ივ. ჯავახიშვილის სახ. თბილისის სახელმწიფო უნივერსიტეტი

ზუსტ და საბუნებისმეტყველო ფაკულტეტი

გურამი ასანიშვილი

უსაფრთხოება IPv6 ქსელებში

სამაგისტრო პროგრამა: ინფორმაციული ტექნოლოგიები

სამაგისტრო ნაშრომი შესრულებულია ინფორმაციული ტექნოლოგიების მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

სამაგისტრო ნაშრომის ხელმძღვანელი
ასისტენტ-პროფესორი: პაპუნა ქარჩავა

თბილისი 2015

ს ა რ ჩ ე ვ ი

ა ნ ო ტ ა ც ი ა

ამ ნაშრომში განხილულია IPv6 ქსელთან დაკავშირებული უსაფთხოების პრობლემები. საფრთხის და შეტევის ძირითადი ტიპები, მათი აღმოჩენის, იდენტიფიკაციის და მათგან თავის დაცვის მექანიზმები. ასევე განხილულია IPv6 ქსელში არსებული დამისამართების მეთოდები. აქ წამოდგენილია იდეა DHCPv6 პროტოკოლის განახლების შესახებ. გაუმჯობესებულ მოდელში განახევრებულია შუამავალი პაკეტების რაოდენობა, რომელიც აუცილებელია იმისთვის რომ მოწყობილობამ მიიღოს IPv6 მისამართი და სხვა კონფიგურაციის პარამეტრები. ასევე წარმოდგენილია მისი უპირატესობები IPv6 ქსელის უსაფრთხოების საკითხებში. შემოთავაზებულია ოპერაციული სისტემებისთვის ინტერნეტ პროტოკოლის კონფიგურაციის განახლებული ინტერფეისი.

In this work are discussed security problems that exist associated with IPv6 network. Threat and types of attacks, how to detect, identify and protect the computer system. Here it is presented idea about one improvements of the DHCPv6 protocol. In the improved model the quantity of packages which are necessary to dynamically assign the IPv6 address and other necessary parameters of a configuration to the device decreased to a half. Also is presented its advantages in IPv6 security and suggested new interface for IP configuration for operating systems.

შესავალი

კომპიუტერების გამოჩენის პირველივე დღიდან არ შეწყვეტილა სამუშაოები გაუმჯობესებინათ ის, ყოფილიყო უსაფრთხო და ხელმისაწვდომი ნებისმიერი ადამიანისათვის. ტექნოლოგიების სწრაფმა განვითარებამ პერსონალური კომპიუტერები ხელმისაწვდომი გახადა ნებისმიერი მსურველისათვის. 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 საშუალებით 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) [1]. IPv4 პროტოკოლის დამპროექტებლების მიერ მოწყობილობათა იდენტიფიცირებისათვის გამოყენებული იყო დამისამართების 32-თანრიგა ორობით სისტემა, რაც იძლეოდა დაახლოებით 4 მილიარდ 300 მილიონი მოწყობილობის დამისამართების შესაძლებლობას.

ტექნოლოგიების სწრაფი განვითარებით გაიზარდა არამხოლოდ ქსელში გაწევრიანების შესაძლებლობის მქონე მოწყობილობების რაოდენობა, არამედ გაიზარდა ქსელთან დაკავშირებული მოწყობილობების რაოდენობაც. ამან წარმოქმნა მრავალი საფრთხე მათ შორის, IPv4 პროტოკოლის მიერ მოწყობილობათა დამისამართებისათვის გამოყენებული სივრცეში მისამართების სიმცირე, გლობალურ ქსელში ინფორმაციის უსაფრთხო გადაცემა ყოველდღიურად ახალი საფრთხის წინაშე დგას.

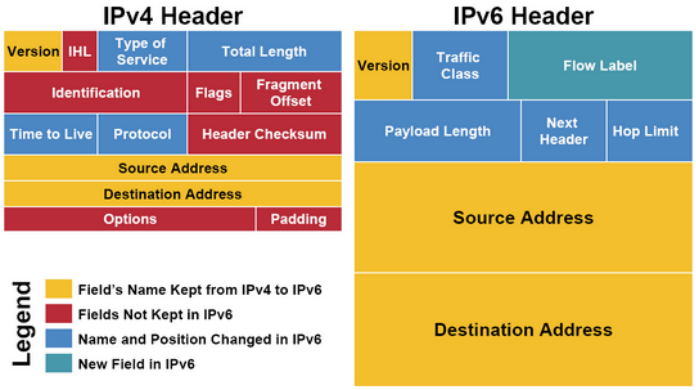
თავდაპირველად IPv4 პროტოკოლის დამპროექტებლებმა ჩათვალეს, რომ მონაცემთა გადაცემას რაიმე სახის საფრთხე არ უნდა შექმნოდა და შესაბამისად, მასში

არ იყო გათვალისწინებული უსაფრთხოების მექანიზმები. უსაფრთხოებასთან დაკავშირებული სიტუაცია შეცვალა 90-იან წლებში გამოჩენილმა ე.წ „ჭიამ“ (worm) [2]. ამ დროიდან მოყოლებული აქტიურად მიმდინარეობს სამუშაოები მონაცემთა უსაფრთხო გაცვლის უზრუნველსყოფად. შედეგად საკმარისად განვითარდა IPv4 პროტოკოლიც.

მიუხედავად IPv4 პროტოკოლის განვითარებისა და მასში მრავალი მექანიზმის (NAT [3], PAT [4] და ა.შ.) გამოჩენისა, რომელიც მიმართული იყო მისამართების სივრცის დიდი ხნით შენარჩუნებისა და უსაფრთხოების პრობლემების აღმოსაფხვრელად, აუცილებელი შეიქმნა ახალი პროტოკოლის შემუშავება. IP პროტოკოლის დამპროექტებლებმა შეიმუშავეს ინტერნეტ პროტოკოლის ახალი ვერსია 6 (IPv6) [5], რომელშიც გაითვალისწინეს IPv4 პროტოკოლის გამოყენებისას მიღებული ცოდნა და გამოცდილება.

IPv6 პროტოკოლი შეიქმნა გასული საუკუნის 90 -იანი წლების ბოლოს და მას სრულად უნდა ჩაენაცვლებინა მისი წინამორბედი, მაგრამ მან ჯერჯერობით ამის გაკეთება გარკვეული ფინანსური და მატერიალური დანახარჯების გამო ვერ ხერხდება. ვინაიდან IPv6 შიქმნა არსებული ცოდნისა და გამოცდილების გათვალისწინებით, ამიტომ ის წარმოადგენს IPv4-ის ერთადერთ ხანგრძლივ შემცვლელს.

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.



ნახ. 1. განსხვავება IPv4 და IPv6 პაკეტების თავსართებს შორის

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.

სამაგისტრო ნაშრომი შეეხება IPv6 ქსელის უსაფრთხოებას. მასში განხილულია IPv6 ქსელში არსებული უსაფრთხოების მექანიზმები.

სამაგისტრო ნაშრომი დაყოფილია სამ თავად:

1. IPv6 პროტოკოლთან დაკავშირებული ძირითადი ცნებები;
2. IPv6 ქსელზე შემოტევის ტიპები;
3. IPv6 ქსელზე შემოტევისაგან დაცვის მექანიზმები.

მოკლედ აღვწეროთ თემის შინაარსი.

თავი I - IPv6 პროტოკოლთან დაკავშირებული ძირითადი ცნებები

§1 -ში განსაზღვრულია IPv6 პროტოკოლი [6, 7]. მოყვანილია IPv6 პაკეტის თავსართის სტრუქტურა და ის შედარებულია მისი წინამორბედი IPv4 პაკეტის შესაბამის თავსართს. განხილულია IPv6 დამისამართების სქემები. პარაგრაფის ბოლოს შემოღებულია დამისამართების ახალი სქემა, რომელიც მიიღება დამისამართების EUI-64 [8] და DHCP [9] მეთოდების გამოყენებით (ამ მეთოდს პირობითად ვუწოდოთ DHCP-EUI-64 [10]). დამისამართების ახალი მეთოდი იძლევა კომუნიკაციისათვის საჭირო პარამეტრების მიღებას პაკეტების განახევრებული რაოდენობით, რაც თავისმხრივ მნიშვნელოვანია უსაფრთხოების თვალსაზრისით.

§2 -ში განხილულია IPv6 ქსელში კომუნიკაციისათვის მნიშვნელოვანი პროტოკოლები, როგორიცაა ICMPv6 [11], MLD [12], NDP [13], DAD [14] და ა.შ., აღწერილია მათი როლი IPv6 ქსელში, პაკეტის ფორმატი და ფუნქციები, რომლებიც მათ გააჩნიათ.

თავი II - IPv6 ქსელზე შემოტევის ტიპები:

§1-ში აღწერილია უსაფრთხოების არსებული კატეგორიები, რა ნაკლოვანება გააჩნა თითოეულ მათგანს.

§2 -ში განხილულია IPv6 ქსელის უსაფრთხოებასთან დაკავშირებული საკითხები. აღწერილია IPv6 ქსელში არსებული რისკები. განხილულია საფრთხეები, რომლებიც შეიძლება გამოჩნდეს IPv6 ქსელში.

§3 -ში განხილულია გლობალური ქსელიდან მომავალი საფრთხეები.

§4 -ში განხილულია IPv6 პროტოკოლის მიერ გამოყენებული პროტოკოლების სუსტი მხარეები.

§5 -ში ერთმანეთთან შედარებულია IPv4 და IPv6 პროტოკოლების ყოფაქცევა უსაფრთხოების საკითხებში.

თავი III - IPv6 ქსელზე, შემოტევის აღმოჩენა და დაცვის მექანიზმები

§1 -ში განხილულია სხვადასხვა ტიპის საფრთხეების აღმოჩენის მეთოდები და მათგან დაცვის მექანიზმები.

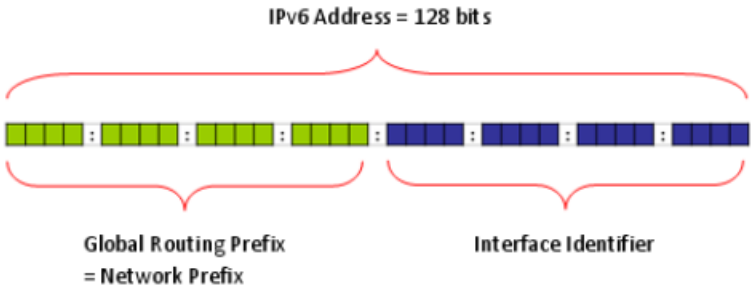
§2-ში განხილულია IPv6 ქსელში DHCP-EUI-64 მეთოდის შემოღებით გაუმჯობესებული უსაფრთხოება

§3 -ში განხილულია თანამედროვე ოპერაციულ სისტემებში არსებული IPv6 პროტოკოლის კონფიგურირების სამომხმარებლო ინტერფეისი და შემოთავაზებულია განახლებული ინტერფესი, რომელშიც გათვალისწინებულია IPv6 -ში დამისამართების ყველა სქემა.

