GELECEK NESİL IP – YEREL ALTYAPILARDA AĞ VE GÜVENLİK ANALİZİ

HASAN ATAN

İçindekiler

Şekil Listesi

Kısaltmalar

IANA : Internet Assigned Numbers Authority (İnternet atanan numaralar otoritesi)

RFC : Request for Comments

RIR : Regional Internet Registry (Bölgesel internet kayıt merkezi)

ISP : Internet Servis Provider (İnternet Servis Sağlayıcı)

MTU : Maximum Transmission Unit (Maksimum iletim birimi)

NDP : Neighbour Discovery Protocol (Komşu keşif protokolü)

NS : Neighbour Solicitation (Komşu talebi)

NA : Neighbour Advertisement (Komşu duyurusu)

RS : Router Solicitation (Yönlendirici talebi)

RA : Router Advertisement (Yönlendirici duyurusu)

CP : Certification Path Solicitation (Sertifika yolu talebi)

CP : Certification Path Advertisement (Sertifika yolu duyurusu)

SLAAC : Staless Adress Autoconfiguration (Durumsuz adres otokonfigürasyonu)

DHCPv6: Dynamic Host Configuration Protocol Version 6

DNS : Domain Name System (Alan adı sistemi)

DAD : Duplicate Adres Detection (Yinelenen adres belirleme)

NUD : Neighbor Unreachability Detection (Komşu erişilemezlik keşfi)

EUI-64 : Extended Unique Identifier (Genişletilmiş benzersiz tanıtıcı)

MAC : Media Access Control (Ortam erişim yönetimi)

SEND : Secure Neighbor Discovery (Güvenli komşu keşfi)

CGA : Cryptographically Generated Address (Kriptografik üretilmiş adres)

TA : Trust Anchor (Güven kaynağı)

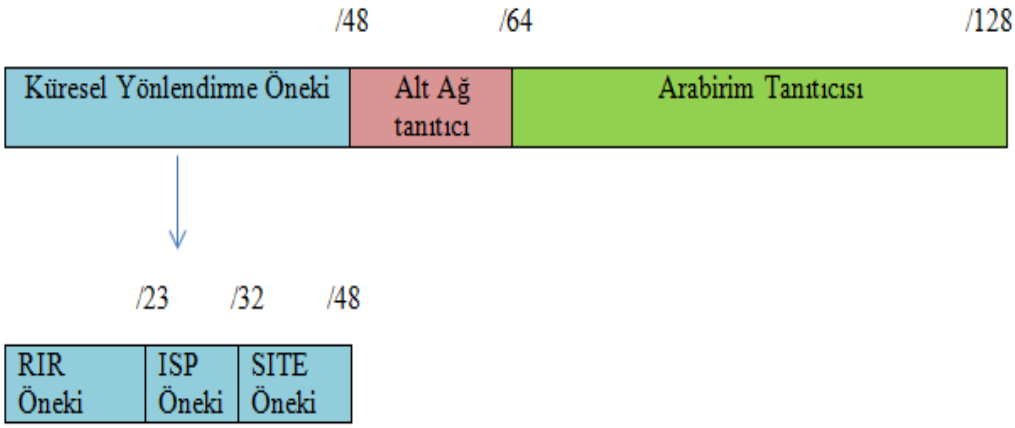
ADD : Authorization Delagation Discovery (Yetkilendirme delegasyonu keşfi)

CC : Collision Counts (Çarpışma Sayısı)

1. IPV6

1.1 IPv6 Adres Yapısı

IPv6 Temel olarak aşağıdaki şekilde görüldüğü gibi bir adres formatına sahiptir.



