების ფიქსირებული IPv6 ქსელის დაკავშირება შესაძლებელია იმ ადგილზე სადაც მოხდა შეცვლა, ზემოთ თქმულიდან გამომდინარე დაკავშირება IPv6 კვანძებს შორის მზადდება (იუზერების ურთიერთობების გარეშე) კონკრეტული მისამართისთვის რომელიც ყოველთვის არის მინიჭებული მობილური კვანძისთვის და რომლის მეშვეობითაც მობილური კვანძი ყოველთვის ხელმისაწვდომია.

განმარტებები და თვისებები, რომლებიც საჭიროა IPv6–სთვის

რამდენიმე მნიშვნელოვანი ინფორმაცია მობილურ IPv6 შესახე:: უცხო ლინკი განსაზღვრავს ლინკს,, რომელიც არ არის მობილური კვანძის home ლინკი. Care მისამართები ნიშნავს რომ მისამართებისთვის გამოიყენება მობილური კვანძები სანამ ის არის foreign link. როდესაც მობილური კვანძები გადაადგილდება home link–დან foreign link-კენ , ის ყოველთვის იქნება ხელმისაწვდომი home მისამართებისთვის, მიუხედავად მისი ქსელის IPv6 მდებარეობისა.

გაერთიანება home address-ის care-of address-თან ერთად არის მაკავშირებელი. მთავარი აგემტი არის როუტერი, რომელიც მხარს უჭერს მობილური კვანძების რეგისტრაციას რომლებიც არიან შორს მათი მისამართებიდან. A corespondet არის IPv6 კვანძი რომელიც ურთიერთქმედებს communicate მობილურ კვანძთან. მობილურიi IPv6 იყენებს IPv6–ის ორი სახის ავტოკონფიგურაციას არამდგრადი(ქსელის თავსართის პრეფიქსის ID),და stateful ავტოკონფიგურაციას (DHCPv6).

მობილური IPv6 პროცესები

როცა მობილური კვანძები არის შორი home –დან ის უგზავნის ინფორმაციას თავისი მიმდინარე გადაადგილების შესახებ. home agent–ის კვანძს სურს გადაცემა მობილურ კვანძთან ერთად გამოიყენებდეს home address მობილური კვანძისას, რომელსაც უგზავნის პაკეტებს. home agent იწერს ოაკეტებს და იყენებს ცხრილს, მობილური IPv6 იყენებს care of address, როგორც source მისამართი. მობილურ IPv4–ში სასარგებლო თვისება იყო optional set-ის გავლით კომპლექსის გაგრძელება , რომელიც მხარს არ უჭერდა ყველა კვანძს. ეს არ არის მოთხოვდანი კვანძი foreign Agentmobile IPv6-ში. როგორც ადრე აღვნიშნეთ Neighbour–ის აღმოჩენა და მისამართების ავტოკონფიგურაციის თვისებები საშუალებას აძლევს მობილური კვანძების ფუნქციონირების მომსახურებას სპეციალური როუტერის გარეშე. არ არის ფილტრაციის პრობლემა IPv6-Si. მობილურ IPv6-ში the correspondent კვანძი აკეთებს care of address მიმართვას, რომელსაც აქვს home address–ის დანიშნულების ვარიანტი.

1.4 ადრესაცია IPv6

პირველი მთავარი უპირატესობა IPv6–ისა IPv4–სგან განსხვავებით აქვს დიდი დამისამართების სივრცე, რომელიც შეიცავს მისამართებს, ინფორმაციას როუტერის პარამეტრებზე შემდეგი თაობის ინტერნეტში. IPv6 მხარს უჭერს 128–ბიტიან სამისამართო სივრცეს, რაც ტოლია 2_{128} ან უფრო ზუსტად 34w1038 უნიკალური IP მისამართი, დიდი სამისამართო სივრცის სქემასთან ერთად ერთად IPv6 აქვს შესაძლებლობა უნიკალური მისამართებით უზრუნველყოს თითოეული მოწყობილობა და კვანძი, რომელიც მიერთებულია ქსელში.

IPv6 მისამართების ტიპები:

IPv6 მისამართები არის ფართოდ კლასიფიცირებული და არსებობს 3 კატეგორიის:

1. Unicast address- მოქმედებს როგორც ერთი იდენტიფიკატორი ერთი ინტერფეისისთვის, IPv6 პაკეტები გაეგზავნება Unicast მისამართზე, რომელიც არის მიწოდებული ინტერფეისისათვის მათი მისამართებისთვის.
2. Multicast address- მოქმედებს როგორც, იდენტიფიკატორი ინტერფეისის ჯგუფს ან კომპლექტისათვის, რომლებიჩ შეიძლება ეკუთვნოდეს სხვადასხვა კვანძებს. IPv6–ში პაკეტის გაგზავნა არის Multicast address მიწოდება მრავალჯერადი ინტერფეისისათვის.
3. Anycast address – არის იდენტიფიკატორი ინტერფეისისა და განსხვავებული კვანძებს შორის. IPv6 –ში პაკეტი განკუთვნილია მისამართისთვის, ნიშნავს გაგზავნილია Anycast paketi erTi ერთი ინტერფეისიდან განსაზღვრული მისამართებისათვის..

1.5 ქსელის ნოტაცია Ipv6–ში

QIPv6 ქსელი არის აღნიშნული inter doman Routing-თვის. ქსელი ან მასკა Ipv6 პროტოკოლს, იგი აღინიშნება როგორც მომიჯნავე ჯგუფი Ipv6 მისამართების, რომლის ზომა უდნა იყოს ორის ტოლი, საწყისი ბიტი Ipv6 მისამართის ქმნის ქსელის პრეფიქსს. ბიტის ზომა ქსელის პრეფიქსში არის გამოყოფილი, მაგალითად 2001:cdba:9abc:5678::/64 . ქსელის მისამართს აღნიშნავს 2001:cdba:9abc:5678. ასეთი ქსელი შეიცავს მისამართებს 2001:cdba:9abc:5678:: –დან, 2001:cdba:9abc:5678:ffff:ffff:ffff:ffff.–მდე და აღინიშნება 128–ბიტიანი პრეფიქსით.

Ipv6 Deployment Around The World

პირელი ნაბიჯები Ipv6-ის შემოტანასთან დაკავშირებით: Ipv6-ის ფორუმი დაფუძნდა 1999 წელს ივლისში.მისი საერთო მისიაა ასწავლოს ინტერნეტ მომხმარებლებს Ipv6-ის უპირატესობები. ხელი შეუწყოს და განახორციელოს ამ პროტოკოლის მსოფლიოში დანერგვას.

მას აქვს წევრების სია, რომელიც მოიცავს მწარმოებლებს, წამყვან ტელეკომის ოპერატორებს. ინტერნეტ პროვაიდერებს, საკონსულტაციო კომპანებს და ა.შ. Ipv6-ის მიმდინარე სტატუსი ქვეყნის სხვადასხვა ნაწილებში არის საკმაოდ ხელშემწყობი ფაქტორი იმისა თუ რა შესაძლებლობა ექმენა მსოფლიოს ინტერნეტ სივრცეში უახლეს წლებში.

Canada

კანადის კვლევისა და განვითარების ფირმა სპეციალიზაციას აკეთებს წამყვან კომპიუტერულ ქსელის ტექნოლოგიებში. The freenet6.net უფლებას აძლევს ნებისმიერ. Ipv4 კვანძს დაუკავშირდნენ 6Bone. Ipv6-ის კავშირი მიღწეულია ა.შ.შ-სა და სხვა ქვეყნების მიერ.

Japan

Ipv6-ის განთაავსება იაპონიაში სარგებლობ, როგორც მთავრობის ძლიერი მხარდაჭერით.

China

ჩინეთის მთავრობამ ინიციატივა გამოთქვა პროექტზე, რომელიც არის 5 წლის გეგმა და რომელიც ეხება ინტერნეტ სივრცეს. Ipv6-ის განხორციელებასთან დაკავშირებით. ჩინეთი გეგმავს,
სათვალთვალო კამერიდან ყველაფერი შესრულდება Ipv6-ის გავლით.

France

Ipv6-ის სამუშო ჯგუფი შეიქმნა საფრანგეთში 2002 წლის 25 სექტემბერს. Ipv6-ის გავრცელება შესრულდა ეტაპობრივად საფრანგეთის ტელეკომის აქტიური ჩართულობით.

თავი 2

IPV4 ქსელები

2.1 IP V4-ის დახასიათება

IP - მისამართი (შემოკლ. ინგლ. Internet Protocol - ინტერნეტ ოქმი) – ლოკალურ ქსელში ან ინტერნეტში ჩართული მოწყობილობის (როგორც წესი კომპიუტერის) უნიკალური იდენტიფიკატორია (მისამართია).