თავი I. IPv6 პროტოკოლთან დაკავშირებული ძირითადი ცნებები

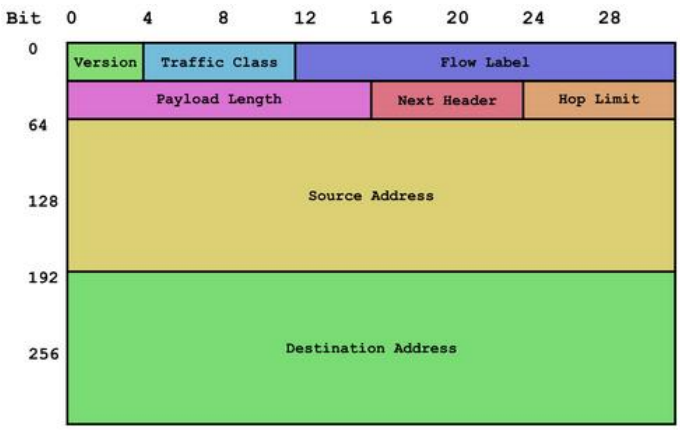
§1. IPv6 პროტოკოლი

IPv6 პროტოკოლი (Internet Protocol version 6) მოწყობილობათა დამისამართებისათვის იყენებს 128 ბიტიან ორობით სისტემას (მისამართს, ნახ. 2), შედეგად მისამართების რაოდენობა 2^{32} -დან (IPv4) გაზრდილია 2^{128} -მდე, რაც კოლოსალურ რიცხვს წარმოადგენს და ეს საშუალებას გვაძლევს თითქმის შეუზღუდავად იქნას გამოყენებული მისი მისამართები.



ნახ. 2. IPv6-ის მისამართის სტრუქტურა

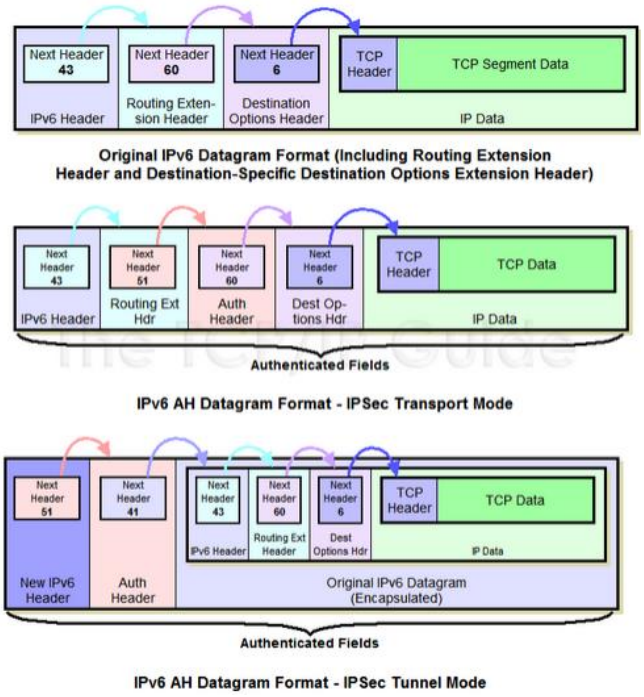
გარდა ამისა IPv6-ში განსაზღვრულია თავსართის ახალი ფორმატი (ნახ. 3). ახალი თავსართი ოპტიმიზირებულია არააუცილებელი და ოფციური ველების გაფართოებულ თავსართში გადატანით. ოპტიმიზირების შედეგად მიღებული IPv6 თავსართის დამუშავება დანიშნულებისაკენ მიმავალ გზაზე შუამავალ როუტერებზე მოითხოვს პროცესირების ნაკლებ 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 - დათვირთვის სიგრძე;
- Next Header - ახდენს რიგში შემდგომი თავსართის იდენტიფიკაციას;
- Hop Limit - იგივე TTL რაც IPv4 -ის შემთხვევაში;
- Source Address - მონაცემების გამგზავნის მისამართი;
- Destination Address - მონაცემების დანიშნულების მისამართი.



ნახ. 4. გაფართოებილი თავსართის ფორმატი

უნდა აღინიშნოს, რომ IPv6 -ში გარდა ჩვეულებრივი თავსართისა არსებობს მეორე ე.წ. გაფართოებული თავსართი. (ნახ. 4 -ზე ნაჩვენებია გაფართოებული თავსართის სამი მაგალითი.) მისი მოქმედების ზონა არის ინტერნეტის დონე, განთავსებულია ფიქსირებული თავსართს (თავსართი რომლის დეკაპუსლაცია არ ცდება) და TCP/IP სტეკის ზედა დონის პროტოკოლის თავსართებს შორის და ქმნის თავსართების ერთგვარ ჯაჭვს. მის ძირითად ფუნქციას წარმოადაგენს სხვადასხვა

პროტოკოლების მხარდაჭერა. 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

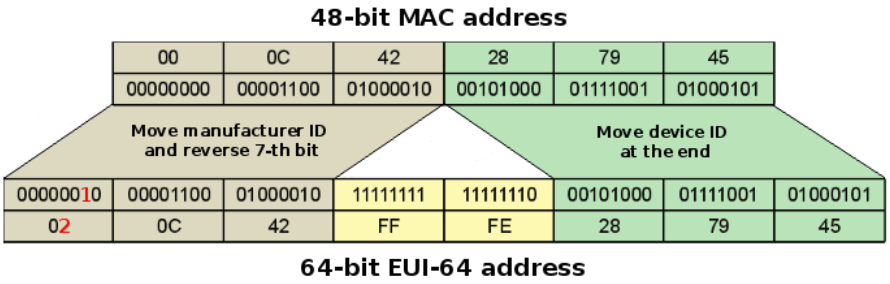
ქსელურ დონეზე ემატება პაკეტს) დაჯგუფებულია მსგავსი ფუნქციების მიხედვით სხვადასხვა თავსართებში და მათი პროცესიება (შემოწმება) ხდება იმის მიხედვით თუ რისი გაკეთებაა საჭირო შუამავალ მოწყობილობაზე (მაგალითად, გზის შერჩევა თუ აუთენთიკაციის). ინტერნეტ დონის ინფორმაციის გადანაწილება სხვადასხვა თავსართებში ამცირებს პაკეტის დამუშავების დროს და დატვითვას პროცესორზე.

შევნიშნოთ, რომ პროცესირების დროის შემცირება ერთის მხრივ კარგია, მაგრამ მეორეს მხრივ უსაფრთხოების თვალსაზრისით გაფართოებული თავსართი არ არის საკმარისად დაცული ჰაკერული შემოტევებისგან. 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 [15]), რომლის ანალოგი IPv4 ქსელში არ არსებობს. მოკლედ აღვწეროთ თითოეული მეთოდით IPv6 მისამართის დანიშვნის პროცესი.

- სტატიკური მეთოდ, რომელიც გულისხმობს მოწყობილობისათვის IPv6 მისამართის დანიშვნისათვის ქსელის ადმინისტრატორის აქტიურ ჩართულობას. ამ შემთხვევაში IPv6 მისამართების დუბლირების და სხვა კონფიგურაციაზე 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) 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): როგორც ვიცით MAC მისამართი შედგება 48 ბიტისაგან, რომელიც იყოფა ორ ტოლ ნაწილად (24-24 ბიტი) და მათ შორის იწერება 16 ბიტი შემდეგი ფიქსირებული ორობითი მნიშვნელობით 1111111111111110 (თექვსმეტობითი მნიშვნელობა FFFE). ამის შემდეგ, თუ მომხმარებლის ნაწილში მეშვიდე (მარცხნიდან) ბიტი აღმოჩნდა 0 -ის ტოლი მისი მნიშვნელობა შეიცვლება 1-ით, წინააღმდეგ შემთხვევაში, თუ 1 -ია შეიცვლება 0 -ით. ამ ფორმით მიღებული IPv6 მისამართი ენიჭება მოწყობილობას. ვინაიდან MAC მისამართი უნიკალურია ასევე უნიკალური იქნება EUI-64 მეთოდით მიღებული IPv6 მისამართი.



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.);

  შევნიშნოთ, რომ თუ ქსელში რამდენიმე სერვერია გამოყენებული, მაშინ თითოეული სერვერი DHCP solicit მოთხოვნას პასუხობს საკუთარი DHCP advertise შეტყობინებით. ამ შეტყობინებებს შორის განსხვავება შეიძლება არსებობდეს მხოლოდ IPv6 მისამართზე, კონფიგურაციის სხვა პარამეტრები ერთიდაიგივეა.
- **Request შეტყობინება**. DHCP client -ი DHCP advertise შეტყობინებას პასუხობს DHCP request შეტყობინებით (ეს შეტყობინებაც იგზავნება multicas მისამართზე), რომლითაც DHCP server -ს უდასტურებს მისთვის გამოყოფილი კონფიგურაციის პარამეტრების ნაკრებზე თანხმობას და ელოდება DHCP server -საგან დადასტურების მიღებას. (შევნიშნოთ, რომ რამდენიმე DHCP server -საგან DHCP advertise შეტყობინების შემთხვევაში DHCP client -ი პასუხობს მხოლოდ პირველად შემოსულ შეტყობინებას. სხვა სერვერები გამოყოფილ კონფიგურაციის პარამეტრებს აბრუნებენ საკუთარ წყებაში და ელოდებიან შემდეგ მოთხოვნას);
- **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.