Şekil 1.1: Temel IPv6 Yapısı

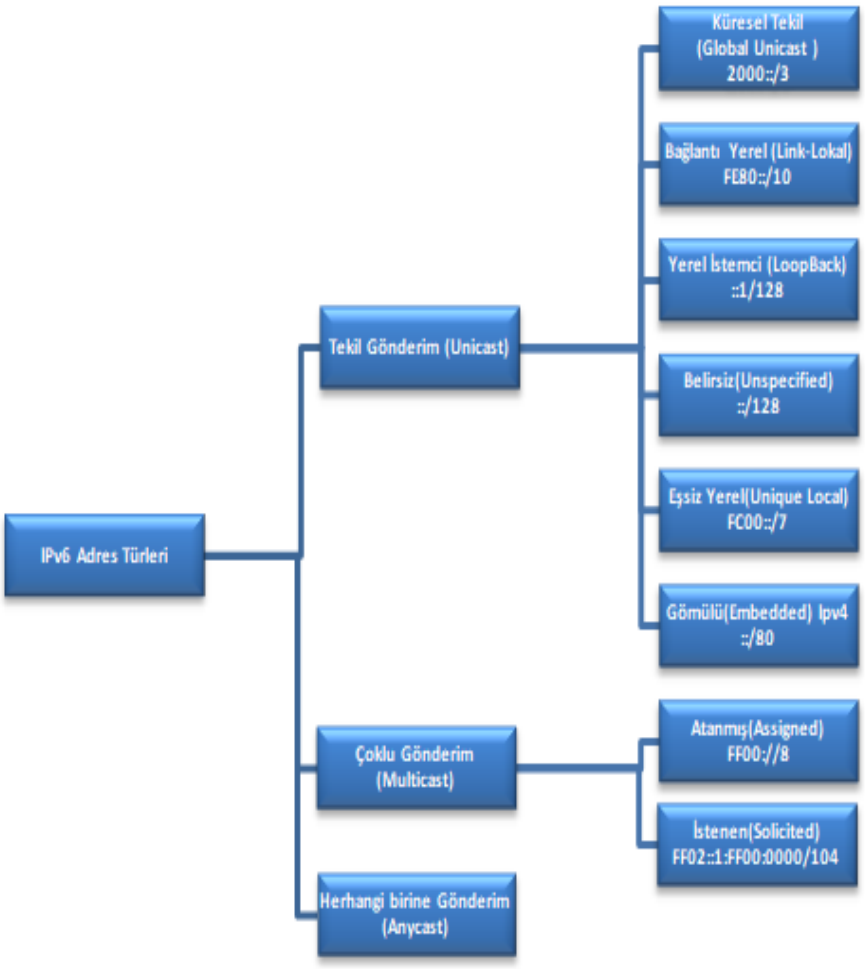
Formattaki her bir kısmın anlamı şu şekildedir;

Küresel Yönlendirme Öneki: İnternet servis sağlayıcılar(ISP) veya Bölgesel İnternet Kayıt Merkezi (RIR) tarafından kurumlara verilen önek bilgisini içermektedir. IPv6 adres yapısındaki küresel yönlendirme öneki ilk 48 biti ifade etmektedir. Bunun 23 biti RIR'lar tarafından, her bir RIR için sonraki 32 bite kadar olan kısım ISP'lere dağıtılmakta, her bir ISP ise sonraki 16 biti kurumlara dağıtmaktadır [1].

Alt Ağ Arabirim Tanıtıcısı: Bir kurumun aldığı öneke göre gerekli gördüğü sayıda kendi içerisinde oluşturduğu alt ağları ifade etmektedir ve 2^{16} adet alt ağa olanak tanımaktadır.

Arabirim Tanıtıcısı: Her bir alt ağ içerisindeki istemcilere verilecek olan IP aralıklarını ifade etmektedir. 64 bitlik bir alan olduğu için her bir yerel ağ için 2^{64} adet istemci IP adresine olanak tanımaktadır.

1.2 IPv6 Adres Türleri



Şekil 1.2: IPv6 Adres Türleri

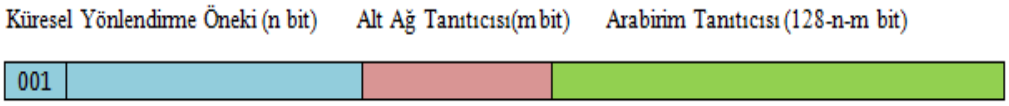
IPv6'da temelde üç farklı türde IP adresi vardır. Bunlar yukarıda ki şekilde de görüldüğü üzere Tekil Gönderim Adresi(Unicast), Çoklu Gönderim Adresi(Multicast) ve Herhangi Birine Gönderim Adresi(Anycast) türleridir. Bu adresler sırasıyla şu şekilde incelenebilir.

1.2.1 Tekil Gönderim Adresi

Tek bir hedef veya kaynak arabirim belirten adreslerdir. 6 farklı tekil gönderim adresi vardır. Bunlar şu şekildedir;

Küresel Tekil: Arabirimlerin küresel bağlantıları için kullanılan ve '001' ile başlayan IP adreslerini ifade etmektedir. Küresel ortamda yönlendirilebilmektedirler. IPv4 ortamında genel IP adreslerine karşılık geldiği düşünülebilir. IANA (Internet Assigned Numbers Authority) tarafından IP dağıtım yetkilisi kuruluşlar olan servis sağlayıcılara

oradan da isteyen kurumlara dağıtılır [1]. Küresel tekil gönderim adres IP aralığı 2000://3 olarak ifade edilir ve IP aralığı 2000::/3 ile 3FFF::/3 aralığında yer almaktadır. Aşağıdaki şekilde RFC (Request For Comments) 3587'ye göre bir küresel tekil gönderim adresinin yapısını göstermektedir.