IP - მისამართი ენიჭება ჰოსტის ქსელის ინტერფეისს ანუ ქსელურ ინტერფეისულ კარტას (network interface card (NIC)), რომელიც კომპიუტერის ერთ-ერთი შემადგენელი მოწყობილობაა. მაგალითად, საბოლოო მომხმარებლის მოწყობილობები ქსელური ინტერფეისებით მოიცავს მუშა სადგურებს - სერვერებს, ქსელურ პრინტერებს და IP - ტელეფონებს. სერვერებს შეიძლება ჰქონდეთ ერთზე მეტი NIC და შესაბამისად ყოველ მათგანს ცალკეული IP - მისამართი. მარშრუტიზაციის ინტერფეისებსაც, რომლებიც უზრუნველყოფენ კავშირს IP ქსელთან, შეიძლება გააჩნდეთ საკუთარი IP - მისამართი.

IP მისამართი

IP - მისამართი – ეს არის 32 ბიტის (ნულებისა და ერთების) კომბინაცია (IP V4). ორობითი IP- მისამართის წაკითხვა ძალიან რთულია და ამიტომაც 32 ბიტი იყოფა 4 ბაიტად, რომლებსაც უწოდებენ ოქტეტებს. ბიტებისგან შემდგარი IP - მისამართის ფორმატი ძალიან რთულია წასაკითხად, ჩასაწერად და დასამახსოვრებლად და ამიტომ, რომ უფრო ადვილი გახდეს IP - მისამართის წაკითხვა ყოველი ოქტეტის წარმოდგენა ხდება მისი ათობითი მნიშვნელობით, რომლებიც ერთმანეთისგან გამოყოფილია წერტილით.

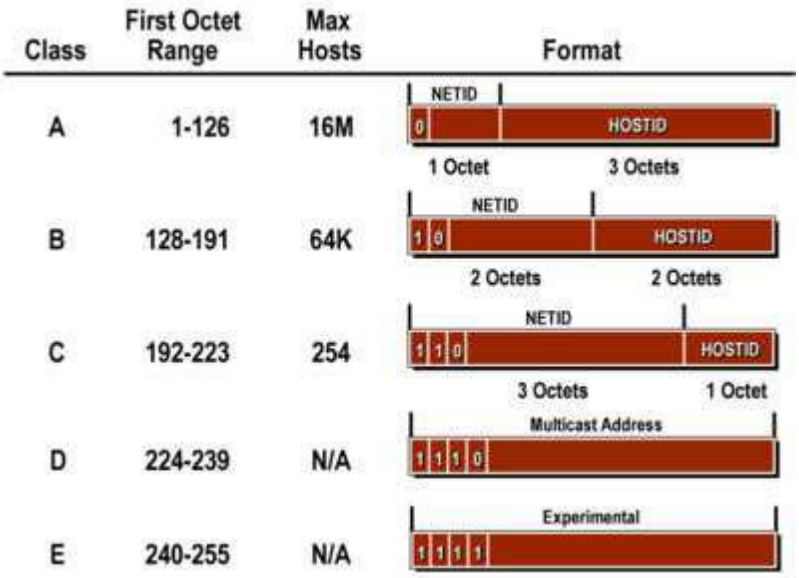
ყოველი პაკეტი, რომელიც გადაიცემა ინტერნეტში, შეიცავს მიმღებისა და გადამცემის IP - მისამართებს, რომლებიც საჭიროა იმისათვის, რომ მიაღწიოს ინფორმაციამ ადრესატამდე და უკან დაუბრუნდეს პასუხი.

IP V4 არის ინტერნეტ პროტოკოლის ყველაზე გავრცელებული ვერსია. იგი იყენებს 32 ბიტიან (4 ბაიტიან) მისამართებს, რომლის საზღვარიც არის 4294967296(2_{32}) მისამართი. მაგ. 123.123.123.123. თითოეულ სამ ციფრიან სექციას შეუძლია მიიღოს მაქსიმალური მნიშვნელობა 255.

ნებისმიერ კომპიუტერს ან მოწყობილობას, რომელსაც ინტერნეტთან აქვს კავშირი აუცილებლად უნდა ქონდეს უნიკალური IP მისამართი რათა ქონდეს კავშირი სხვა სისტემებთან ინტერნეტში. იმის გამო, რომ ინტერნეტში ჩართული სისტემების რაოდენობა დღითი დღე იზრდება IP V4 მისამართები მალე გათავდება.

2.2 კლასები

ამ შეზღუდვის დასაძლევად შეიქმნა კლასები. სისტემაში განისაზღვრება ხუთი კლასი A, B, C, D და E. A, B და C ქსელს გააჩნია განსხვავებული რაოდენობის ბიტები ქსელის იდენტიფიკაციისთვის. რაც ნიშნავს რომ თითოეული კლასი განსაზღვრავს სხვადასხვა რაოდენობის ქსელს. D კლასი არის მულტიკასტ მისამართებისთვის და E კლასი დარეზერვებულია. მაგრამ არც ეს აღმოჩნდა საკმარისი და ამ პრობლემის გადასაჭრელად შემოიღეს 128 ბიტიანი მისამართები IP V6, რომელიც ნელ-ნელა ანაცვლებს IP V4 სისტემას.



თუ IP მისამართის პირველი ბიტი იწყება 0-ით მაშინ ის მიეკუთვნება A კლასს 0-126. 127 არ გამოიყენება, რადგან იგი დარეზერვებულია სხვა მიზნებისათვის. A კლასის ქსელები ცოტაა, ხოლო მათში ჰოსტთა რაოდენობა შეიძლება იყოს 2^{24}.

თუ IP მისამართის პირველი ბიტი იწყება 10-ით მაშინ ის მიეკუთვნება B კლასს. ამ კლასის ქსელები მიეკუთვნება საშუალო სიდიდის ქსელებს, რადგან ქსელის და

ჰოსტის იდენტიფიკაციისთვის გამოიყენება 16-16 ბიტი.

თუ IP მისამართის პირველი ბიტი იწყება 110-ით მაშინ ის მიეკუთვნება C კლასს. აქ ქსელის ნომრისთვის გამოყენებულია 24 ბიტი, ხოლო ჰოსტისთვის 8 ბიტი.

თუ IP მისამართის პირველი ბიტი იწყება 1110-ით მაშინ ის მიეკუთვნება D კლასს ანუ multicast ჯგუფს.

თუ IP მისამართის პირველი ბიტი იწყება 11110-ით მაშინ ის მიეკუთვნება E კლასს რომელიც დარეზერვებულია.

1985 წლიდან გამოიგონეს მეთოდი რომ დაეყოთ IP მისამართები. მოხერხებული მეთოდი არის განსხვავებული სიგრძის ქვექსელის მასკა (VLSM (variable-length subnet mask)).

ეს არის რიცხვი, რომელიც გამოიყენება IP მისამართთან ერთად. მასკას ორობითი ფორმა შეიცავს ერთიანებს სამ თანრიგად, რომლებიც IP მისამართში განსაზღვრავს ქსელის ნომერს, რადგანაც ქსელის ნომერი შეადგენს მიმართის მთელ ნაწილს, ერთიანები მასკაში უნდა წარმოადგენდეს უწყვეტ თანმიმდევრობას.

თუ ყოველ IP მისამართში გამოვიყენებთ მასკას, მაშინ დამისამართების სისტემა უფრო მოქნილი ხდება. მაგ. 123.123.123.123 ასოცირდება 255.255.255.0 მასკასთან, ქსელის ნომერი იქნება 123.123.123. ხოლო ჰოსტ-ის 123. და არა 123 123.123.123 როგორც ეს კლასის მიხედვით არის განსაზღვრული

2.3 ჰოსტების რიცხვის გამოთვლა

ჰოსტების რიცხვი გამოითვლება შემდეგნაირად: ჰოსტების ბიტების რიცხვი უნდა ავიყვანოთ 2-ის ხარისხში ანუ (28 = 256). ამ რიცხვს უნდა გამოვაკლოთ 2 (256-2=254). 2-იანს იმიტომ ვაკლებთ, რომ ყველა 1-იანი IP-მისამრთის ჰოსტის ნაწილში არის ფართოამუწყებლობითი მისამართი ქსელისათვის და შეუძლებელია მინიჭებული ჰქონდეს ჰოსტისთვის. ხოლო 0-იანები ჰოსტის ნაწილში მიეკუთვნება ქსელს და ასევე შეუძლებელია მიენიჭოს ჰოსტს.

მეორე მეთოდი ჰოსტების რიცხვის განსასაზღვრავად: შევკრიბოთ ჰოსტის ყველა შესაძლო ბიტი (128+64+32+16+8+4+2+1=255). ამ რიცხვს გამოვაკლოთ 1 (255-1=254), რადგანაც ჰოსტის ბიტები ყველა არ შეიძლება იყოს 1-ის ტოლი. აქ არ არის აუცილებელი გამოვაკლოთ 2, რადგანაც 0-ის მნიშვნელობა 0-ია და თავისთავად არ დაემატება.