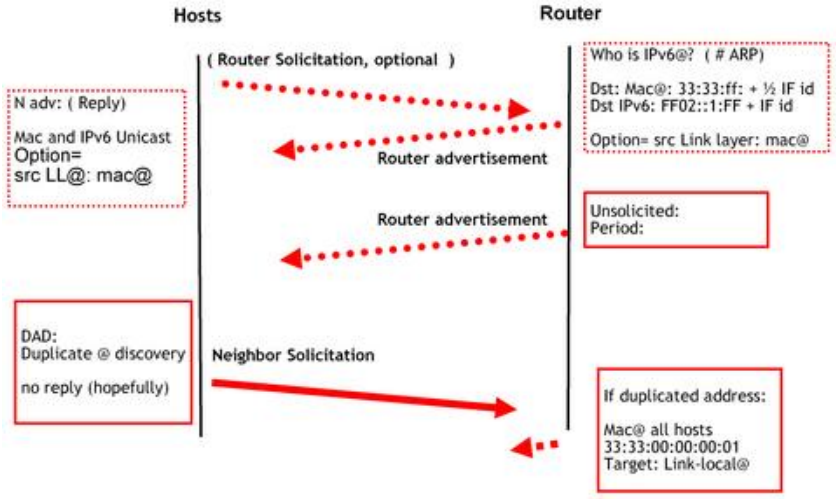
სანამ DHCP client -ი საბოლოოდ შეეცდებოდეს მიღებული კონფიგურაციის პარამეტრების გამოყენებას ის DAD პროტოკოლის გამოყენებით ამოწმებს კავშირს მისთვის გამოყოფილ IPv6 მისამართთან. თუ კავშირის შემოწმებას გამოხმაურება არ მოჰყვა DHCP client -ი იწყებს კონფიგურაციის პარამეტრების მეშვეობით კომუნიკაციას. წინააღმდეგ შემთხვევაში ის ცდილობს თავიდან გაიაროს ზემოთ აღწერილი პროცესი.

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. ამ შემთხვევაში ქსელს გარეთ კომუნიკაციისათვის DHCP სერვერის გამოყენების აუცილებლობა მაინც არსებობს, მაგალითად, DNS (Domain Name System) სერვერზე ინფორმაციის მისაღებად. ამ მეთოდის გამოყენებით IPv6 მისამართის მიღება ხდება შემდეგნაირად (ნახ. 7): ქსელში ჩართული მოწყობილობა ქსელში აგზავნის RS (router solicit) შეტყობინებას (შეტყობინება იგზავნება multicast მისამართზე), რომლითაც ცდილობს აღმოაჩინოს ქსელში გამოყენებული როუტერი.

[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

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 მისი საბოლოო დანიშვნამდე DAD პროტოკოლის გამოყენებით ამოწმებს კავშირს დაგენერირებულ მისამართთან იმ მიზნით, რომ გამოირიცხოს IPv6 მისამართის დუბლირება. თუ გაგზავნილ შეტყობინებაზე პასუხი არ მოვიდა ინიშნავს IPv6 მისამართს და იწყებს ქსელში კომუნიკაციას, წინააღმდეგ შემთხვევაში აგენერირებს ახალ IPv6 მისამართს.



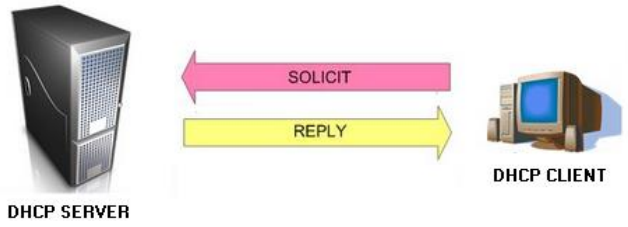
ნახ. 7. SLAAC მეთოდის გამოყენებით IPv6 მისამართის მიღების პროცესი

სამაგისტრო ნაშრომში შემოღებულია დამისამართების ახალი სქემა, რომელიც ეყრდობა IP პროტოკოლში არსებულ დამისამართების ორ მეთოდს: EUI-64 და DHCP. ამ მეთოდს პირობითად ვუწოდეთ DHCP-EUI-64. მისი გამოყენებით მოწყობილობა IPv6 მისამართის მიღებას შეძლებს შემდეგ ორი შეტყობინებით (ნახ. 8):

- **DHCP-EUI-64 Solicit შეტყობინება.** რომელიც იდენტურია DHCP პროტოკოლის გამოყენებისას შესაბამისი Solicit შეტყობინებისა იმ განსხვავებით, რომ ამ შემთხვევაში მოითხოვება პაკეტში (DHCP server -ში მისატანად) DHCP client -ის

MAC მისამართი[2]. ეს შეტყობინებაც DHCP Solicit შეტყობინების მსგავსად უნდა გაიგზავნოს multicast მისამართზე;

- **DHCP-EUI-64 Reply შეტყობინება.** DHCP server -ი მიღებული შეტყობინებიდან MAC მისამართის საფუძველზე EUI-64 მეთოდის გამოყენებით დააგენერირებს IPv6 მისამართს, Reply შეტყობინებით გაუგზავნის კონფიგურაციის აუცილებელ პარამეტრებს და გააკეთებს ჩანაწერს საკუთარ ბაზაში.
  შევნიშნოთ, რომ რამდენიმე DHCP server -ის შემთხვევაში მათი ბაზები უნდა იყვნენ ერთმანეთთან სინქრონიზირებული.



ნახ. 8. DHCP მეთოდით IPv6 მისამართის მიღების პროცესი

ბუნებრივად ისმის კითხვა:

1. რამდენად არსებობს მსგავსი მეთოდის შემოღების აუცილებლობა?
2. რა არის საჭირო მეთოდის რეალიზებისათვის?
3. რა უპირატესობებს იძლევა ის?

მცირე მოცულობის ქსელში ცხადია IPv6 მისამართების დინამიური მიღება და დუბლირებული მისამართების საკითხი პრობლემას არ წარმოადგენს, მაგრამ დიდი ზომის შემთხვევაში სულ სხვა სურათს ვღებულობთ. როგორც DHCP პროტოკოლის მუშაობის პრინციპის აღწერისას ვნახეთ მოწყობილობის მიერ კონფიგურაციის აუცილებელი პარამეტრად მისაღებად საჭიროა 4 შეტყობინების გადაგზავნა სერვერსა და კლიენტს შორის. შეტყობინებებიდან 3 (ან 2) multicast -ი, ხოლო 1 (ან 2) unicast შეტყობინებაა. ასევე, ქსელში იგზავნება ერთი multicast გადაცემა DAD პროტოკოლის

[2] ამის უზრუნველყოფა შესაძლებელია რეზერვირებული ველების ან იმ ველების ხარჯზე, რომლებიც ივსება შესაბამისი მნიშვნელობებით პაკეტის მინიმალურ ზომამდე შესავსებად.

მიერ[3]. DHCP server -ზე ხშირი მიმართვის შემთხვევაში პაკეტების მოცულობამ შეიძლება საგრძნობი ზეგავლენა იქონიოს ქსელის გამტარუნარიანობაზე.

DHCP-EUI-64 მეთოდით დამისამართების შემოღების შემთხვევაში, ერთის მხრივ, აუცილებელი კონფიგურაციის პარამეტრების მისაღებად საკმარისი იქნება მხოლოდ ორი multicast შეტყობინება DHCP server -სა და DHCP client -ს შორის. ამ შემთხვევაში DAD პროტოკოლის გამოყენების აუცილებლობა არ არსებობს ვინაიდან მისამართის დუბლირების შემოწმება პირდაპირ ეკისრება DHCP server -ს, რომელიც ამის უზრუნველყოფას შეძლებს ბაზის ჩანაწერის უნიკალურობის შენარჩუნებას MAC მისამართებზე დაყრდნობით. მეორეს მხრივ, მეზობელი მოწყობილობის აღმოსაჩენად, ჩვეულებრივ შემთხვევაში, NDP პროტოკოლის გამოყენებით საჭიროა ერთი multicast და ერთი unicast შეტყობინების გადაცემა. ჩვენს შემთხვევაში კი საკმარისი იქნება ორი unicast შეტყობინება DHCP server -სა და DHCP client -ს შორის. კერძოდ, მეზობლის აღმოსაჩენად DHCP client -ი DHCP server -თან გააგზავნის შესაბამის მოთხოვნას მეზობელი მოწყობილობის IPv6 მისამართით. DHCP server -ი პასუხობს შესაბამის მოთხოვნას და DHCP client -ს უგზავნის მეზობელი მოწყობილობის MAC მისამართს, თუ DHCP client -ზე ჩანაწერი არსებობს DHCP server -ის ბაზაში. ეს იქნება მოწყობილობის ერთგვარი აუთენთიკაცია.

DHCP-EUI-64 მეთოდის რეალიზაციისათვის საჭიროა რამდენიმე მოთხოვნის დაკმაყოფილება:

- პაკეტის სტრუქტურა
    - DHCP-EUI-64 მეთოდის გამოყენებით IPv6 მისამართის მისაღებად პაკეტში საჭიროა MAC მისამართის ჩასაწერად ველის გამოყოფა;
    - მეზობელი მოწყობილობის აღმოჩენისას შესაბამის მოთხოვნაზე საპასუხო პაკეტში საჭიროა MAC მისამართის ჩასაწერად ველის გამოყოფა;
- DHCP server -ზე

[3] შეტყობინება ეგზავნება იმ 2^{16} მისამართს, რომლის ბოლო 16 ბიტის ემთხვევა IPv6 მისამართის შესაბამის ნაწილს

- რამდენიმე DHCP server -ის არსებობის შემთხვევაში საჭიროა ბაზის სინქრონიზაცია;
- უნდა არსებობდეს EUI-64 მეთოდით IPv6 მისამართის დაგენერირების მექანიზმი;
- IPv6 და MAC მისამართით ბაზაში ძებნის შესაძლებლობა;

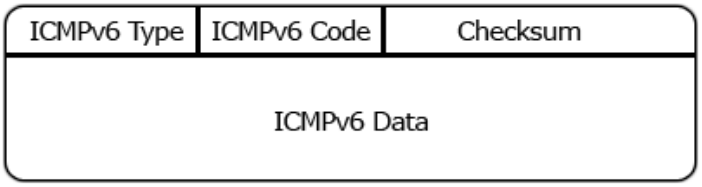
- DHCP client -ზე
  - IPv6 მისამართიდან link-local მისამართის მიღების შესაძლებლობა.

DHCP-EUI-64 მეთოდის გამოყენებით მიღებული უპირატესობა მდგომარეობს იმაში, რომ ქსელში შემცირებულია აუცილებელი კონფიგურაციის პაკეტების შემცირებული მოცულობა, მეზობლის გაადვილებულებული აღმოჩენა და ა.შ.