Şekil 1.3: Küresel Tekil Gönderim Adres Yapısı [2]

IANA internet sitesinden [3] internet servis sağlayıcılara IP dağıtacak olan bölgesel RIR'lara atanan IPv6 küresel tekil gönderim IP aralığı görülebilmektedir.

Bir küresel tekil gönderim adresi manuel olarak veya dinamik olarak arabirimlere atanabilir. Dinamik atama DHCPv6 (Dynamic Host Configuration Protocol Version 6) veya SLAAC(Staless Adress Autoconfiguration) ile sağlanabilmektedir. Detayları sonraki bölümlerde incelenmiştir.

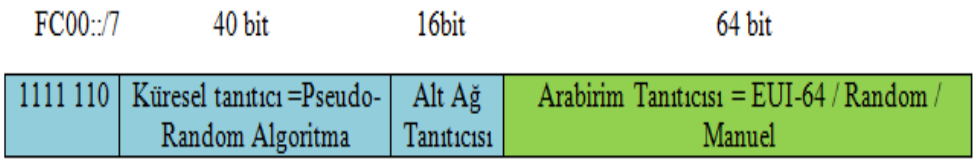
Bağlantı Yerel Adresi: Aynı yerel ağdaki cihazların birbirleri ile haberleşmeleri için kullanılan tekil gönderim ipv6 adresleridir.FE80::/10 önekindeki, yani FE80::/10 ile FEBF::/10 arasındaki IP adreslerini içermektedir. Yönlendiriciler tarafından yerel ağ dışında yönlendirilmezler. Bu anlamda IPv4 uzayında özel IP adreslerine karşılık gelmektedirler. Statik veya dinamik olarak arabirimlere atanabilirler. Dinamik atama EUI-64(Extended Unique Identifier) ile veya random arabirim IP adresi üretilerek sağlanmaktadır. Bağlantı yerel IP adresi atamaları için DHCPv6 kullanılmamaktadır. Aşağıdaki şekilde bir bağlantı yerel tekil gönderim adresinin yapısı gösterilmektedir.

Şekil 1.4: Bağlantı Yerel Tekim Gönderim Adres yapısı

IPv6 bağlantı yerel tekil gönderim IP adreslerinin en önemli kullanım alanlarından biri de yönlendiricilerin kendi aralarındaki haberleşmelerin bu IP türü üzerinden gerçekleşmesidir. Örneğin yönlendiriciler arasında komşuluk bilgilerinin paylaşılması, yönlendiricilerin sonraki atlama IP adreslerinin bağlantı yerel IP

adresleri olması ve yönlendiricilerin istemcilere ağ geçidi bilgisini RA mesajları ile kendi bağlantı yerel IP adresi olarak bildirmesidir [4]. Kısaca yönlendiricilerin kendi aralarındaki trafik bağlantı yerel IP adresleri üzerinden iletilirken, internet trafiği küresel tekil IP adresleri ile sağlanmaktadır.

Eşsiz Yerel Adres: Küresel olarak eşsiz olan yerel IP adresleri olarak da tanımlanabilir.FC00::/7 olarak ifade edilir ve FC00::/7 to FDFF::/7 aralığındaki IP adreslerini kapsamaktadır. Yerel IP adresi olarak kullanıldığı için küresel ortamda yönlendirilmemelidirler . Bu IP adresinin temel amacı farklı sitelara sahip bir organizasyonda farklı siteler için küresel ortamda eşsiz yerel IP adresleri oluşturmaktır. Siteler arasında yönlendirilebilir. Fiziksel olarak çok ayrı olan iki farklı siteyi tek bir organizasyon altında yönetmek için kullanılabilir. Bu IP adreslerinin küresel ortamda eşsiz olmasını sağlayan ise 40 bitlik küresel tanıtıcı kısmının RFC 4193'te tanımlanan Sample Code for Pseudo-Random Global ID algoritmasına göre üretilmesidir [5].



Şekil 1.5: Eşsiz Yerel Tekil Gönderim adresi yapısı [5]

Yerel İstemci Adresi: İşletim sisteminin kendi içerisinde kullandığı IP adreslerini ifade eder. IPv4 uzayındaki 127.0.0.1 IP'sine denk gelir ve '::1/128' ile ifade edilir. İşletim sisteminde TCP/IP yığını üzerinde test yapmak için kullanılır. İşletim sisteminden çıkıp ağ üzerinde dolaşan bir paketin kaynak veya hedef IP adresi yerel istemci IP adresi olamaz ve herhangi bir fiziksel arabirime atanamaz.