2.4 დამისამართება

ჰოსტის მისამართის დაკონფიგურირებისას გამოიყენება ათობითი სისტემა. ჰოსტი ღებულობს მისამართს 32 ორობითი ბიტის სახით NIC(Network Interface Card) ის მიერ. რომელიც მომხმარებლისთვის გარდაიქმნება ათობით ოთხ ოქტეტად. თითოეული ოქტეტი შედგება 8 ბიტისგან.

ლოგიკური IP მისამართი იერარქიულია და შედგება ორი, ქსელისა და ჰოსტის ნაწილისგან. მაგ. 123.124.125.126. პირველი ოქტეტი განსაზღვრავს ქსელს(123), ხოლო დანარჩენი ჰოსტს 124.125.126.

IP მისამართთან ერთად მოიცემა ქვექსელის მასკა, რომელიც ასევე 32 ბიტიანია და განასხვავებს მისამართში თუ რომელია ქსელის ნაწილი და რომელი ჰოსტის.

ქვექსელის მასკის და IP მისამართის შედარება ხდება მარცხნიდან მარჯვნივ თითოეული ბიტით. ერთიანები ქვექსელის მასკაში განსაზღვნავენ ქსელის ნაწილს, 0-იანები ჰოსტს.

როცა ჰოსტი გზავნის პაკეტს, ადარებს ქვექსელის მასკას თავის IP მისამართს და მიმღების IP მისამართს. თუ ქსელის ბიტები როგორც გადამცემის ასევე მიმღების შეესაბამება ერთმანეთს, მაშინ ორივე - გადამცემიც და მიმღებიც ერთ ქსელშია და პაკეტი გადაიცემა ლოკალურად. თუ არა, მაშინ გადამცემი პაკეტს გადაუგზავნის როუტერს სხვა ქსელში გასაგზავნად.

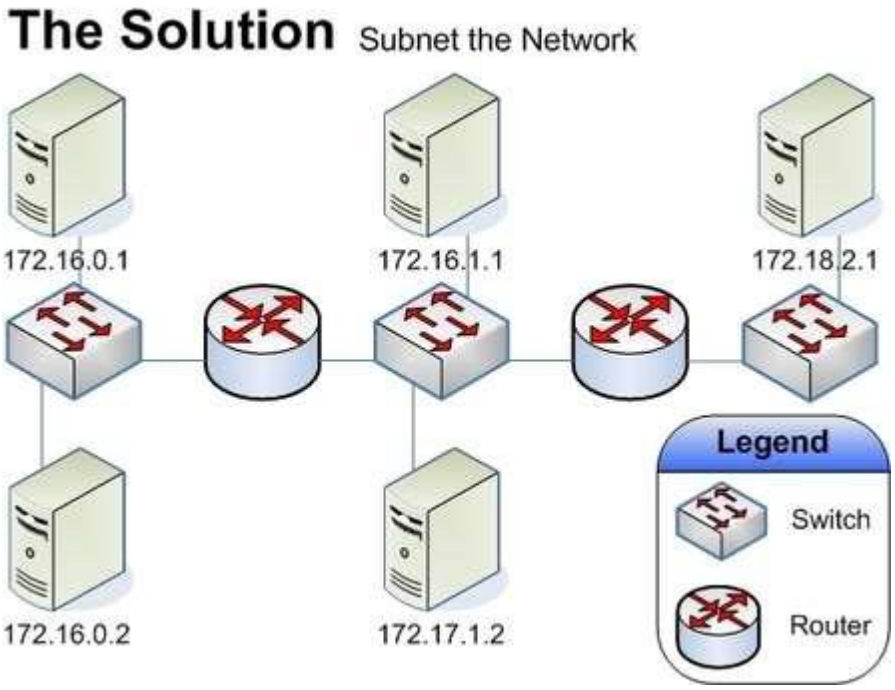
A 0-127

B 128-191

C 192-223

D 224-239

E 240-255



ყოველ ჰოსტს, რომელიც შეერთებულია ინტერნეტთან გააჩნია უნიკალური გარე IP მისამართი. რადგანაც 32-ბიტიანი მისამართების განსაზღვრული რაოდენობაა, არსებობს რისკი იმისა, რომ შეიძლება არ იყოს საკმარისი. ერთ-ერთი გადაწყვეტილება ამ პრობლემისა პერსონალური მისამართების დარეზერვებაა ორგანიზაციის შიგნით, რაც საშუალებას აძლევს ჰოსტებს ორგანიზაციის შიგნით ჰქონდეთ კომუნიკაციის საშუალება ერთმანეთთან უნიკალური IP მისამართის გარეშე.

RFC 1918 სტანდარტია, რომელიც არეზერვებს მისამართების რამოდენიმე დიაპაზონს შესაბამისად ყოველი კლასისათვის (A,B,C). პერსონალური მისამართები შეიცავენ ერთ A კლასის ქსელს, 16 B კლასის ქსელს და 256 C კლასის ქსელს. რაც ადმინისტრატორს აძლევს საკმაო მოქნილობას მიანიჭოს შიდა მისამართები.

IP მისამართები იყოფა შემდეგ კატეგორიებად: Unicast, Broadcast და Multicast მისამართები. ჰოსტი იყენებს Unicast IP მისამართს ერთი-ერთთან კომუნიკაციისას, Broadcast IP მისამართს ერთი-ბევრთან, ხოლო Multicast IP მისამართს ერთი-ყველასთან.

Unicast მისამართს ერთი-ყველასთან. IP ქსელისა. პაკეტი Unicast მისამართით დანიშნულია სპეციალური ჰოსტისთვის. მაგალითად შეიძლება მოვიყვანოთ ჰოსტი 192.168.1.5 IP მისამართით (გადამცემი), რომელმაც გააგზავნა მოთხოვნა WEB გვერდზე სერვერისგან IP მისამართისგან 192.168.1.200 (მიმღები).

Unicast პაკეტის გადაცემის და მიღების მომენტში მიმღების IP მისამართს შეიცავს IP პაკეტის თავსართი. შესაბამისი მიმღების MAC მისამართი გამოისახება Ethernet frame-ის თავსართი. IP მისამართი და MAC მისამართი კომბინირდება მონაცემების

გადასაცემად სპეციალური ჰოსტისთვის.

Broadcast მისამართის შემთხვევაში პაკეტი შეიცავს მიმღების IP მისამართს, რომელიც შეიცავს მხოლოდ ერთიანებს ჰოსტის ნაწილში. ეს ნიშნავს, რომ ყველა ჰოსტს ლოკალურ ქსელში შეუძლია მიიღოს და ნახოს პეკეტები. ქსელური პროტოკოლების უმრავლესობა, როგორიცაა: ARP და DHCP იყენებენ Broadcast –ს.

Multicast მისამრთის მეშვეობით გადამცემი პაკეტს გადასცემს მოწყობილობათა ჯგუფს.

მოწყობილობებს, რომელიც მიეკუთვნება Multicast ჯგუფს მიენიჭება Multicast ჯგუფის IP მისამართი. Multicast მისამრთის დიაპაზონი შეადგენს 224.0.0.0-დან 239.255.255.255-მდე. ე.ი. Multicast მისამრთები გამოსახავენ მისამართების ჯგუფს (ზოგჯერ უწოდებენ ჰოსტის ჯგუფებს), რომლებიც გამოიყენება პაკეტის მიმღები. გადამცემს კი ყოველთვის Multicast მისამართი გააჩნია.

2.5 IP V6 vs IP V4

IPv6 შემოთავაზებულ იქნა 1998 წელს RFC 2460.

თავდაპირველად ამიტომაც შეიქმნა ეს სისტემა, რომ მოგვარებულიყო IPv4 –ის IP მისამართების არასაკმარისი რაოდენობის პრობლემა, მაგრამ იყო სხვა მიზეზებიც. IPv4-ის თავდაპირველი სტანდარტიზაციისას ინტერნეტი საკმაოდ გაიზარდა. ამ დროს გამოჩნდა IPv4-ის უპირატესობები და ნაკლოვანებები, აგრეთვე ახალი შესაძლობლობების განახლებისა და დამატების შესაძლებლობები.

IPv6-ის მიერ შემოთავაზებული გაუმჯობესებული სერვისების ჩამონათვალი:

- სამისამართო სივრცის გაფართოება
- სამისამართო სივრცის უფრო სრულყოფილი მართვა
- მრავალმისამართიანი დამისამრთების, უსაფრთხოებისა და TCP/IP-ის გამარტივებული მართვა
- მარშრუტიზაციის ფუნქციის მოდენიზაცია
- მობილურობის გაუმჯობესებული მხარდაჭერა

სამისამართო სივრცის დიაპაზონი შეადგენს 2^128, ათობით ნოტაციაში ეს არის დაახლოებით 3 38 ნულით

IP V6-ს გააჩნია დაშიფვრის და აუტენტიფიკაციის უფრო მეტი შესაძლებლობა ვიდრე IP V4-ს. რაც ნიშნავს რომ ქსელები არის მეტად დაცული.