§2. IPv6 ქსელში კომუნიკაციისათვის აუცილებელი პროტოკოლები

IPv6 ქსელში კომუნიკაციისათვის არსებობს რამდენიმე მნიშვნელოვანი პროტოკოლი რომლის გარეშე თითქმის შეუძლებელი იქნებოდა ჩვენთვის საჭირო მოქმედებების შესრულება ან რაც მთავარია, ქსელში კომუნიკაციის დაწყება. ასეთი პროტოკოლები დიდ და საპასუხისმგებლო როლს ასრულებენ თანამედროვე ტექნოლოგიებში.

ასეთი პროტოკოლების სიის ჩამონათვალში ერთ-ერთი პირველი ადგილი უკავია, ICMPv6 (Internet Control Message Protocol version 6), მისი ძირითადი დანიშნულებაა გვაცნობოს იმ შეცდომების შესახებ რომელიც პაკეტების დამუშავების პროცესში ხდება და ასევე მას შეთავსებული აქვს სხვა რიგი ფუნქციებიც, მაგალითად, დიაგნოსტიკა (ICMPv6 "ping"). ICMPv6 წარმოადგენს IPv6 ქსელის საბაზისო პროტოკოლს, ამიტომ მისი რეალიზაცია უნდა მოხდეს ქსელის ნებისმიერ მონაკვეთში. ყოველი ICMPv6 პაკეტის გაგზავნა წინ უძღვის IPv6 თავსართს, მისი მნიშვნელობა არის ან ნული ან შეიცავს IPv6-ის გაფართოებულ თავსართს და მისი ყოველი ახალი თავსართი იდენტიფიცირდება ნომრით 58.



ნახ. 9. ICMPv6 პაკეტის ფორმატი

შესაძლებელია ICMPv6 პროტოკოლის ძირითად ფუნქციების სიის სახით წარმოადგენა:

- Neighbor Discovery Protocol (NDP), Neighbor Advertisements (NA) და Neighbor Solicitations (NS) - IPv6 ქსელისათვის ანხორციელებს ისეთ ფუნქციებს როგორსაც IPv4 ქსელში ARP პროტოკოლი;
- Router Advertisements (RA) და Router Solicitations (RS) - ეხმარება კვანძს საკუთარ ქსელში აღმოაჩინოს საკუთარ ქსელზე ინფორმაცია, როგორიცაა ქსელის პრეფიქსი, default gateway და სხვა ინფორმაცია, რომელიც ქსელში კომუნიკაციისათვის დამხმარე;

- Echo Request და Echo Reply - გამოიყენება Ping6 უტილიტის მხარდაჭერისათვის;
- PMTUD განსაზღვრავს კომუნიკაციისათვის შესაბამის MTU-ს;
- Multicast Listener Discovery (MLD) - ანხორციელებს IGMP-მსგავს ფუნქციონალურობას IP multicast კომუტირებისას ჯგუფში გაწევრიანებას და მის დატოვებას;
- Multicast Router Discovery (MRD) - გამოიყენება multicast როუტერების აღმოსაჩენად.
- Node Information Query (NIQ) shares information about nodes between nodes.
- Secure Neighbor Discovery (SEND) - გამოიყენება მეზობელ კვანძებს შორის მონაცემთა უსაფრთხო გადაცემისათვის;
- Mobile IPv6 - გამოიყენება მობილური კომუნიკაციისათვის.

შემდეგი მნიშვნელოვანი პროტოკოლი არის NDP (Neighbor Discovery Protocol), მისი მიზანია IPv6 ქსელში მეზობელი კვანძის (კომპიუტერის) ან როუტერის აღმოჩენა. მეზობელი კვანძის აღმოჩენის მიზნით წყარო multicast მისამართზე აგზავნის NS შეტყობინებას. ქსელში შესაბამისი კვანძის არსებობის შემთხვევაში წყაროს უბრუნდება NA შეტყობინება დანიშნულების კვანძის მიერ გამოგზავნილი unicast მისამართით.

ND პროცესი მოიცავს შემდეგ ფუნქციებს:

- router discovery - იმ როუტერის აღმოჩენა, რომელიც ლოკალურ ქსელს უკავშირდება;
- prefix discovery - ლოკალური ქსელის პრეფიქსის აღმოჩენა;
- parameter discovery - კომუნიკაციისათვის საჭირო სხვადასხვა პარამეტრების აღმოჩენა. მაგალითად, როგორიცაა ორ ინტერფეისს შორის გადასაცემი მონაცემის მოცულობა;
- address autoconfiguration – IPv6 მისამართის დინამიური მიღება;
- address resolution - მეზობელი კვანძის link-local მისამართის აღმოჩენა;
- next-hop determination - მეზობელი კვანძის აღმოჩენა, რომლისთვისაც პაკეტი არის დანიშნული;

MLD (Multicast Listener Discovery) პროტოკოლი IPv6 ქსელისათვის წარმოადგენს IPv4 ქსელისათვის წარმოადგენს IGMP პროტოკოლის ანალოგს. MLD განსაზღვრავს შეტყობინებათა ნაკრებს, რომელიც იცვლება როუტერსა და ჰოსტებს შორის და როუტერს საშუალებას აძლევს აღმოაჩინოს multicast მისამართების ჯგუფი, რომელთაგან ერთერთ ინტერფეისზე არსებობს ერთი მაინც „მსმენელი“ კვანძი, უზრუნველყოფს მომხმარებელთა შესაბამის ჯგუფებში გაერთიანებასა და იქიდან გამოყოფის შესაძლებლობას. ამასთან, ერთი მრავალთან კომუნიკაციის ინიციატორი შეიძლება იყოს ცალკეული მომხმარებელი.

DAD (Duplicate Address Detection) პროტოკოლის ძირითადი დანიშნულებაა დუბლირებული IP მისამართების აღმოჩენა. მის გარეშე დიდი ალბათობაა იმის, რომ ქსელის ადმინსტრატორის უნებლიე შეცდომით ან DHCP პროტოკოლის მიერ დაშვებული შეცდომით ორ ან რამდენიმე ჰოსტ მიენიჭოს ერთი და იმავე IP მისამართ. მსგავსი შემთხვევა დაარღვევს იმ ძირითად პირობას, რომ ქსელში არ უნდა არსებობდეს ორი მსგავსი IP მისამართი. შედეგად კი მივიღებთ IP მისამართების კონფლიქტს და შეუძლებელი გახდება კომუნიკაცია.

თავი II. IPv6 ქსელზე შემოტევის ტიპები

§1. ინფორმაციის უსაფრთხოების კატეგორიები

ინფორმაციის უსაფრთხოება და მისი ტექნოლოგიები დროთა განმავლობაში ვითარდებოდა. მისმა განვითარებამ მიგვიყვანა იქამდე, რომ ინფორმაცია მეტნაკლებად დაცულია. საწუხაროდ ინფორმაციის სრული დაცვა ვერ ხერხდება, რადგან ყოველთვის შეიძლება მოიძებნოს ისეთი საშუალება, რომლის გვერდის ავლით შესაძლებელია ნებისმიერი წინაღობის გადალახვა.

ინფორმაციის უსაფრთხოების არსებობს რამდენიმე კატეგორია.

- **ფიზიკური უსაფრთხოება** - წარმოადგენს ყველაზე ადრეულ უსაფრთხოების კატეგორიას. მის მაგალითად შეიძლება განვიხილოთ წერილი ან ობიექტი, რომელსაც იცავს მცველი;
- **კომუნიკაციის უსაფრთხოება** - იმ შემთხვევაში, თუ ფიზიკური უსაფრთხოება ვერ უზრუნველყოფდა ინფორმაციის დაცვას უნდა შექმნილიყო მექანიზმი, რომელიც ამას შეძლებდა. ამიტომ გამოიგონეს ინფორმაციის შიფრაციის მექანიზმი. მისი ერთ-ერთი პირველი მაგალითია ე.წ ცეზარის შიფრი;
- **ემისიური უსაფრთხოება** - ნებისმიერი ელექტრონული მოწყობილობა, იქნება ეს სატელეფონო კაბელი თუ ტელეფონი, ქმნის ელექტრულ ველს. აღმოჩნდა, რომ მიუხედავად იმისა, ინფორმაცია დაშიფრულია თუ არა, შესაბამისი ტექნიკური საშუალებებით აღჭურვილ გარეშე პირს შეუძლია ელექტრული ველისგან მიიღოს და გაშიფროს ინფორმაცია. სწორედ, ამიტომ ა.შ.შ -ში შეიქმნა სტანდარტი სახელად TEMPEST, რომელიც ახდენს ამ პრობლემის დეტექციას და პრევენციას;
- **კომპიუტერის უსაფრთხოება** - კომპიუტერის უსაფრთხოება ერთ-ერთი მნიშვნელოვანი საკითხია რადგან სწორედ კომპიუტერში ინახება თითქმის ყველა პერსონალური მონაცემი და ინფორმაცია, რომელზეც წვდომა გარეშე პირისათვის უნდა იქნას შეზღუდული. სტანდარტულად კომპიუტერის უსაფრთხოებისთვის საჭიროა: ლიცენზირებილი ოპერაციული სისტემა და პროგრამები, ანტივირუსი, პროგრამების განახლებები და რთული პაროლები.

ასევე არსებობს დამატებითი პროგრამული საშუალებები, რომლებიც გვიცავენ ინფორმაციის გადინებისგან;

- **ქსელის უსაფრთხოება** - ქსელის უსაფრთხოება შედგება დებულებების და პოლიტიკებისგან, რომლებიც მიღებულია ქსელის ადმინისტრატორს მიერ რათა, თავიდან აცილებული იქნას და განხორციელდეს მონიტორინგი არასანქცირებული წვდომაზე, კომპიუტერული და ქსელური მოწყობილობების კონფიგურაციის შეცვლაზე. ქსელის უსაფრთხოება მოიცავს ავტორიზაციის მისაწვდომობას მონაცემებზე და ქსელზე, რომელსაც აკონტროლებს ქსელის ადმინისტრატორი;
- **ინფორმაციის უსაფრთხოება** - ინფორმაციის უსაფრთხოება მოიცავს ყველა ზემოთ ჩამოთვლილ კატეგორიების კომპლექსურ და მიზანმიმართულ გამოყენებას.

§2. IPv6 ქსელის უსაფრთხოებასთან დაკავშირებული საკითხები.