Belirsiz Adres: Henüz IP adresi atanmamış bir işletim sistemi ağa bir paket gönderecek ise belirsiz adresi kaynak IP adresi olarak kullanılır. Yani o an ilgili cihazda IP olmadığını ifade etmektedir. Örneğin DAD(Duplicate Address Detection) süreci başlangıcında işletim sistemi henüz geçerli bir IP adresine sahip olmadığı için komşu keşfi için gönderdiği paketlerin kaynak adresi olarak belirsiz adres kullanmaktadır. Belirsiz adres ' ::/128' veya 0:0:0:0:0:0:0:0 şeklinde ifade edilebilir. Yerel istemci adresler gibi fiziksel bir arabirime atanamaz ve hedef adres olamazlar.

Gömülü IPv4: IPv4'ten IPv6'ya geçiş sırasında bu iki farklı IP altyapısının birbirleri ile uyumlu çalışabilmesi açısından IPv4'ün IPv6 içerisine gömülmesi ile oluşturulmuştur. 128 bitlik IPv6'nın son 32 biti IPv4 yazılır ilk 96 biti de sıfır olarak işaretlenir. Böylelikle NAT-PT, NAT-64 ve tünelleme gereken alanlarda bu iki farklı IP bir arada kullanılabilir. Gömülü Ipv4 adresi '::/96' olarak ifade edilebilir.

1.2.2 Çoklu Gönderim Adresi

Belli bir grup içerisinde birden fazla hedef arabirim belirten ipv6 çeşidini ifade etmektedir. '*Atanmış' ve 'İstenen'* olmak üzere ikiye ayrılmaktadır.

Atanmış: Cihazlara varsayılan olarak atanmış kalıcı çoklu gönderim grup IP adresleridir. IP aralığı FF00::/8 olarak ifade edilebilir. Hangi tür cihazların hangi çoklu gönderim IP grubuna dahil edileceği RFC 2375' te tanımlanmıştır. Örneğin bağlantı yerel çoklu gönderim IP tanımlarında 'FF02::1' bütün düğümlerin IP adreslerini, 'FF02::2' bütün yönlendiriciler için çoklu gönderim IP adreslerini ifade etmektedir [6].

İstenen(Solicited): IP adres aralığı 'FF02::1:FF/104' olarak ifade edilir. Son 24 bit ise cihazın sahip olduğu tekil gönderim adresinin son 24 biti eklenerek tamamlanır. Eğer bir cihazı bir tekil gönderim adresi varsa o aynı zamanda solicited multicast adresi de almış olur ve bu çoklu gönderim grubuna dahil olur. Aynı çoklu gönderim grubuna gelen istekleri o çoklu gönderim grubundaki bütün cihazlar dinler ve kendilerini ilgilendiren isteklere cevap verirler. IPv6 ND (Neighbour Discovery) sürecinde adres çözümlemesi ve adres çakışması mesajı (DAD) için kullanılır. IPv4'da adres çözümü için kullanılan ARP protokolü yerine IPv6'da NDP kullanılmaktadır.

1.2.3 Herhangi Birine Gönderim

Aynı IPv6 adresinin birden fazla cihaza veya bir cihazda farklı arabirimlere verildiği durumu ifade etmektedir. Genellikle önemli görevleri olan sunucuları hizmet kesintisi olmaması için ağ yedekliliğini sağlamak için kullanılır. Örneğin birden fazla alan adı sunucusu bulunduran kurumlarda sunucuların her birine aynı IP adresi verilmekte, istemci kendisine en yakın alan adı sunucusuna sorgulama yaparak internete çıkmaktadır. En yakın alan adı sunucusunda bir arıza olması durumunda diğer alan adı sunucusu tercih edilmektedir.

Bunların yanında belirtmek gerekir ki IPv6'da broadcast IP adresi mevcut değildir. Broadcast IP adresinin IPv4'te ki işlevleri ağırlıklı olarak IPv6'da çoklu gönderim adresleri tarafından sağlanmaktadır.

2. IPv6 ADRESLERİNİN ÜRETİLME ve DAĞITILMA SÜRECİ

IPv6'nın küresel önek kısmının RIR veya ISP'ler tarafından dağıtıldığını bilmekteyiz. Arabirim tanıtıcı kısmı da farklı yöntemlerle istemcilere dağıtılmaktadır. Burada genel bakış açısı istemcinin kendi IPv6 arabirim adresini kendisi üretmesidir. Bunun yanında istemcilerin küresel tekil ve bağlantı yerel IP adreslerini tanımlama yöntemleri aşağıdaki şekilde gösterilmiştir.