კიდევ ერთი გაუმჯობესებაა უფრო მეტი მისამართების სივრცე. რაც გამომდინარეობს იქიდან რომ მე-6 ვერსიას აქვს 128 ბიტიანი მისამართების სივრცე. შესაბამისად ერთ პერსონას შეიძლება ქონდეს უფრო მეტი მისამართი.

IP V6-ში არის ქსელის მენეჯმენტის და მარშრუტიზაციის უკეტესი სისტემა რადგან ქვექსელის უფრო დიდი სივრცეა.

ახალ ვერსიაში პროცესი გამარტივდა. IP V6 როუტერი აღარ ახორციელებს ფრაგმენტაციას. ამ სამუშაოთი დაკავებულია ჰოსტი. საერთო ჯამში პაკეტების დამუშავება როუტერის მიერ არის უფრო ეფექტური ვიდრე IP V4-ის შემთხვევაში.

ერთ-ერთი ყველაზე აღსანიშნავი დადებითი მხარე არის მულტიკასტინგი (multicasting). აღარ არის რთული ორგანიზაციებისთვის რომ მიიღონ გლობალურად მარშრუტირებატი მუტიკასტ ჯგუფი. უმჯობესდება მულტიკასტინგი, ჩაშენებულია წერტილების მისამართების დამთხვევა, საბოლოო ჯამში გაუმჯობესებულია ინტერ-დომენული გადაწყვეტილებები.

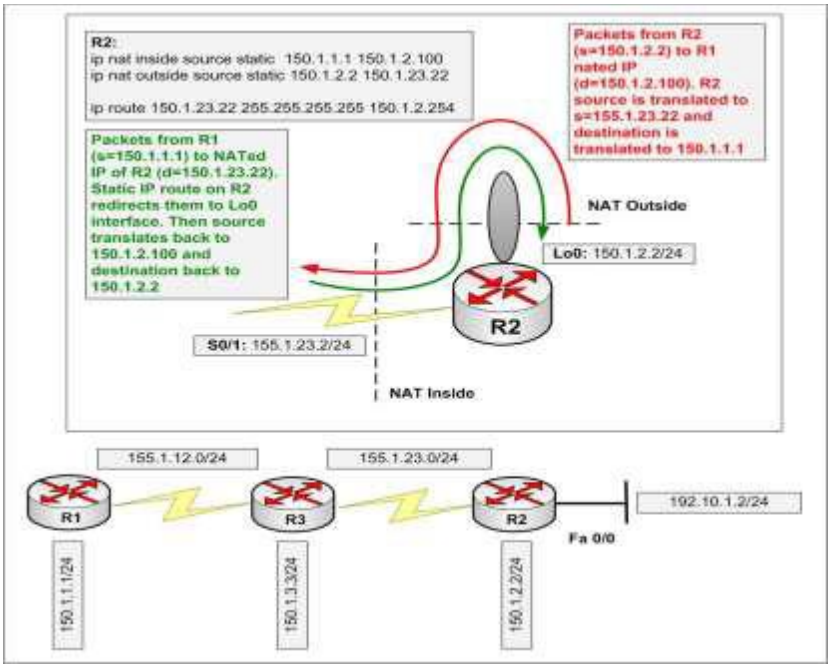
რადგან ინტერნეტი იზრდება და უფრო და უფრო მეტი მომხმარებელი ემატება, საჭირო იყო ინტერნეტ პროტოკოლის ახალი ვერსიის შემოღება რათა თავიდან აგვეცილებინა IP V4 -თ გამოწვეული პრობლემები.

2.6 რა არის NAT

როუტერი იღებს გარე მისამართს ISP- გან, რომლის მეშვეობითაც ის აგზავნის და იღებს პაკეტებს ინტერნეტით, რომელიც, თავის მხრივ, შიდა მისამართებით უზრუნველყოფს ლოკალური ქსელის კლიენტებს. აქედან გამომდინარე შიდა IP მისამართებს არა აქვთ წვდომა ინტერნეტთან, ამიტომ საჭიროა შიდა IP მისამართების გარე მისამართად გარდაქმნა, რომ ლოკალურ კლიენტებს ჰქონდეთ ინტერნეტთან კავშირი.

პროცესს, რომელიც გარდაქმნის შიდა მისამართებს მარშრუტირებად ინტერნეტ-მისამართებად, ეწოდება ქსელური მისამართების გარდაქმნა (Network Address Translation, NAT). NAT- ის მეშვეობით შიდა (ლოკალური) გადამცემის (source) IP მისამართი გარდაიქმნება გარე (გლობალურ) მისამართად. შემომავალი პაკეტების

შემთხვევაში მიმდინარეობს უკუპროცესი. ინტეგრირებული როუტერი გარდაქმნის შიდა IP მისამართებს გარე IP მისამართებად NAT- ის მეშვეობით.



ვინაიდან IP მისამართების რაოდენობა მკაცრად შეზღუდულია, ამიტომ თავისუფალი IP მისამართების რაოდენობა დროთა განმავლობაში სულ უფრო და უფრო მცირდება. ამიტომ კომპიუტერის IP მისამართები შეიძლება ასევე იყოს რეალური და არარეალური. რეალური IP მისამართები არის ისეთი მისამართები, რომლებიც არიან უნიფიცირებული ანუ არ მეორდებიან. არარეალური IP მისამართები კი მოქმედებენ მხოლოდ გარკვეული ლოკალური ქსელის ფარგლებში, ხოლო მის გარეთ ეს მისამართები არიან უჩინარი, უფრო სწორად ისინი ინტერნეტში ჩანან იმ IP მისამართით რაც გააჩნია იმ მოწყობილობას, რომელიც არის მათი ინტერნეტში გასასვლელი ანუ Default gateway. არარეალური მისამართების ერთ რეალურ მისამართად გადაყვანას უზრუნველყოფს NAT (Network Address Translation) ტექნოლოგია, რომელიც გაშვებულია იმ ქსელურ მოწყობილობაზე, რომელიც ასრულებს Default gateway-ის ფუნქციას.

თავი 3

IPsec

3.1 IPsec security

IPsec არის ჩარჩო, რომელი განსაზღვრავს უსაფრთხო კომუნიკაციას ქსელში. ეს სტანდარტი ასევე აღწერს თუ როგორ აღვასრულოთ ეს პოლიტიკა. IPsec–ის გამოყენებით მივაღწევთ მონაცემთა კონფიდენციალურობას, მთლიანობის აღდგენას, და მონაცემთა ავტორიზაციას.

RFC ამბობს: რომ არქიკექტურის მიზანია უზრუნველყოს სხვადასხვა უსაფრთხოების მომსახურება IPv4 და Ipv–ის გარემოში.

IPSec–ის მთავარი მიზანია უზრუნველყოს მაღალი ხარისხისი თავსებადობა. იგი გვთავაზობს სხვადასხვა უსაფრთხოების მომსახურებას და აგრეთვე დაცვას.

უსაფრთხოების მომსახურება არის კონტროლის წვდომისთვის , უკუკავშირის მთლიანობისთვის, მონაცემების წარმოშობის ამოცნობის,კონფიდენციალობის, შეზღუდული მოძრაობის ნაკადის კონფიდენციალურობის.

სპეციალური IPSec მხარდაჭერა

IPSec-is 3 მთავარი უპირატესობა: 1. აქვს სხვადასხვა ოპერაციული სისტემის პ;ატფორმის მხარდაჭერა. 2. სწორი VPN გადაწყვეტა, თუ გვსურს სწორი მონაცემთა კონფიდენტიალურობა ჩვენს ქსელში. 3. თავსებადობა სხვადასხვა მოწყობილობებს შორის არის ადვილი განსახორციელებლად.

3.2 ტექნიკური დეტალები

IPSec–ს აქვს 2 განსხვავებული რეჟიმი: ტრანსპორტირების რეჟიმი და ვირაბის რეჟიმი. ტრანსპორტის რეჟიმში სასარგებლო ტვირთი არის ინკაპსულირებული,გვირაბისრეჟიმი პაკეტებს დეკაპსილირებას უკეთებს. IP პაკეტები მთლიანად დეკაპსულირდება.

IPSec –ის სტანდარტი მხარს უჭრს მიმდინარე თავისებურებანს:

- AH– რომელიც უზრუნველყოფს უტყუარ გარანტიას გადაცენული პალეტებისა.
- ESP უზრუნველყოფს პაკეტების დაშიფვრას
- Pcomp უზრუნველყოფს პაკეტების შეკუმშვას დაშიფვრამდე
- IKE ინტერნეტ გასაღებების გაცვლა

IPSec აგრეთვე შეიცავს მიმდინარე კომპონენტებს: მონაცემთა უსაფრთხოების პოლიტიკა და მონაცემთა უსაფრხოების გაერთიანება.

PSec აგრეთვე ახორციელებს დისტანციური უსაფრთხოების წვდომის კავშირს (VPN–ის გამოყენებით. IPSec არ არის მხოლოდ VPN მექანიზმი. IPSec–ის გამოყენება შეიცვალა უკანასკნელი რამოდენიმე წლის განმავლობაში. როცა იგი გადავიდა –WAN დან LAN –ზე. რომელიც იცავს შიდა ქსელა ფარული გატეხვისა და სახეცვლილებისგან.