მიუხედავად იმისა რომ ქსელის ინფრასტრუქტურაში უკვე გამოჩნდა IPv6 პროტოკოლის მხარდაჭერა, მისი უსაფრთხოების პრობლემები ჯერ კიდევ აქტუალურია. ძირითადად გამოიყოფა რისკის 5 ტიპი, რომელიც დაკავშირებულია IPv6 ქსელთან. ესენია:

1. IPv6 უსაფრთხოებასთან დაკავშირებული განათლების და ტრენინგების ნაკლებობა. № 1 რისკად ითვლება იმ ცოდნის ნაკლებობა, რომელიც საჭიროა IPv6 უსაფრთხოებისთვის. მიუხედავად იმასა, თუ რამდენად თანამედროვე ტექნიკას და ტექნოლოგიებს ვიყენებთ ქსელის აგებისას, ძირითად ფიგურად მაინც ადამიანი რჩება, რადგან სწორედ მან უნდა შექმნას ის კონფიგურაცია, რომელიც საჭიროა ქსელის გამართული მუშაობისთვის. ამიტომაც აუცილებელია მუდმივად ქსელის ადმინისტრატორების ცოდნის განახლება, კვალიფიკაციის ამაღლება და ტრენინგები.
2. არაფილტრირებული IPv6 პაკეტების და ტუნელური ტრაფიკის უსაფრთხოება -კონცეპტუალურად არსებობს ორი მეთოდი, ესენია:

    - საეჭვო IPv6 პაკეტების აღმოჩენა;
    - მათზე კონტროლის დამყარება.

    თუმცა პრაქტიკაში ამის განხორციელება საკმაოდ რთულია. არსებობს 16 სხვადასხვა ტუნელი და რამდენიმე გადასვლის მეთოდი, თუ არ ჩავთვლით ზედა დონის ტუნელებს ისეთი როგორიცაა SSH, IPv4-IPSec, SSL / TLS და DNS.
3. ინტერნეტ პროვაიდერების მხარეს IPv6 მხარდაჭერის არ არსებობა. საფუძვლიანი ტესტირება არის აუცილებელი სანამ IPv6 უსაფრთხოება ფუნქციონალურ და სტაბილურ მუშაობაზე გადავა. მსგავსი ტესტირებები უფრო რთულია პროვაიდერების მიერ, რადგან მათ გააჩნიათ დიდ რაოდენობის მოწყობილობები. სწორედ ამიტომ ინტერნეტ პროვაიდერები უმეტეს შემთხვევაში ჯერჯერობით ერიდებიან სრულად IPv6 -ზე გადასვლას, რადგან ეს დიდ ფინანსებთან და რესურსებთან არის დაკავშირებული.

4. უსაფრთხოების პოლიტიკის შეთანხმება IPv4-სა და IPv6-შორის. სუსტი IPv6 უსაფრთხოების პოლიტიკის პირდაპირი შედეგია ის მიმდინარე დეფიციტი, რომელიც დაკავშირებულია IPv6 უსაფრთხოების ცოდნასთან. უნდა აღინიშნოს რომ, IPv6 უსაფრთხოების პოლიტიკა უნდა იყოს თანაბარი IPv4 -თან, მაგრამ ის, ფართოდ მოიცავდეს ახალი ხარვეზებს, და არ უნდა იყოს განხილული ეს ხარვეზები IPv4-ის ერთგვაროვანი გარემოში.
5. ხარვეზები ახალ კოდში. IPv6 პროტოკოლის უსაფრთხოებასთან დაკავშირებული პრობლემები ძირითადად მოიცავს ხარვეზებს პროტოკოლის ახალ ვერსიაში. სწორედ პროტოკოლში არსებული „ხვრელებია“ ჰაკერული შეტევების და უსაფრთხოების დარღვევის მიზეზები.

§3. გლობალური ქსელიდან მომავალი საფრთხეები.

როგორც ვიცით გლობალური ქსელი (WAN) ლოკალული ქსელისგან (LAN) განსხვავდება იმითი, რომ მასზე მიერთებული მომხმარებლების რაოდენობა არის შეუზღუდავი და მონაცემების გადაცემის სიჩქარე ბევრად უფრო დიდია ვიდრე ლოკალურ ქსელში. თანამედროვე ინტერნეტში ერთმანეთის გვერდიგვერდ ფუნქციონირებს ერთმანეთისაგან დამოუკიდებელი IPv4 და IPv6 ინტერნეტ პროტოკოლები. ერთი ქსელის კვანძებს არ შეუძლიათ მიიღონ სხვა ქსელის სერვისების მომსახურება. რადგანაც IPv4 და IPv6 პროტოკოლებს გააჩნიათ განსხვავებული სტრუქტურა და იყენებენ განსხვავებულ მეთოდებს, ამიტომ ერთი პროტოკოლისათვის საფრთხის შემცველი კოდის ფრაგმენტი შეიძლება მეორე პროტოკოლის მიერ არ იქნას აღქმული საფრთხის შემცველად. ე.წ. ფრაგმენტაციული შეტევა წარმოადგენს იმ ყველაზე თვალსაჩინო მაგალითს, თუ რა სახის შეტევა შეიძლება განხორციელდეს გლობალური ქსელიდან ლოკალურ ქსელზე, მისი ძირითადი არსი მდგომარეობს შემდეგში: ცალკეული ფრაგმენტირებული პაკეტები რომლებიც ინკაპსულირებული არიან ფრეიმებში საფრთხეს არ წარმოადგენს და ფაირვოლი მას არ განიხილავს როგორც პოტენციურ საფრთხეს, მაგრამ მისი დეკაპსულაციის დროს ხდება იმ საზიანო კოდის აღდგენა რომელიც წარმოადგენს შემტევს, შედეგად კი ვიღებთ, დავირუსებულ სისტემას, მოპარულ მონაცემებს და ა.შ.

IPv4-სთვის ცნობილმა საფრთხეებმა განიცადეს გარკვეული განახლება IPv6 ქსელისათვის. ასეთი საფრთხეების რიცხვს მიეკუთვნება ე.წ. Packet-flooding, DoS, DDoS, malware, worm და ა.შ.

§4. IPv6 პროტოკოლის მიერ გამოყენებული პროტოკოლების სუსტი მხარეები

იმის გათვალისწინებით, რომ ICMPv6 პროტოკოლი ერთ-ერთი მნიშვნელოვანი პროტოკოლია IPv6 ქსელში და ფუნქციონალურად დატვირთულია, ამიტომ ბუნებრივია ის წარმოადგენდეს ე.წ. hacker-ების სამიზნეს. როგორც ზემოთ აღვნიშნეთ, ICMPv6 პროტოკოლს საკუთარი ფუნქციების რეალიზებისათვის იყენებს NDP პროტოკოლი. IPv6 კვანძის მიერ დინამიურად IPv6 მისამართის მისაღებად, ქსელის პრეფიქსის მისაღებად, მეზობელი კვანძის აღმოსაჩენად და სხვა მოქმედებების განსახორციელებლად ქსელში გადაცემული პაკეტი შეიძლება მოსმენილი იქნას გარეშე (არაკეთილმოსურნე) კვანძის მიერ, რომელსაც შეუძლია მონაცემების ფალსიფიცირება. ფალსიფიცირებული მონაცემები შეიძლება გამოყენებული იქნას ლეგალური კვანძის მიერ, რომელიც უნებლიედ აღმოჩნდება ინფორმაციის გადინების წყარო. Multicast კომუნიკაციისას შესაბამის ჯგუფში გაწევრიანებულ გარეშე კვანძს შეუძლია ფალსიფიცირებული ინფორმაციის გადაცემა, რომელსაც მიიღებს ჯგუფში გაწევრიანებული ყველა კვანძი.

ასევე შესაძლებელია შეტევის ვექტორი მიმართული იყოს სისტემის მწყობრიდან გამოყვანაზე. დიდი რაოდენობის უცნობი პაკეტების გენერირების ან დიდ მოცულობის პაკეტების დამუშავების დროს ქსელური მოწყობილობა ვალდებულია დაამუშავოს ყველა მოთხოვნა, რაც თავისთავად ნიშნავს მათი პროცესირების დროის გახანგრძლივებას. ყოველ დაფიქსირებულ შეცდომაზე ICMPv6 მოითხოვს პასუხს, შედეგად კი ვიღებთ ხელოვნურად გაზრდილ სამუშაობის მოცულობას. მსგავსი დატვირთვა პირდაპირ დარტყმას აყენებს ქსელური მოწყობილობის პროცესორის მუშაობაზე და ანელებს მის წარმადობას ან და ყველაზე უარეს შემთხვევაში გამოიწვევს მის გათიშვას. კარგი სიახლე არის ის, რომ თანამედროვე მარშუტიზატორებზე შესაძლებელია ICMPv6 შეცდომების შეტყობინებების გენერირების მართვა, უფრო ზუსტად კი იმ სიჩქარის კონტროლირება რომლითაც ხდება ამ შეტყობინებების შექმნა. მექანიზმი კი მდგომარეობს შემდეგში: მარშუტიზატორებზე, ICMPv6 შეცდომების შეტყობინების მართვა შესაძლებელია ბრძანებით ipv6 icmp error-interval, ინტერვალი განისაზღვრება

მილიწამებში. ამ საშუალებით ქსელის ადმისტრატორს მარტივად შეუძლია ICMPv6 შეტყობინებების ხელით მართვა, რაც გამორიცხავს ზედმეტი პაკეტების შექმნას.

ვინაიდან პროტოკოლის სპეციფიურობა არ ზღუდავს დამატებითი თავსართების გამოყენებას, ამიტომ ისინი შეიძლება იყვნენ IPv6 ქსელისათვის პოტენციური საფრთხის შემცველი. ოპტიმიზირებული თავსართის გამოყენება ამცირებს დანიშნულების გზაზე არსებულ შუამავალ როუტერებზე პროცესირების დროს, არ მოწმდება ყველა გაფართოებული თავსართი. ამ შემთხვევაში „შიდა“ თავსართი, რომელიც არ მოწმდება შუამავალ როუტერზე შეიძლება იყოს საზიანო ინფორმაციის მატარებელი. ასეთმა პაკეტმა შეიძლება გამოიწვიოს დანიშნულების სისტემაზე ან მისკენ მიმავალი გზაზე არსებულ მოწყობილობებზე DoS შემოტევა. დაზიანებულმა პაკეტმა შეიძლება გადაკვეთოს მთლიანი ქსელი ყოველგვარი პრობლემის გარეშე. თავსართები შეიძლება გამოყენებული იქნან firewalls-ისა და IPS-ის (Intrusion prevention systems) გვერდის ავლის მიზნით.