Küresel tekil gönderim adresi	- SLAAC (EUI-64 veya DHCPv6 ile), DHCPv6 - Manuel
Bağlantı yerel tekil gönderim adresi	- EUI-64, Random - Manuel

Şekil 2.1: Küresel tekil ve bağlantı yerel IPv6 Dağıtılma Yöntemleri

IP dağıtıma süreci dinamik ve statik olarak tanımlamasının yanında durumsuz(stateless) ve durumlu(statefull) olarak da tanımlanabilir. Durumsuz IP, istemcilerin IP bilgilerinin herhangi bir yerde kayıt tutulmadığı anlamına gelmektedir. Dolayısı ile istemci kendi IPv6 adresini ürettikten sonra çakışma olmaması için IPV6 DAD işlemini yapmak zorundadır. Durumlu IP ise istemcilerin IP bilgilerinin DHCPv6 tarafından tutulduğunu ifade etmektedir. Durumlu IP yapılandırması yapıldığı zaman DAD işlemine gerek olmamakla beraber SLAAC ve DHCPv6 birlikte kullanıldığında DAD istemciler tarafından yapılmaktadır.

Bağlantı yerel ve küresel tekil gönderim adreslerinin arabirim tanıtıcı kısımlarının yapılandırma yöntemleri aşağıda verilmiştir.

2.1 Manuel Konfigürasyon

IPv6 adresinin statik olarak elle girilmesini ifade eder. global unicast address veya link local adress manuel olarak konfigüre edilebilir.

2.2 EUI-64

EUI-64 genişletilmiş benzersiz tanıtıcı, 64 bitlik IPv6 arabirim adresinin 48 bitlik MAC(Media Access Control) adresinden türetilmesidir. Bağlantı yerel adresleri dinamik olarak, küresel tekil gönderim adresleri de hem dinamik hem statik olarak EUI-64 formatına göre istemcilere atanabilirler. MAC adresi küresel çapta eşsiz olduğu için MAC adres tabanlı arabirim tanıtıcısı üretilmesi, IPv6 adresinin eşsizliğini sağlamaktadır. IPv6 arabirim adresi EUI-64 formatından üretilme süreci aşağıda özetlenmiştir.

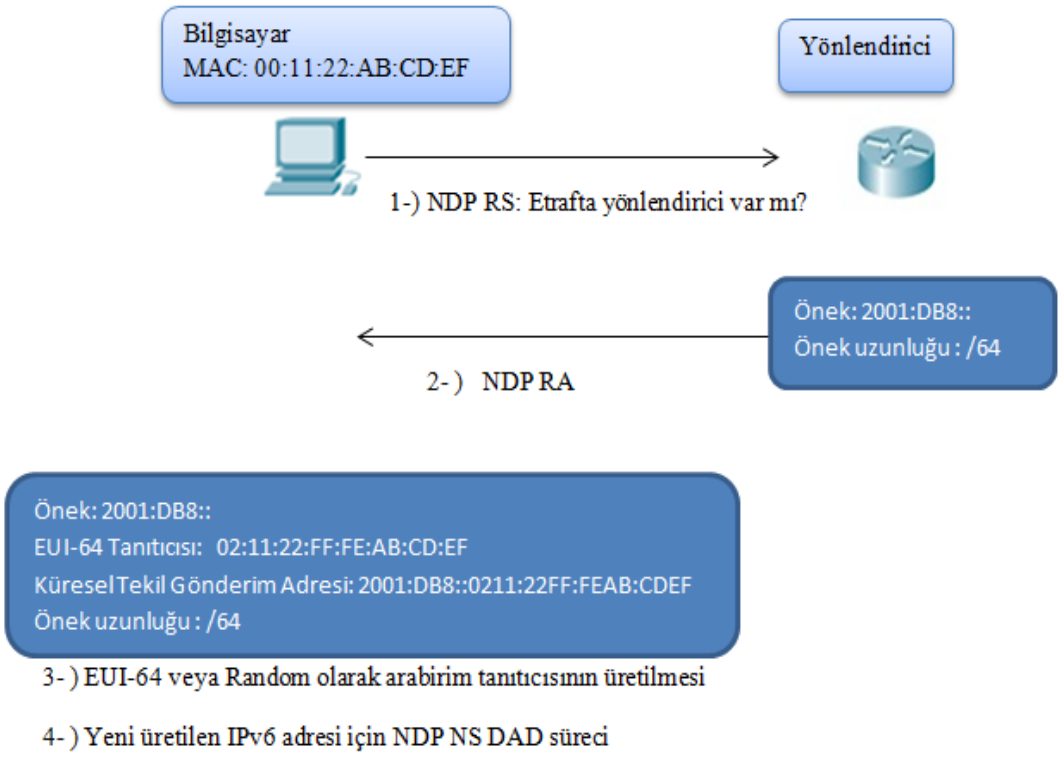
- Cihazın MAC adresinin tam orta kısmına FFFE adresi yerleştirilir. FFFE kısmı bu iş için IEEE tarafından rezerve edilmiştir. 48 bitlik bir adresten EUI-64 adresinin üretildiğini gösterir [4].
- Ardından MAC adresinin 7. biti dönüştürülür. Bu bir yerel/küresel bayrak biti olarak adlandırılır ve küresel eşsiz adresler için sıfır, yerel adresler için ise 1 olarak ayarlanır. Örneğin sanal arabirimler yerel adresler olduğu için bu bit 1 olarak ayarlanır. Bu kurala uymayarak buradaki biti değiştirmeden yazan üreticiler de vardır.
- U/L biti adresin yerel veya küresel olarak yönetildiğini belirlemek için kullanılır. Eğer bir sıfır ise bu MAC adresi IEEE tarafından bir şirkete verildiği anlamına gelir. Eğer bu bit 1 ise yerel olarak yönetildiği anlamına gelir. Bu bit tahmin edilebildiği için ileriki konularda işlenecek olan CGA (Cryptographically Generated Address) doğrulama kısmında önem arz etmektedir.RFC 5342'ye göre U/L bitinin değiştirilmesinin temel amacı ağ yöneticilerinin yerel alan tanımlayıcılarını girmesini kolaylaştırmaktır [7].