როცა 2 კმპიუტერს უნდა დაკავშიერება ერთ,ანეთთან PSec–ის გამოყენებით, პირველ რიგში ისინი ორმხრივად ადასტურებენ ერთმანეთს და იწყებენ მოლაპარაკებას თუ როგორ დაშიფრონ და ციფრულად მონიშნონ ისშემთხვევები რასაც ისინი გაცვლიან. სრული სახელწოდებაა SAs.

3.3 რატომ არის მნიშვნელოვანი IPSec

IPsec არის სავალდებულო კომპონენტი და ამიტომ IPsec უსაფრთხოება საჭიროა ყველა IP6-ის განხორციელებისთვის მომავალში. IPv6-ში IPsec ხორციელდება AH ავტორიზაციით და ESP გაფართოებით. IPv4-ში IPsec ხელმისაწვდომია თითქმის ყველა კლიენტისა და სერვერის ოპერაციული სისტემის პლატფორმისთვის. მნიშვნელოვანი ფაქტები IPv6-ისა დაინერგა ა.შ.შ-ში მიმდინარე წელს.

1. IPv6-ის მიმდინარე სტატუსი ქვეყნის სხვადასხვა ნაწილებში არის საკმაოდ ხელშემწყობი ფაქტორი იმისა თუ რა შესაძლებლობა ექნება მსოფლიოს ინტერნეტ სივრცეში უახლეს წლებში. ამჟამად მთელი დედამიწის მოსახლეობა შეადგენს 6.6 მილიარდს. არსებული IPv4 პროტოკოლის მისამართების დიაპაზონი სულ უფრო და უფრო შეზღუდული ხდება, რადგან შეინიშნება ინტერნეტის მომხმარებელთა მკვეთრი ზრდა ყოველდღიურად მსოფლიოში. ინტერნეტში შეინიშნება საკომუნიკაციო ტექნოლოგიების (ვიდეო, აუდიო, მონაცემების და ხმოვანი შეტყობინებების) IP-ის ბაზაზე კონვერგენციის გიგანტური ზრდა.

ამ პრობლემების გადაწყვეტის ერთ-ერთი გზაა IPv6-ზე გადასვლა. IPv6 პროტოკოლის სტრუქტურის გასაგებად მოცემულ ნაშრომში ძირითადი აქცენტი გადატანილია ქსელის არქიტექტურასა და მიგრაციაზე IPv6 ქსელებში. გამოიყენება ტუნელინგის ტრანზიტის მეთოდი სხვადასხვა ტიპის ქსელებში

თავი 4

ტუნელინგი

4.1 ტუნელინგის ეფექტურობის ანალიზი

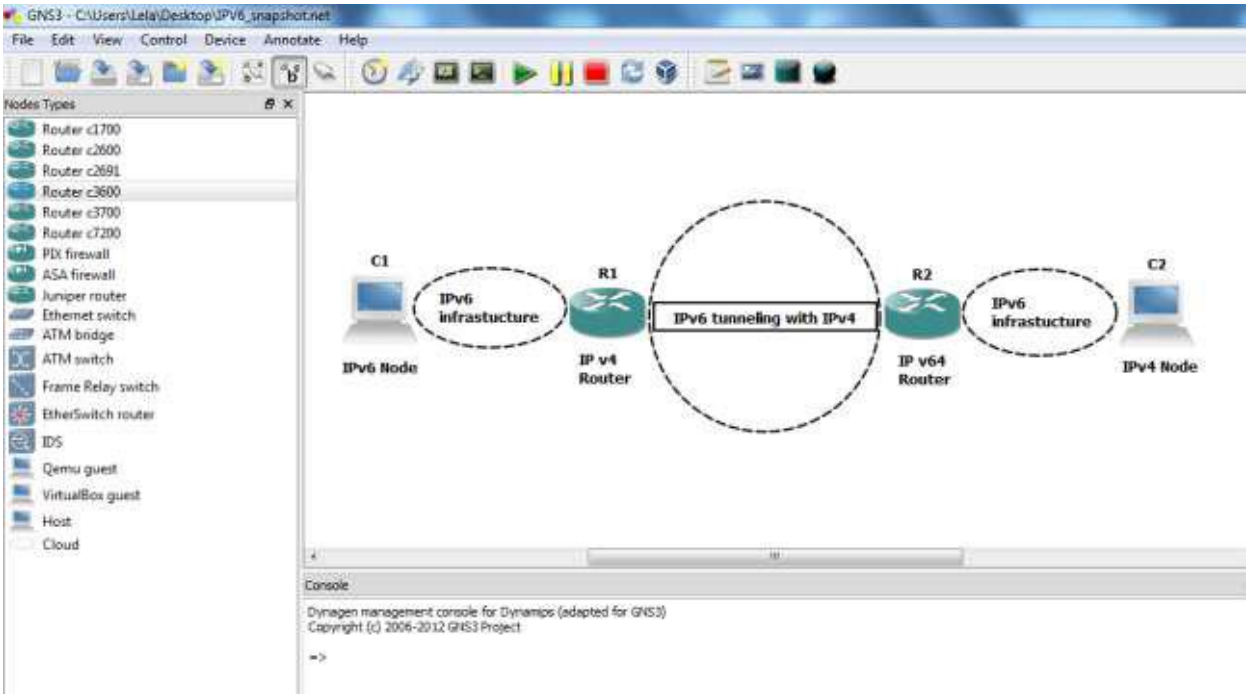
მოცემული სტატიის ძირითადი მთავარი მიზანია გამოვთვალოთ ეფექტურობის მახასითებლები IPv4 და IPv6 ქსელებისა, როგორც Windows გარემოში, ასევე Linux-ის პლატფორმაზე . ასევე გამოითვლება IPv4-დან IPv6-ზე გადასვლის მექანიზმის ეფექტურობის მახასიათებლები.
ზუსტი მიზნებია: I. IPv4 -ისა და IPv6 პროტოკოლების ტესტირება პლატფორმის Windows პლატფორმაზე. II. საწყისი IPv4 რომ IPv6 პროტოკოლი სტეკის სხვდასხვა ტიპის კონვერტაცია . კვლევების პეოცესში ორი სახის ტუნელინგი იყო გამოყენებული.

4.2 ტუნელინგის კონფიგურაციები

ტუნელინგის კონფიგურაციები IPv6/IPv4 სტეკისათვის IPv4 ინფრასტრუქტურისათვის შემდეგია:Router-to-Router ტუნელინგიHost-to-Host ტუნელინგი Router-to-Router ტუნელინგი . ამ ტიპის ტუნელინგს კონფიგურაცია მოიცავს ორი ძირითად IPv6/IPv4 მარშრუტიზატორს მონაწილეობს IPv4-ის ან IPv6-ის არქიტექტურაში IPv4 ინფრასტრუქტურის გამოყენებით.ლოგიკური ლინკის გასაყვანად მიმღებსა და წყაროს შორის, გამოიყენება გვირაბი.

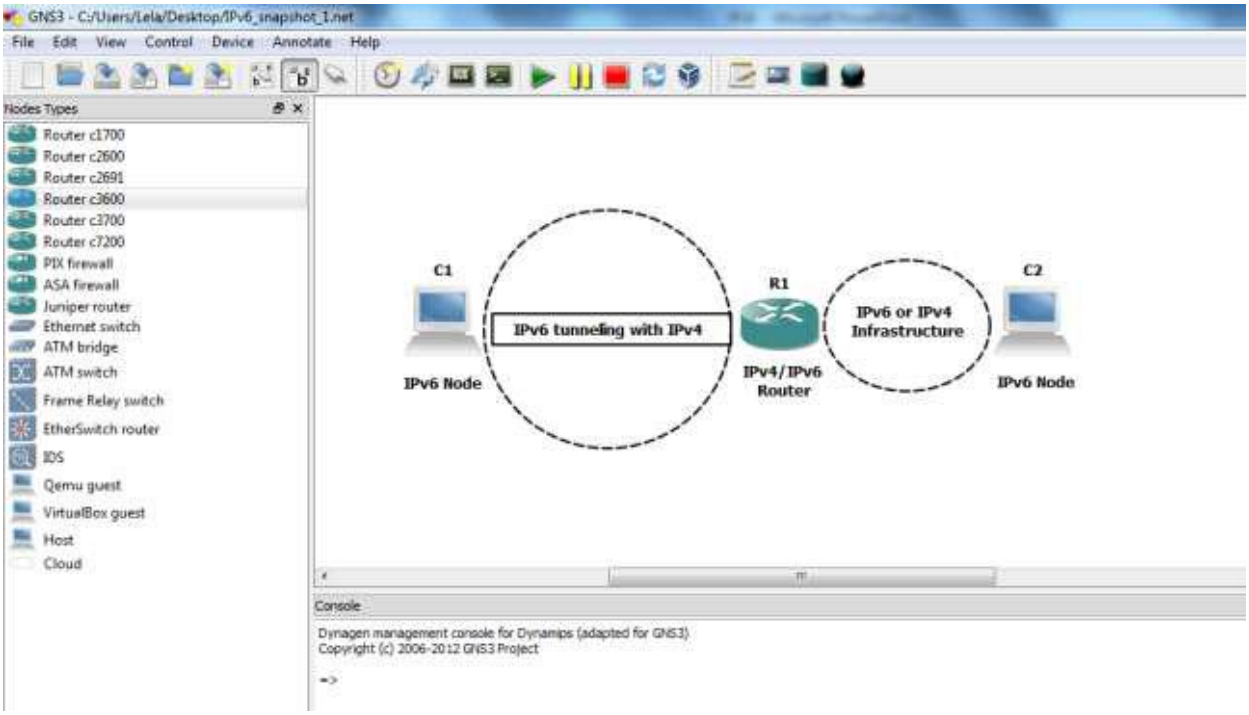
პაკეტი გაივლის IPv6/IPv4 როუტერს გვირაბის ინტერფეისის მეშვეობით, რომელიც შეესაბამება IPv6 ტრაფიკს IPv4 გვირაბში და განისაზღვროს მარშრუტები გვირაბის საზღვარზე.