§5. IPv4 და IPv6 პროტოკოლების ყოფაქცევა უსაფრთხოების საკითხებში

TCP/IP პროტოკოლთა სტეკის განხილვისას IPv4 და IPv6 -ს შორის განსხვავება არსებობს მხოლოდ ინტერნეტის დონეზე. რადგანაც IP პროტოკოლი ურთიერთქმედებს ზედა და ქვედა დონის სხვადასხვა პროტოკოლებთან, ამიტომ ამ შემთხვევაში განსხვავება IPv4-სა და IPv6-ს შორის ვერ იქნება. ამის გამო შემოტევები, რომლებიც ორივე პროტოკოლის მიმართ თანაბრად შეიძლება იქნას რეალიზებული შემდეგია:

- გამოყენებითი დონეზე;
- არაავტორიზირებული;
- Man-in-the-middle attacks;
- Sniffing/eavesdropping;
- DoS;
- Spoofed packets;
- შემოტევა როუტერებზე და სხვა ქსელურ მოწყობილობებზე;
- შემოტევა ფიზიკურ და data link დონეზე.

IPv6 პროტოკოლი დიდად განსხვავდება IPv4-სგან, ამიტომ მასში თავს იჩენს ახალახალი საფრთხეები, რომელთა ანალოგი IPv4 -ში არ გაგვაჩნია. ესენია:

- ლოკალური ბაზური შეტევები (შეტევები NDP პროტოკოლებზე);
- შეტევა DHCPv6 -ზე;
- DOS შეტევა როუტერებზე;
- ფრაგმენტაციის ბოროტად გამოყენება (IPv4 -ში ხდება სრული ფრაგმენტაცია, ხოლო IPv6 -ში გაფართოებული თავსართების);
- პაკეტების გაძლიერებული შეტევა.

IPv6 -ში აღმოფხვრილია IPv4 -თვის დამახასიათებელი საფრთხეები, მაგრამ მისი მოცულობის გამო, ზოგიერთი პროტოკოლის უსაფრთხოების ხარისხი დიდად არ განხვავდება IPv4-ზე მომუშავე პროტოკოლებისგან, რაც არსებით პრობლემებეს ქმნის.

IPv6 პროგრესირებადი პროტოკოლია, რაც საშუალებას გვაძლევს ჩვენ თვითონ შევქმნათ უსაფრთხოების სტანდარტები. IPv6 თავსართში არსებული ველი არის უნიკალური, შესაბამისად შეგვიძლია მასზე მივაბად გაფართოებული თავსართი, რომელიც სწორედ დამატებითი უსაფრთხოებისთვის იქნება განკუთვნილი, მაგრამ ეს იმას არ ნიშნავს რომ არ იქნება შეტევები მასზე ან არ მოიძებნება მეთოდი ან საშულება რომლის დახმარებითაც მესამე პირი შეძლებს მისით მანიპულირებას.

არსებობს IPv6-თვის დამახასიათებელი საფრთხეები, რომლებიც IPv4 -ში არ გვხვდება. ესენია:

- ე.წ მატლების დაყოფა და სკანირება - მათი აღმოჩენა ძალიან რთულია;
- შეტევა ICMPv6 - IPv6-ის ერთ-ერთი სუსტი წერტილი, რადგან როგორც ავღნიშნეთ იგი აუცლილებელი კომპინენტია პროტოკოლებს შორის კომუნიკაციისთვის;
- გაფართოებულ თავსართებზე შეტევა.
- ავტოკონფიგურაცია - შეტევა NDP პროტოკოლზ;
- ტრანზაქციის მექანიზმებზე შეტევა.
- IPv6 მობილურ ქსელზე შეტევა.
- IPv6 პროტოკოლის სტეკზე შეტევა.

საერთო ჯამში შეგვიძლია ვთქვათ რომ, IPv6 პროტოკოლს აქვს ის უნიკალური თავისებურებები, რომლებიც მას ხდის შედარებით უფრო უსაფრთხოს მონაცემთა გადაცემისთვის, ვიდრე IPv4 -ია.

თავი III. IPv6 ქსელზე, შემოტევის აღმოჩენა და დაცვის მექანიზმები

§1. სხვადასხვა ტიპის საფრთხეების აღმოჩენის მეთოდები და მათგან, დაცვის მექანიზმები

ინფორმარციის უსაფრთხოება, განსაკუთრებით კი ქსელის უსაფრთხოება ძალიან მნიშვნელოვანია თანამედროვე კომპიუტერულ სისტემებში რადგან სწორედ იგი წარმოადგენს შეტევების პირველ ხაზს, ამიტომ მისი დაცულობა იძლება იმას გარანტს, რომ არასაქცირებული შესვლა სისტემაში ან ძალიან გაძნელებულია ან შეუძლებელი.

უსაფრთოხება უნდა განიხილებოდეს არა როგორც რაიმე პროდუქტი არამედ როგორც პროცესი, რომელიც უზრუნველყოფს ქსელის ან სისტემის უსაფრთხოებას. სამწუხაროდ თანამედროვე პროგრამული უზრუნველყოფების თუ ფიზიკური მოწყობილობების მწარმოებლები ცდილობენ შექმნან პროდუქტი, რომელიც იქნება უნიკალური და შეძლებს წინააღმდეგობა გაუწიოს შეტევებს, მაგრამ ასეთი პროდუქტის შექმნა ფაქტიურად შეუძლებელია. სისტემის დაცვა უნდა იყოს კომპლექსური და უნდა შედგებოდეს ისეთი მექანიზმებისგან როგორიცაა: ანტივირუსები, დაშვების სიები, ფაირვოლები, სმარტ-ბარათები, ბიომეტრიკა.

ყველაზე დიდ პრობლემა და საპასუხისმგებლოა საშიშროების აღმოჩენა იქამდე ვიდრე ის ზიანს მომტანი გახდება. შემოტევების პრევენციას ახდენს ე.წ. შემოტევის აღმოჩენის სისტემები (intrusion detection system (IDS)), მსგავსი დაცვის მექანიზმები გვაძლევს დამატებითი უსაფრთხოების, საშუალებას. მათი ძირითადი მიზანი არის გარკვეულის საფრთხის შემცველი აქტივობებისგან თავის დაცვა. როგორც წესი IDS მოიცავს შემდეგ ოპციებს :

- სენსორული ქვესისტემა, რომელიც განკუთვნილია ავტომატურ რეჟიმში მონაცემების შეგროვებისთვის;
- ანალიზის ქვესისტემა განკუთვლინია იმ მონაცემების ანალიზისთვის, რომელსაც აგროვებს სენსორული ქვესისტემა;

- საცავი - მასში ინახება ანალიზის დროს დამუშავებული მონაცემები;
- მართვის კონსოლი, რომელიც საშუალებას გვაძლევს ვმართოთ IDS სისტემები.

მიუხედავად იმისა რომ ავტომატიზირებილი სისტემა თავიდან გვარიდებს დიდ ფიზიკურ თუ გონებრივ შრომას იგი მაინც არ წარმოადგენს იმ უნიკალურ საშუალებას, რომლის გამოყენებით სრულად შესაძლებელია თავის დაცვა შემოტევებისგან. ასევე უნდა უნდა ითქვას ისიც, რომ მსგავს სისტემაზე მთლიანად დაყრდნობა და მისი ინტენსიურად გამოყენებამ შეიძლება ცალკეული პრობლემები გაგვიჩინოს, მაგალითად, შეცდომა ანალიზის დროს, რომელიც შეზღუდავს დაშვებული ტრაფიკს გატარებას.

ყველაფერი ამის გათვალისწინებით საჭიროა გქვონდეს იმის ცოდნა და საშუალება, რომ ცალკეული შემოტევები აღმოვაჩინოთ და მოვახდინოთ მათი იზოლირება. ამიტომაც განვიხილავთ იმ ძირითადი შემოტევების ტიპებს, რომლებიც საფრთხეს უქმნის, როგორც ქსელის სტაბილურ მუშაობას ასევე, სისტემის უსაფრთხოებას.

Snooping -ი, მისი მიზანია შემოტების დროს იპოვოს რაიმე საინტერესო ფაილი ან მონაცემი. მოქმედების ტაქტიკა მდგომარეობს შემდგომში: ის სათითაოდ ხსნის და კითხულობს ფაილებს სანამ არ იპოვის მისთვის საჭირო ინფორმაციას. მისგან თავის დასაცავად საჭიროა სერვერზე არ კომპიუტერზე გვეყენოს სპეციალური პროგრამული უზრუნველყოფა (მაგალითად, Xarp გამოიყენება arp პროტოკოლის Snooping -ის აღმოჩენის დროს), რომელიც აღმოაჩენს აქტიურობას სისტემაში, და გვაცნობებს მის შესახებ ან ავტომატურ რეჟიმში მოადხენს მისგან თავის დაცვას.

Man-in-the-middle attacks - შეიძლება არც განვიხილოთ შეტევების კატეგორიაში რადგან იგი პირდაპირ ზემოქმედაბას არ ახდენს სისტემის მუშაობაზე. მისი ძირითადი მიზანი არის კომუნიკაციის არხის დუბლირება და მიმოწერის ან მონაცემების კითხვა. ასევე, კოპირებული ფაილების სხვა მისამართზე გადაგზავნა. მისგან თავის დასაცავად ყველაზე მარტივი საშუალებაა მონაცემების დაშიფრვა (დახურული (private) გასაღებით). რადგან, კომუნიკაციაში არასანქცირებულად წვდომის შემთხვევაშიც ინფორმაცია გარეშე პირისთვის იყოს გაუგებარი. ასევე შესაძლებელია ისეთი პროგრამული უზრუნველყოფის და პროტოკოლების,

გამოყენება როგოროცაა Ipsec (Internet Protocol Security), PPTP (Point-to-Point Tunneling Protocol) და ა.შ

Denial-of-service attack (DOS) - ყველაზე გავრცელებული შეტევა კომპიუტერულ სისტემებში. მისი მიზანია მთლიანი სისტემის მუშაობის მწყობრიდან გამოყვანა. იგი ამისთვის იყენებს კოლოსალური რაოდენობის პაკეტებს, რომლებიც მიმართულია კონკრეტული სისტემისკენ, მაგალითად, web-გვერდი ან მონაცემების საცავი და ა.შ. იმის გათვალისწინებით, რომ ყოველი ქსელური მოწყობილობა შეზღუდულია მონაცემების პროცესირებისას, DOS შეტევის დროს იგი ვეღარ ახერხებს ყოველ მოთხოვნაზე რეაგირებას, ხდება პროცესორის გადატვირთვა და შედეგად ვიღებთ უსარგებლო მოწყობილობას, რომელიც უბრალოდ ვეღარ ამუშავებს ინფორმაციას და ვეღარ აწვდის სერვისს მომხმარებლებს.