2.3 Random Arabirim Tanıtıcısı

EUI-64 formatı her ne kadar küresel ortamda eşsizliği sağlasa da farklı ağlardan bağlanan aynı cihazlar aynı arabirim tanıtıcısına sahip olacağı için IP katmanında izlenebilirler. Buna uygulama katmanında yer alan çerezlerin izlenmesine benzer bir izleme olarak bakılabilir. Hangi cihazın nerelerde hangi internet adreslerine bağlandığı gibi bilgiler elde edilebilir. Bunun güvenlik açığını kapamak için RFC 4941'de arabirim tanıtıcısının random olarak üretilme yöntemi tanımlanmaktadır [8].

2.4 EUI-64 metodu veya Random Arabirim Tanıtıcısı ile SLAAC

SLAAC, durumsuz adres yapılandırması anlamına gelmektedir. Bağlantı yerel adresine sahip bir istemcinin yönlendiriciden küresel önek bilgilerini alması ve bu önek bilgisine ek olarak EUI-64 metoduna veya RFC 4941' de tanımlanan random yöntem ile arabirim tanıtıcısını üretmesi sonucunda küresel tekil gönderim adresini oluşturmasıdır.



Şekil 2.2: SLAAC Yöntemi

Yukarıdaki şekilde bir istemcinin bir yönlendiriciden önek bilgisini alıp kendi küresel tekil tanıtıcısını ve IP adresini oluşturma süreci gösterilmiştir. Bu durum kısaca şöyle özetlenebilir;

İstemci bilgisayar ilk açıldığında manuel, EUI-64 veya Random arabirim tanıtıcı vasıtasıyla kendisine bir bağlantı yerel IPv6 adresi oluşturulur. EUI-64 veya Random arabirim tanıtıcısına göre IP üretme süreci işletim sistemine göre farklılık gösterebilir. İlgili işletim sistemi Random arabirim üretme algoritması destekliyorsa Random üretilir, EUI-64 kullanıyorsa EUI-64 formatına göre arabirim tanıtıcısı oluşturulur. Örnek vermek gerekirse Windows işletim sistemi günümüzde Random

arabirim tanıtıcısı üretim algoritmasını desteklemektedir fakat bazı Linux işletim sürümleri EUI-64 ile arabirim üretimine devam etmektedir.

Normalde ortamdaki yönlendirici periyodik olarak NDP-RA mesajı ile kendi varlığını bildirir ve önek bilgisini paylaşır.

İstemci bilgisayar açıldığında kendisi ile önek bilgisi paylaşan bir NDP-RA mesajı duyamazsa kendi bağlantı yerel IPv6 adresini kullanarak NDP-RS mesajı ile çevresinde kendisine önek bilgisi yollayabilecek bir yönlendirici arar.

Ortamdaki yönlendirici kendi önek bilgisini NDP-RA mesajı ile istemci bilgisayara yollar

İstemci bilgisayar önek bilgisini alır ve EUI-64 veya RANDOM olarak arabirim tanıtıcısı üretmesi sonucunda kendi küresel tekil adresini üretir.

Bu adresin başkası tarafından kullanılıp kullanılmadığını anlamak amacıyla NDP DAD mesajları yollar. Başkası tarafından kullanılmıyorsa kendi bu adresi kullanmaya başlar. NDP-RS, NDP-RA, DAD sonraki bölümlerde detaylı işlenecektir.