შემდეგი სქემა აგებულია GNS3 პროგრამული უზრუნველყოფის გამოყენებით



პირველ შემთხვევაში ტუნელინგი ჰოსტი- როუტერი, IPv6 -ის ან IPv4-ის კვანძები, რომლებსაც მოიცავს ინფრასტრუქტურა თუ ორგანიზაცია IPv4 გენერირდება გვირაბი IPv6 IPv4 -ის გავლით, რომ მიაღწიონ IPv6/IPv4 დანიშნულების მარშრუტს.

ქვემოთ მოცემულ დიაგრამაზე ნაჩვენებია ჰოსტ- როუტერი ტუნელინგი (სადაც მონაცემთა პაკეტები გაივლიან A-დან B-მე) და როუტერის-ჰოსტი (მონაცემთა როუმინგისათვის B-დან A-მდე)

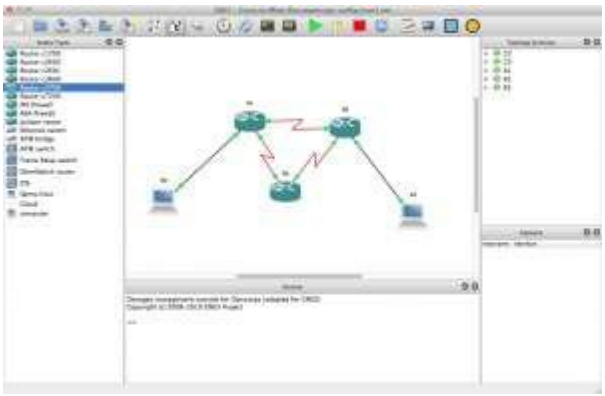


4.3 ლაბორატორია GNS3-ში

ლაბორატორიის აგება, რომელიც არის კონფიგურაციის შემოწმება. ქსელის ოქმებისა და თვისებებისთვის შეუცვლელი ნაბიჯია ამ ოქმებისა და მახასიათებლებისთვის წარმატებული დანერგვისთვის, რომელიც შევიდა წარმოების ქსელში. ქსელში კონფიგურაციის აგება და შემოწმება რისკის გარეშე, ორივე არის აუცილებელი პირობა.

რას გავაკეთებთ, როცა გავუშვებთ ვირტუალურ ლაბორატორიას: პირველ რიგში მრავალჯერადი როუტერის და ჰოსტის მაგალითი დესკტოპზე. როცა გამოვიყენებთ ამ ლაბორატორიას რომ შევქმნათ უსაფრთხო IPv6 ქსელი და მივიღოთ პრაქტიკული გამოცდილება.

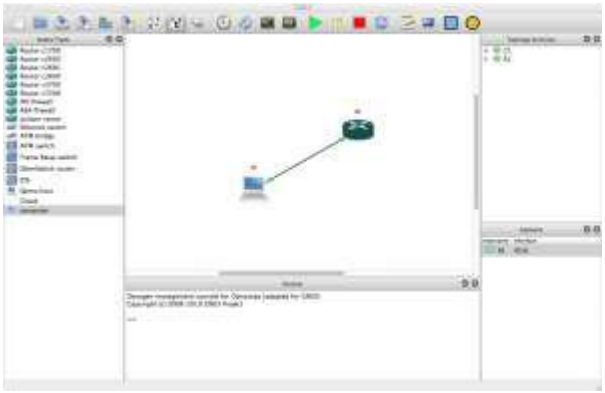
GNS3 არის გრაფიკული ქსელის სიმულატორი, რომელიც კომპლექსური ქსელის სიმულაციის საშუალებას გვაძლევს.



GNS3 საშუალებას გვაძლევს მოვახდინოთ როუტერის გადაადგილება. Line ბარათები შეიძლება დაემატოს ან შეიცვალოს ჩამოსაშლელი მენიუების გავლით. ტოპოლოგია და შემდგომი კონფიგურაცია არის ორივე შენახვადი. ძირითადად ყველა თვისება, რომელიც საჭიროა კონფიგურაციისთვის, იმისთვის რომ აიღოს საჭირო ტოპოლოგია. მინიჭებული აქვს GUI-ს ექვივალენტი, რომელიც მუშაობს Windows, Mac OSX, and Linuxგარემოში. არის კიდევ ძალიან ბევრი თვისება, მაგალითად უნარი დაუკავშირდეს სიმულაციურ გარემოს. პირველ რიგში საჭიროა GNS3 მუშაობის შემოწმება, სადაც შემდეგ გავივლით IPv6–ის ქსელის კონფიგურირებას. ცისკოს როუტერის მარტივი ტოპოლოგიის გამოყენებით.

4.4 ავტომატური დამისამართება

თვალი გადავავლოთ ავტომატურ დამისამართებას IPv6-ში. ვრთავთ როუტერს და ვუკავსირდებიტ IPv6-ის მარშუტიზატორს. სერვერი უკავშირდება ინტერნეტს და უმატებს IPv6-ის მისამართს. დავრწმუნდეთ, რომ ვიყენებტ a /64 პრეფიქსს და ამის შემდეგ SLAAC იმუშავებს შესაბამისად.

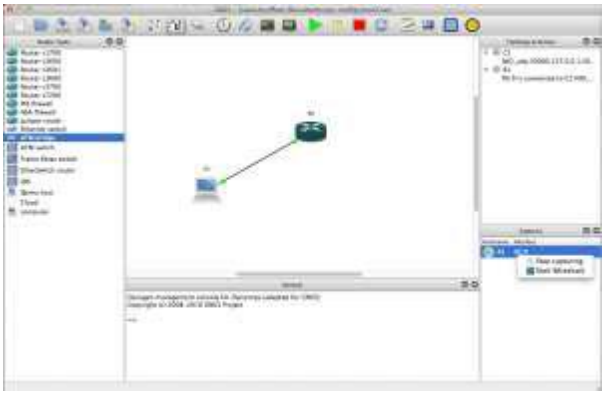


QEMU ან VPCS სერვერზე დავრწმუნდეთ, რომ ip auto დაკონფიგურირებულია. შემდეგ ვუშვებთ show ბრძანებას. სავარაუდოდ თუ ყველაფერი მუშაობს, უნდა დავინახოთ SLAAC-ის მისამართი, რომელიც მიეთითა როუტერის ინტერფეისს.

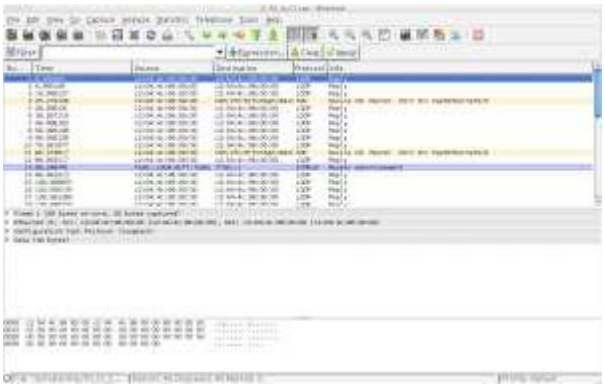
დავპინგოტთ როუტერის ინტერფეისი. შემდეგ გავუშვათ რამოდენიმე სხვადასხვა ბრძანება როუტერზე. დავუბრუნდეთ ის ადგილს, სადაც გავცერდით. შევხედოთ captures, რომელიც მოგვცემს უფრო მეტ გამტარუნარიანობას, თუ რა ხდება SLAAC-თან.