DOS შეტევის დროს ყველაზე ეფექტური საშუალებაა ის რომ, მოხდეს მოწყობილობის დროებით გათიშვა ან იმ გეოგრაფიული ტერიტორიის დაშვების შეზღუდვა, საიდანაც მოდის შეტევა. ასევე ეფექტურია სარეზერვო ინტერნეტ პროტოკოლზე გადართვა და DNS (Domain Name System) (ვებგვერდზე შეტევის დროს) კონფიგურაციის დროებით შეცვლა.

როგორც წინა თავში ავღნიშნეთ არსებობს IPv6-თვის დამახასიათებელი საფრთხეები, რომლებიც IPv4-ში არ გვხვდება. საგულუსხმოა ორი ტიპის შეტევა ესენია ფრაგმენტული შეტევა და შეტევა dual stack სისტემაზე. განვიხილოთ თითოეული მათგანი.

ფრაგმენტული შეტევის დროს ცალკეული ფრაგმენტირებული პაკეტები, რომლებიც ინკაპსულირებული არიან ფრეიმებში საფრთხეს არ წარმოადგენს და ფაირვოლი მას არ განიხილავს როგორც პოტენციურ საფრთხეს, მაგრამ მისი დეკაპსულაციის დროს ხდება იმ საზიანო კოდის აღდგენა რომელიც წარმოადგენს შემტევს, შედეგად კი ვიღებთ, დავირუსებულ სისტემას, მოპარულ მონაცემებს და ა.შ. მსგავსი შეტევისგან თავის დასაცავად საჭიროა ე.წ. „მონაცემის ვირტუალური ამწყობი“, ანუ პროგრამა, რომელიც ერთ მონაცემთან დაკავშირებული პაკეტებისაგან, იზოლირებულ გარემოში ააწყობს საწყის მონაცემს და მასზე ანალიზის გაკეთების შემდეგ დადებითი შედეგის შემთხვევაში გადააგზავნის მას სისტემაში. ამით ჩვენ

ვახდენ იმის პრევენციას, რომ საზიანო კოდის შემცველი ინფორმაცია აღმოჩენილი იქნეს მის გავრცელებამდე.

როგორც ვიცით IPv4 და IPv6 პროცესის გაშვება შესაძლებელია ერთ სერვერზე ე.წ. dual stack მექანიზმით, მაგრამ უსაფრთხოების მხრივ მისი გამოყენება რეკომენდირებული არ არის რადგან IPv4 -ის პაკეტებს IPv6 -ი ვერ ხედავს და პირიქით. ამიტომ, თუ მომხმარებლის მოწყობილობაზე არსებობს ორივე ტიპის მისამართი, გარეშე პირს თავისუფლად შეუძლია რომელიმე ერთი მათგანით მოახდნოს შეტევა იმ პროგრამულ უზრუნველყოფაზე ან აპლიკაციაზე, რომელიც იყენებს მეორე მისამართს, ანუ ვიღებთ შეტევის მექნიზმს რომლისგანაც თავის დაზღვევა თითქმის შეუძლებელია.

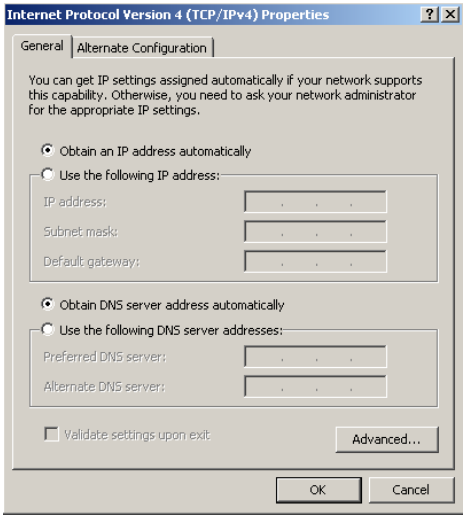
§2. IPv6 ქსელში DHCP-EUI-64 მეთოდის შემოღებით გაუმჯობესებული უსაფრთხოება

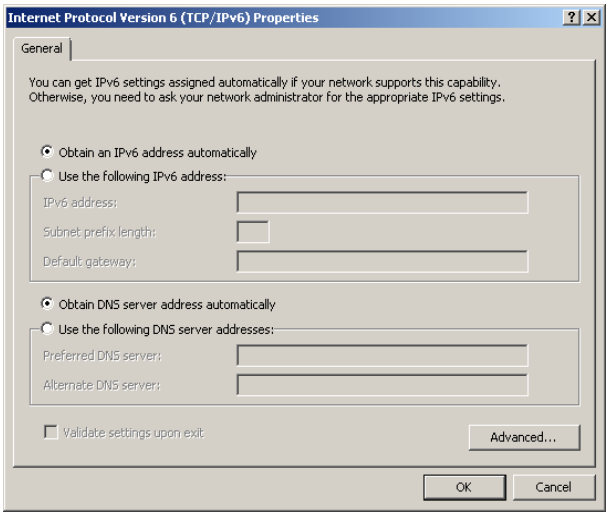
სწორედ უსაფრთხოების პრობლემები გახდა ის მიზეზი, რომ მოგვეხდინა რაიმე პროგრესი პროტოკოლთა შორის, რათა უფრო მეტად დაცული ყოფილიყო კომუნიკაცია. ერთ-ერთი ასეთი პროტოკოლია DHCPv6 რომელიც საშუალებას გვაძლევს დინამიურად მივანიჭოთ IPv6 მისამართები ქსელში ჩართულ მოწყობილობებს.

ამ მოდელით მიღებული უპირატესობა მდგომარეობს შემდეგში: რადგანაც ქსელური მოწყობილების მიერ გაგზავნილ პაკეტში ეთითება გამგზავნის MAC მისამართი, ამიტომ თავიდანვე შეიძლება DHCP სერვერს მოვთხოვოთ მიღებული MAC მისამართისათვის, EUI-64 მეთოდის გამოყენებით, დააგენერიროს შესაბამისი IP მისამართი, გაუგზავნოს ის DHCP CLIENT-ს და ერთიან ბაზაში გააკეთოს ჩანაწერი გაცემულ IP მისამართზე. ამ შემთხვევაში 4 შეტყობინების ნაცვლად 2 შეტყობინების გადაცემა იქნება საკმარისი. გარდა ამისა, DHCP CLIENT-ს არ დასჭირდება მისთვის გამოყოფილი IP მისამართის შეამოწმება დუბლირებაზე. ამის შემოწმება მოხდება MAC მისამართის საფუძველზე IP მისამართის დაგენერირების დროს. ამის შედეგად ვიღებთ იმას რომ ქსელში მოძრავი პაკეტების რაოდენობა, რომელიც საჭიროა დამისამართებისთვის მცირდება ორჯერ, რაც იმის საშუალებას იძლება, რომ შემცირდეს გარეშე პირის მიერ პაკეტების დაჭერის ალბათობა. ასევე ვქმნით დინამიური და სტატიკური დამისამრთების შერწყმას, ამით იქმნება უნიკალურ მისამართი ყოველი კონკრეტული მოწყობილობისთვის და ამიტომაც შეტევები, რომლებიც ხორციელდება მისამართების დუბლირებით თითქმის შეუძლებელი იქნება. გარდა ამისა, ერთიანი MAC მისამართების ბაზის შემთხვევაში ადვილი ხდება მეზობელი მოწყოლობილობს აღმოჩენა, რომელიც ასევე ოპტიმიზაციას გაუკეთებს ქსელს და შეამცირებს მასში მოძრავი პაკეტების რაოდენობას.

§3. IPv6 კონფიგურირების განახლებული ინტერფესი

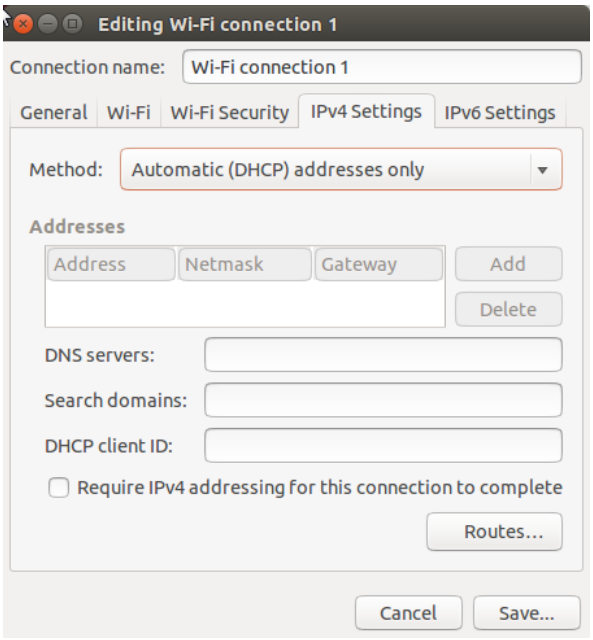
ახალ პროტოკოლზე გადასვლა ასევე გულისხმობს ოპერაციულ სისტემაში მათი მხარდაჭერის გათვალისწინებას. თითქმის ყველა თანამედროვე ოპერაციულ სისტემას გააჩნია IPv6 პროტოკოლის მხარდაჭერა. მიუხედავად ამისა, თანამედროვე ოპერაციული სისტემებში არ არის გამოყენებული IPv6 პროტოკოლში გამოჩენილი დამისამართების ახალი სქემები. თითქმის ყველა ოპერაციული სისტემა დამისამართებისათვის იყენებს IPv4 პროტოკოლში არსებული დამისამართების სქემის ანალოგს და თითქმის იდენტური სამომხმარებლო ინტერფეისებს. ნახ. 10-ზე ნაჩვენებია რამდენიმე სხვადასხვა თანამედროვე ოპერაციული სისტემის IPv4 და IPv6 პროტოკოლების დაკონფიგურირების გრაფიკული ინტერფეისები.