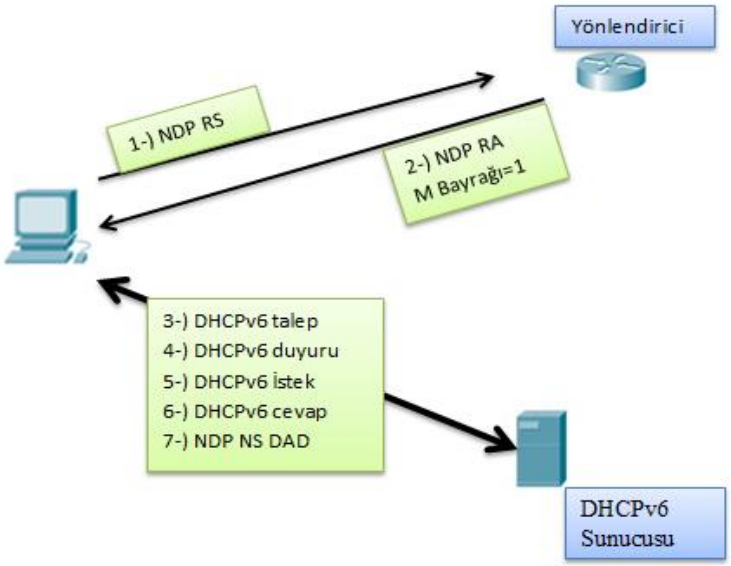
2.5 DHCPv6 ile Durumlu Adres Yapılandırması

Küresel tekil adresleri için istemcinin istediği tüm IP yapılandırma bilgilerinin DHCPv6 tarafından istemcilere dağıtılmasıdır. DHCPv6 durumlu veya durumsuz olarak hizmet verebilmektedir. DHCPv6 sunucusu, SLAAC ile IP dağıtılması sırasında durumsuz olarak DNS(Domain Name System) , NTP veya ihtiyaç duyulan herhangi bir DHCP seçeneğini istemcilere sunabilir, durumlu olarak da bütün DHCP bilgilerini kendisi sunabilir. Bu süreç genel olarak şu şekilde yürümektedir:

- İstemci IP almak istediğinde çevresine bir NDP RS mesajı yayar.
- Çevredeki bir yönlendirici ise NDP RA mesajı ile geri döner. Burada RA mesajındaki bir bit istemciyi durumlu veya durumsuz olarak yapılandırılması konusunda bilgi verir. Managed Address Configuration(M) biti olarak geçen bu bit eğer sıfır olarak işaretlenmişse yönlendirici istemciyi SLAAC ile yapılanması gerektiği konusunda uyarır.

Eğer bu bit 1 ise yönlendirici istemciye kendisine bir DHCPv6 bularak durumlu olarak yapılanması gerektiği konusunda bilgi verir.

- Yönlendiriciden gelen RA mesajında M biti 1 olarak işaretlenmişse istemci çevresine DHCPv6 talep mesajı yayarak çevresinde bir DHCP sunucusu arar ve bu sunucu sayesinde durumlu olarak yapılandırılabilir.DHCPv6 istek mesajları çoklu gönderim olarak FF02::1:2 adresine gönderilir. Bu adres IANA tarafından yerel IP kapsamında "Bütün DHCP Agent IP adresleri" için tahsis edilmiş çoklu gönderim IP grubudur.



Şekil 2.3: DHCPv6 ile Durumlu IPv6 Yapılandırması

2.6 DHCPv6 ve Durumsuz Otomatik Yapılandırma(SLAAC)

EUI-64 veya Random arabirim tanıtıcısı ile SLAAC yapılandırmasında dikkat edilmesi gereken önemli hususlardan biri istemcinin sadece önek bilgisini yönlendiriciden almasıdır. DNS, NTP gibi bilgilere ihtiyacı olduğunda bu bilgiler ya statik olarak veya DHCPv6 aracılığıyla sağlanmak zorundadır. Dolayısı ile ortamda SLAAC kullanılsa bile bu tür bilgilerin statik olarak girilmesi istenmiyorsa DHCPv6 sunucusuna da ihtiyaç vardır. SLAAC'ın DHCPv6 ile beraber çalışması durumunda ise genel süreç aşağıdaki şekilde özetlenmiştir.

- İstemci IP almak istediğinde çevresine bir NDP RS mesajı yayar. Çevredeki bir yönlendirici ise NDP RA mesajı ile geri döner.