ახლიდან შევქმნათ ტოპოლოგია და კონფიგურაცია ბოლო პოსტიდან. ტოპოლოგიის ფანჯარაში დავაწკაპუნოთ მარჯვენა ღილაკით ლინკზე, რომელიც არის როუტერსა და პორტს შორის. ავირჩიოთ captures და შემდეგ ავირჩიოთ ინტერფეისი. (თუ ვიყენებდით როუტერის პორტის ტოპოლოგიას, როუტერის ინტერნეტის ინტერფეისი გამოჩნდება როგორც არჩევანი). თუ გვაქვს გააქტიურებული ინტერფეისი, GNS3 გამოთქვამს უკმაყოფილებას,რომ არ არსებობს ტრანსპორტი მის გასაშვებად. (რომ გქონდეს, მაინც შეიძლება მიიღო შეცდომა ყველა შემთხვევაში, მაგრამ უნდა ვნახოთ როუტერის ინტერფეისი GNS3-ის ეკრანის captures ნაწილში.

Captures ვინდოუსში დავაჭიროთ ღილაკს ინტერფეისზე და ავირჩიოთ Start Wireshark X11.

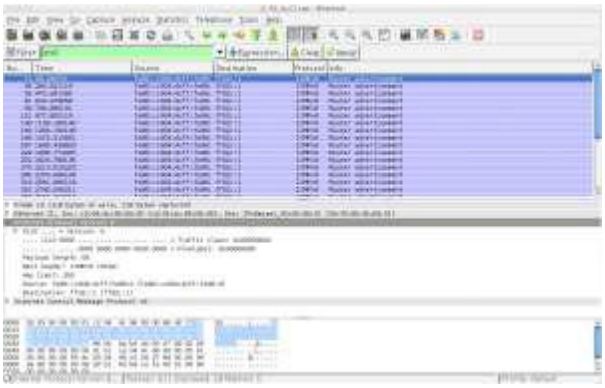


შემდეგ გაეშვება Wireshark და უნდა მივიღოთ ასეთი ეკრანი.



გავფილტროთ პაკეტები, რომლებიც არ არის დაკავშირებული IPv6-თან. IPv6-ის შემდეგ ფილტრის ყუთში ვაჭრთ Apply. თუ ჯერ არ გაუკეთებია კონფიგურაცია IPv6 მისამართისთვის, ჩვენ მხოლოდ ვნახავთ როუტერის გამცხადებებს.

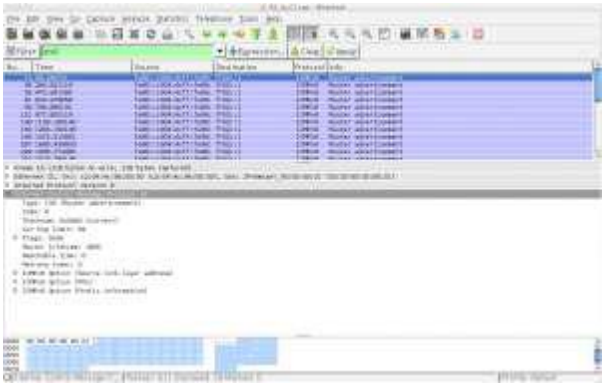
პირველ რიგში გავაფართოვოთ Ethernet II-ის სათაური ვინდოუსის ცენტრში. შენიშვნა:



EtherType არის მითითებული 0x86DD –სთვის,
რომელიც მიუთითებს IPv6-ს. შემდეგი სათაური მიუთითებს 56-ის მნიშვნელობას.
რომელიც ადნიშნავს, რომ პაკეტი არის ICMPv6.

Hop ლიმიტი არის მითითებული როგორც 255, რომელიც გულისხმობს, რომ პაკეტი არის შეზღუდული ადგილობრივი სეგმენტისთვის და იქნება შეზღუდული რომელიმე როუტერისთვის.

საწყისი მისამართი იქნება ლინკი ადგილობრივი მისამართისა, ხოლო დანიშნულების მისამართი არის ლინკი, რომელიც მოიცავს ff02::1 მისამართის ყველა კვანძს.

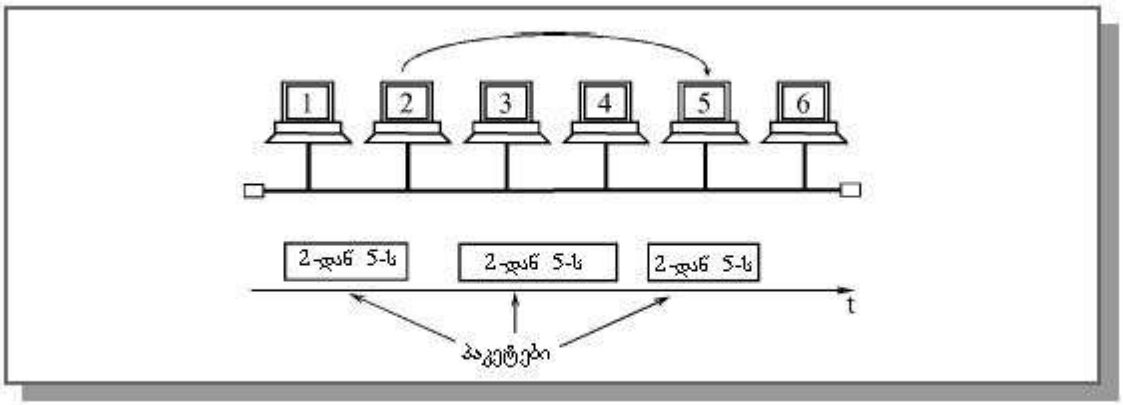


ბოლოს გავაფართოვოთ Internet Control
Message Protocol v6 სათაური, შემდეგ კი ICMPv6 Option ქვესათაური.

ICMPv6 პაკეტის ტიპი ზუსტად არის განსაზღვრული, როგროც 134. კოდი Router Advertisements და ICMPv6 Option ქვეშ განთავსებულ ქვესათაურად. ჩვენ შეგვიზლია ვნახოთ გამოქვეყნებული პრეფიქსი /64, რომელიც დავაკონფიგურირეთ როუტერის ინტერფეისზე. მაგალითად: 2001:db8:cafe:1::). ვცადოთ ამოვშალოთ და ხელმეორედ დავამატოთ /64 ინტერფეისი როუტერის ინტერფეისზე. ეს გამოიწვევს მეზობელი პაკეტების აღმოჩენას უნდა გვქონდეს უფლება, თუ როგორ დაგვეხმაროს GNS3 peek under the hood IPv6-ისთვის

4.5 პაკეტის ფორმატი

პაკეტები შედგება მმართველი ინფორმაციისგან , რომელიც აუცილებელია იმისათვის რომ პაკეტი მიეწოდოს აგენტს და სასარგებლო მონაცემებისგან , რომლების აუცილებელია გადასაგზავნად . მმართველი ინფორმაცია იყოფა შემდეგ ნაწილებად : ზირითადი ფიქსირებული სათაურის შემადგენლობაში მყოფი და დამატებით არა საჭირო სათაურის შემადგენლობაში მყოფი . სასარგებლო მონაცემები , როგორც წესი არის დეიტაგრამა ან უფრო მაღალი სატრანსპორტო დონის პროტოკოლის ფრაგმენტი , მაგრამ შეიძლება იყოს ასევე ქსელის დონის ფრაგმენტები (მაგ : ICMPv6) ან არხული დონის (მაგ : OSPE) .



ნახ.3.1. პაკეტების გადაცემა ქსელში ორ აბონენტს შორის

IPv6 პაკეტები ჩვეულებრივ გადაეცემა არხული დონის პროტოკოლების მიერ , მაგ : Enthernet , რომელიც ინკაპსულაციას უკეთებს თითოეულ პაკეტს , მაგრამ IPv6 შეიძლება გადავიდეს ასევე უფრო მაღალი დონის საგვირაბო პროტოკოლით .