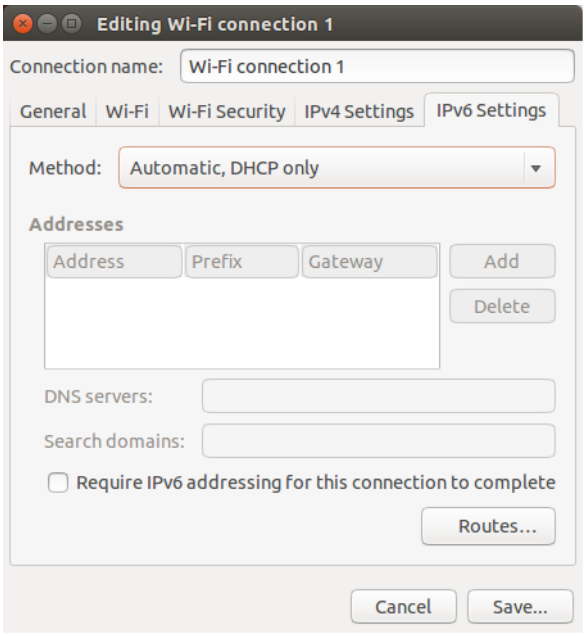




Windows ოპერაციული სისტემა

MAC ოპერაციული სისტემა

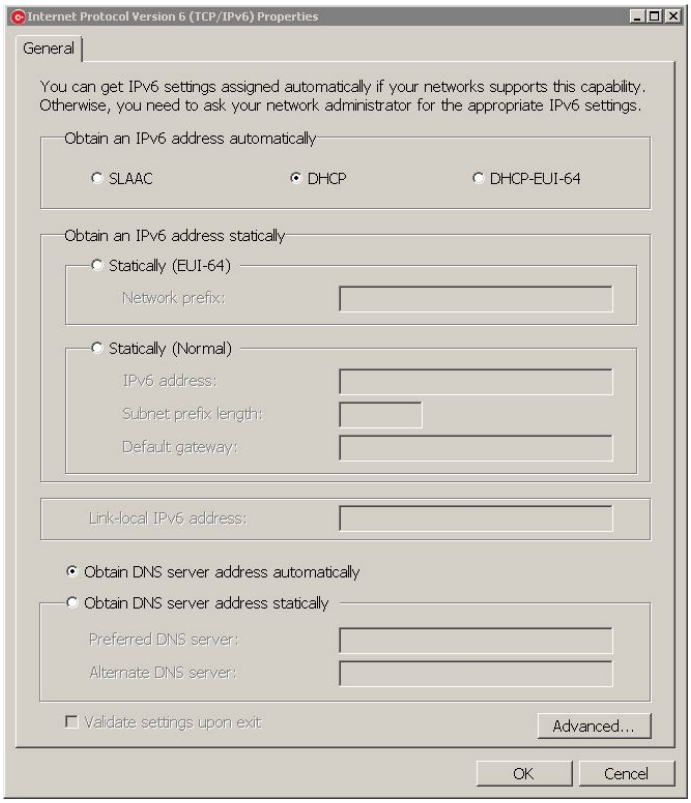




Ubuntu-ს ოპერაციული სისტემა

ნახ.10. სხვადასხვა ოპერაციული სისტემის IP პროტოკოლის კონფიგურირების სამომხმარებლო ინტერფეისი

შევნიშნოთ, რომ Ubuntu-ს ოპერაციული სისტემაში გარკვეული ფორმით გათვალისწინებულია დამისამართების ახალი სქემები.



ნახ. 11. IPv6 პროტოკოლის კონფიგურირების სამომხმარებლო ინტერფეისი

რადგანაც თითქმის არცერთ ოპერაციული სისტემაში მოწყობილობის კონფიგურირებისათვის არაა გათვალისწინებული IPv6 პროტოკოლის დამისამართების ახალი სქემები, ამიტომ შევიმუშავეთ გრაფიკული ინტერფეისი მოდელი (ნახ. 11), რომელშიც გათვალისწინებულია არამხოლოდ IPv6 პროტოკოლში არსებული დამისამართების ყველა სქემა, არამედ ნაშრომის ფარგლებში შემოღებული დამისამართების სქემაც.

შევნიშნოთ, რომ ნახ. 11-ზე ნაჩვენები ინტერფეისი შემუშავებულია Windows ოპერაციული სისტემაში არსებული შესაბამისი გრაფიკული ინტერფეისის ბაზაზე.

დ ა ს კ ვ ნ ა

შესაბამისად DHCP-EUI-64 მეთოდის გამოყენებისას მიღებული შედეგები და უპირატესობები შეგვიძლია ჩამოვაყალიბოთ პუნქტების სახის.

- უნიკალური IPv6 მისამართი EUI-64-ის გამოყენებით;
- იმისთვის, რომ მივიღოთ IPv6 მისამართი და დავიწყოთ ქსელში კომუნიკაცია, ოთხი შუამავალი შეტყობინების ნაცვლად ვიყენებთ მხოლოდ ორს რაც ზრდის მისამართის მიღების სიჩქარეს, უზრუნველყოფს დამატებით უსაფრთხოებას, რომ არ იქნეს პაკეტები დაჭერილი და რაც მთავარია ხდება პროცესების გამარტივება, რაც პირდაპირ კავშირშია სერვერზე, მარშუტიზატორზე, თუ კომუტატორზე დამატებითი დატვირთვის მოხსნასთან.
- მეზობელი მოწყობილობის აღმოჩენისთვისა საჭიროა მხოლოდ ორი unicast შეტყობინება.
- ასევე, იმის გათვალისწინებით, რომ გვექნება უნიკალური IPv6 მისამართების ბაზა, შეიძლება მოხმარებიდან ამოღება DAD პროტოკოლისა, რომელიც უზრუნველყოფს დუბლირებული IP მისამართების აღმოჩენას. უნიკალურობიდან გამომდინარე დუბლირებული მისამართები არ გვექნება.

ამ მეთოდის რეალიზაციისთვის საჭიროა DHCP პროტოკოლის შემდგომი ცვლილებები:

- მონაცემთა ბაზის ცხრილების ფრაგმენტაცია, რომ მოხდეს დროის და უსაფრთხოების ოპრიმიზაცია.
- DHCP პროტოკოლის მიერ მოწყობილობიდან MAC მისამართის მიღების შესაძლებლობა.
- ბაზაში MAC და IPv6 მისამართით ძებნის მეთოდის დამატება, აუცილებელი ჩანაწერების მოსაძებნად.

ასევე მცირე ცვლილება მოხდება DHCP შეტყობინებების პაკეტში.

- აღნიშვნა, რომ მომხმარებელს სურს რეგულარული DHCP პროტოკოლის გამოყენება IP მისამართის მისაღებად.

- აღნიშვნა, რომ მომხმარებელს სურს DHCP-EUI-64 მეთოდით IP მისამართის მიღება.

მსგავსი აღნიშვნა DHCP შეტყობინებაში შესაძლებელია წარმოვადგინოთ როგორც BOOL, ფუნქცია.

საერთო ჯამში ამ მეთოდის გამოყენება IPv6 ქსელში გვაძლევს საშუალებას რომ გავზარდოთ უსაფრთხოების ხარისხი. მისი გამოყენებით ვახდენთ ქსელში პაკეტების შემცირებას, მომხმარებლის უნიკალურ იდენტიფიცირებას, არ გვაქვს დუბლირებული IP მისამართების საფრთხე, შუამავალ მოწყობილობებზე ხდება დატვირთვის შემცირება და ეს ყველა კომბინერებული მექანიზმი საშუალებას გვაძლებს, რომ ქსელში ინფორმაციის გადაცემა იყოს შედარებით უსაფრთხო.

ამის მიუხედავად ლოგიკურია ყოველთვის იქნება შეკითხვა, რამდენად დაცულია ქსელში კომუნიკაცია და მონაცემების თუ ინფორმაციის მიღება-გაგზავნა? ამ შეკითხვაზე პასუხის გაცემა არც თუ ისე ადვილია, რადგან ყოველი ახალი დაცვის სისტემის ან მეთოდის შექმნისას, დროთა განმავლობაში აუცილებლად მოიძებნება მექანიზმი, რომელიც მეთოდის გვერდით საზიანო საქმიანობის წარმოებას. ასევე უნდა ითქვას, რომ მიუხედავად ამისა არ უნდა შევწყვიტოთ ახალი და ეფექტური მეთოდების შექმა რადგან ამაზეა დამოკიდებული კომუნიკაციის დაცულობა და მრავალი ადამიანის პირადი ცხოვრების თუ კომპანიების ინფორმაციის კონფიდენციალურობა.

ლ ი ტ ე რ ა ტ უ რ ა

1. Internet Protocol, University of Southern California, RFC: 791, 1981 (https://tools.ietf.org/html/rfc791);
2. S. Hogg, E. Vyncke, IPv6 Security. Cisco Press. 2009;
3. P. Srisuresh, M. Holdrege, IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663, 1999 (https://tools.ietf.org/html/rfc2663);
4. P. Srisuresh, K. Egevang, Traditional IP Network Address Translator (Traditional NAT), RFC 3022, 2001 (https://tools.ietf.org/html/rfc3022);
5. S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, 1998 (https://www.ietf.org/rfc/rfc2460.txt);
6. R. Graziani, IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6, 2012;
7. S. McFarland, M. Sambi, N. Sharma, S. Hooda IPv6 for Enterprise Networks, 2011;
8. R. Hinden, S. Deering, IP Version 6 Addressing Architecture, RFC 2373, 1998 (www.ietf.org/rfc/rfc2373.txt);
9. Droms R., Volz B., Lemon T., Perkins C., Carney M., Dynamic Host Configuration ProtocolforIPv6 (DHCPv6), RFC 3315, 2003 *(*https://www.ietf.org/rfc/rfc3513.txt*);*
10. პ.ქარჩავა, გ.ასანიშვილი, DHCPv6 პროტოკოლის ერთი გაუმჯობესების შესახებ, სტუ ა.ელიაშვილის მართვის სისტემების ინსტიტუტი, 234-238 გვ. #18, 2014.
11. A. Conta, S. Deering, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC 2463, 1998 (https://tools.ietf.org/html/rfc2463);
12. S. Deering, W. Fenner, B. Haberman, Multicast Listener Discovery (MLD) for IPv6, RFC 2710, 1999 (https://tools.ietf.org/html/rfc2710);
13. T. Narten, E. Nordmark, W. Simpson, H. Soliman, Neighbor Discovery for IPv6, RFC 2461, 1998 (https://tools.ietf.org/html/rfc 2461);
14. N. Moore, Optimistic Duplicate Address Detection (DAD) for IPv6, RFC 4429, 2006 (https://tools.ietf.org/html/rfc4429);
15. S. Thomson, T. Narten, IPv6 Stateless Address Autoconfiguration, RFC 2462, 1998, (https://tools.ietf.org/html/rfc2462).