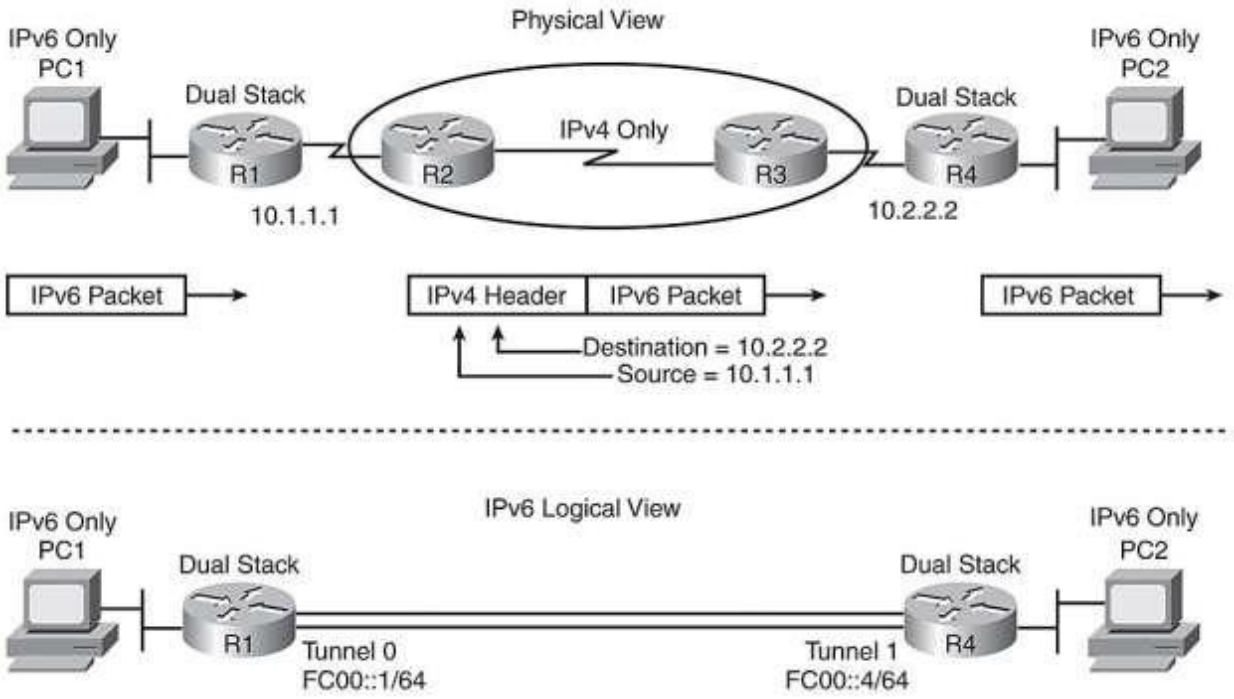
4.6 ნოტაცია

IPv6 მისამართები გამოისახება როგორც 8 ჯგუფი , ოთხი თექვსმეტობითი ციფრით . რომლებიც გაყოფილნი არიან ორი წერტილით . მისამართის მაგალითი :

```
2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d
```

თუერთი ან მიყოლებით რამდენიმე ჯგუფი ტოლია 0000 , მაშინ ისინი შეიძლება გამოტოვოს და ჩასმული იყოს მათ მაგივრად ორმაგი წერტილები (::) მაგ :

```
http://[2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d]:8080/
```



4.7 IP V4 მისამართების შემცირება 2012 წლისთვის

ადრე IP V4 მისამართების შემცირება ემთხვეოდა 2000 წელს, მაგრამ ახლა ითვლება 2012 წელი. 2033 წელს APWIC დირექტორმა პოლ უილსონმა განაცხადა რომ ეყრდნობოდა იმდროინდელ ინტერნეტის ქსელის გაფართოების მონაცემებს . თავისუფალი სამისამართო სივრცე საკმარისია მხოლოდ ერთი ორი ათწლეული. 2005 წლის სექტემბერში cisco systems ივარაუდა, რომ ხელმისაწვდომი მისამართების რაოდენობა ეყოფოდა 4 5 წელი.

2011 წლის 3 თებერცვალს JAVA სააგენტომ გაუნაწილა IP V4 -ის ბოლო 5 ბლოკი რეგიონალურ ინტერნეტ-რეგისტრატორებს. დიაპაზონური მისამართების გამოყოფა RIR-ის რეგიონალურ სამსახურებზე გრძელდება. მაგრამ გამოკვლევების თანახმად დარჩენილი მისამართები საკმარისია მხოლოდ 2012 წლის აგვისტომდე.

პროტოკოლის ტესტირება

2011 წლის ივნისში შედგა IP V6-ის საერთაშორისო დღე. ეს არის ღონისძიება ტესტირების სახით, თუ როგორ არის მსოფლიო ინტერნეტ-საზოგადოება IP V4 -დან IP V6-ზე გადასასვლელად. ამ ღონისძიებების გარგლებში აქციაში მონაწილე კომპანიებმა დაუმატეს თავის საიტებს IP V6-ის ჩაწერები ერთი დღით. ტესტირებამ ჩაიარა წარმატებით.

დაგროვილი მონაცემები გაანალიზდება და იქნება გათვალისწინებული პროტოკოლის შემდგომი დანერგვისას და რეკომენდაციების შემუშავების დროს.

4.8 პროტოკოლის დანერგვა

IP V6-ზე გადასვლა დაიწყო google-ში 2008 წელს. IP V6-ის ტესტირება ჩაითვალა წარმატებულად. 2012 წლის 6 ივნისს შედგა IP V6-ის საერთასიშორისო გაშვება. ინტერნეტ პროვაიდერები ჩართავენ თავისი მომხარებლების 1% IP V6-. ქსელური აღჭურვილობის მწარმოებლები აქტიურებენ IP V6 დამარეგულირებლების სახით მარშუტიზატორების გასაჩუმებლად(cisco, D link). ვებ კომპანიები ჩრთავენ IP V6 თავიას ძირითად საიტებში(google). ხოლო ზოგიერთებს გადაყავთ IP V6-ზე კორპორატიული ქსელები. მომავალი სტანდარტის სპეციფიკაციის LTE მობილური ქსელებისთვის აუცილებელია IP V6 პროტოკოლის მხარდაჭერა.

4.9 IP V4-თან შედარება

ამტკიცებენ ხანდახან რომ ახალმა პროტოკოლმა შეიძლება უზრუნველყოს $5 \cdot 10^{28}$ მისამართი დეედამიწის თითოეულ მცხოვრებზე. ამავე დროს ასეთი უზარმაზარი სამისამართო სივრცე შემოტანილი იყო მისამართების იერარქიისათვის(ეს ამარტივებს მარშუტიზაციას). მისი უდიდესი ნაწილი არ დარეგისტრირდება არასოდეს. მიუხედავად ამისა მისამართების გადიდებული სივრცე შექმნის NAT-ს არასაჭიროდ.

IP V6-დან ამოღებული იყო მარშუტიზატორების მუშაობის გამამნელებელი ფუნქციები:

- მარშუტიზატორები აღარ ყოფენ პაკეტებს ნაწილებად.(შეიძლება პაკეტის გაყოფა მიმწოდებლის მხრიდან). შესაბამისად ოპტიმალური MTU უნდა მოიძებნოს path MTU discovery-ს დახმარებით პროტოკოლის უკეთესი მუშაობისთვის. მინიმალური MTU აწეულია 1280 ბაიტამდე. ინფორმაცია პაკეტების გაყოფის შესახებ გამოტანილია საერთო წინასიტყვაობიდან

- გაქრა საკონტროლო მასა. იმის გათვალისწინებით რომ არხული და სატრანსპორტო პროტოკოლებო ამოწმებენ პაკეტის კორექტულობას, ამიტომ საკონტროლო მასა IP დონეზე აღიქმება როგორც ზედმეტი.

მიუხედავად IP V6-ის დიდი ზომის მისამართისა ყოველმა ასეთმა გაუმჯობესებამ გააგრძელა პაკეტის სათაურის სიგრძე მხოლოდ 20დან 40 ბაიტამდე.

IP V6-ის შედარება IP V4თან

- ზესწრაფ ქსელებში შესაძლებელია უდიდესი პაკეტების მხარდაჭერა 4 გიგაბაიტამდე.
- Time to live გადასათაურებულია hop limit-ად.

- გაჩნდა ნაკადების ნიშნულები და ტრაფიკის კლასები

- გაჩნდა მრავალმისამართიანი მაუწყებლობა

დასკვნა

მოცემულ სამაგისტრო ნაშრომში გამოთვლილია IPv4-დან IPv6-ზე გადასვლის მექანიზმის ეფექტურობის მახასიათებლები. წარმოდგენილია ტუნელინგის კონფიგურაციები IPv6/IPv4 სტეკისათვის IPv4 ინფრასტრუქტურისათვის, როგორიცაა: Router-to-Router ტუნელინგი და Host-to-Host ტუნელინგი. Router-to-Router ტიპის ტუნელინგის კონფიგურაცია მოიცავს ორი ძირითად IPv6/IPv4 მარშრუტიზატორს, რომელიც მონაწილეობს IPv4-ის ან IPv6-ის არქიტექტურაში IPv4 ინფრასტრუქტურის გამოყენებით, სადაც ლოგიკური ლინკის გასაყვანად მიმღებსა და წყაროს შორის გამოიყენება გვირაბი.

ლიტერატურა

1. http://www.infoblox.com/community/blog/using-gns3-model-simple-ipv6-network-part-1
2. http://www.infoblox.com/community/blog/using-gns3-model-simple-ipv6-network-part-2
3. http://www.infoblox.com/community/blog/using-gns3-model-simple-ipv6-network-part-3
4. http://www.ipv6.com/articles/general/ipv6-the-next-generation-internet.htm
5. http://www.ipv6.com/articles/mobile/Mobile-IPv6.htm
6. http://www.ipv6.com/articles/general/IPv6-Addressing.htm
7. http://www.ipv6.com/articles/deployment/IPv6-Deployment-Status.htm
8. http://www.ipv6.com/articles/security/IPsec.htm