- Bu mesaj içerisinde “O” (Other Configuration) biti olarak geçen bit eğer 1 olarak işaretlenmişse yönlendirici istemciyi SLAAC ile yapılanması gerektiği fakat önek bilgisi dışındaki DNS gibi ihtiyaç duyulabilecek bilgilerin DHCPv6 sunucusundan alınması gerektiği konusunda bilgi verir [9]. Böylelikle istemci önek bilgisini yönlendiriciden alır, kendi arabirim tanıtıcısını Random veya EUI-64 ile üretir ve DNS, NTP gibi geri kalan bilgileri almak için DHCP talep mesajı ile ortamdaki DHCPv6 sunucusundan faydalanır

SLAAC bu özellikleri ile özellikle kablosuz ortamlar için uygun olmakla beraber avantajlarını şu şekilde sıralayabiliriz:

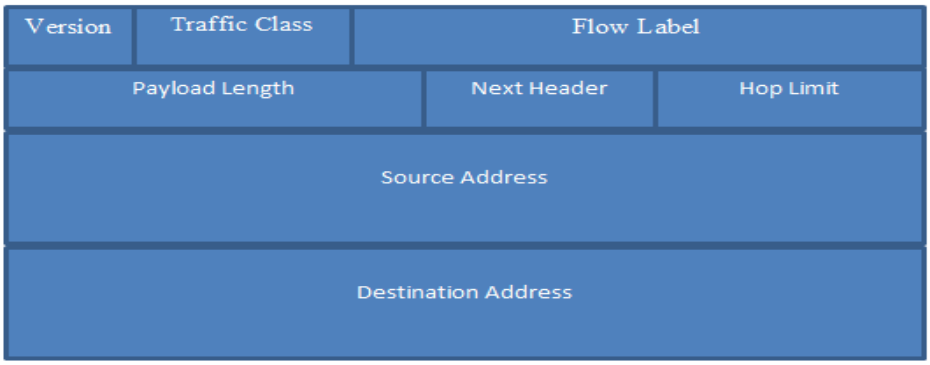
- DNS bilgilerinin statik olarak girilmesi veya bir merkezi ortamdan istemcilere dağıtılması halinde internete bağlanmak için DHCPv6 sunucusuna ihtiyaç yoktur [10].
- Ağ cihazları açılır açılmaz manuel bir IP bilgisi girmeden IP adresi alabilir ve internete bağlanabilirler [10]. Bu özellik bilhassa “Nesnelerin İnterneti” ortamlarında kullanılacak cihazların kendi IP adreslerini otomatik atayabilmelerini sağlayacağı için cihazların yönetimini kolaylaştıracaktır.

- İnternete bağlanan cihaz sayısının her geçen yıl arttığını düşünürsek ve bunlar için manuel veya DHCP servisleri ile IP dağıtımının yönetilmesi günden güne zorlaşmaktadır. Bu anlamda SLAAC cihazların kendi kendilerini yapılandırmasını sağlayarak daha az işgücü ihtiyacı gerektirmektedir [10].

3. IPv6 ve ICMPv6 BAŞLIK YAPISI ve İNCELEMESİ

3.1 IPv6 Başlık Yapısı

IPv6 başlık yapısı RFC 2460’a göre aşağıda şekilde gösterilen şekilde tanımlanmaktadır.



Şekil 3.1: IPv6 Başlık Yapısı [11]

IPv6 başlık yapısı yukarıdaki şekilde gösterilmektedir. Bu başlık yapısındaki her bir alanı açıklamak gerekirse;

Version(Sürüm): IP başlığının sürüm 4 veya sürüm 6 olduğunu belirtmek için kullanılan 4 bitlik bir alandır. Sürüm 6 için bu alan '0110' değerini almaktadır.

Traffic Class(Trafik Sınıfı): IPv4'te TOS (Type of Service/Servis Tipi) alanına karşılık gelen 8 bitlik alandır. Bu alan farklı önceliklere ve sınıflardaki IPv6 paketlerini ayırt etmek ve tanımlamak için kullanılır [4]. Örneğin ses veya video trafiğini önceliklendirmek bu alanda yapılacak ayarlarla mümkündür.

Flow Label (Akış Etiketi): 20 bit uzunluğundaki bu alan cihazlar tarafından bir akışın paketlerini kaynak ve hedef IP adreslerine göre sınıflandırmak ve etiketlemek için kullanılır. Bu sayede hangi paketin hangi akışın parçası olduğu daha rahat belirlenebilmektedir. Akış belli bir kaynaktan bir hedef noktaya giden ve cihazların sırasına göre etiketlemek istediği paket dizisi olarak adlandırabilir [12]. Bu alan IPv6 yönlendiricileri tarafından gerçek zamanlı servisler gibi özel olarak işlenmesi, etiketlenmesi istenen paket dizilerinin etiketlenmesi için kullanılabilir [4].

Payload Length(Yük Uzunluğu): IPv6 başlığını takip eden alanların toplam uzunluğunu gösteren 16 bitlik alandır. IPv6 uzantı başlıkları ve datanın toplam uzunluğunu gösterir. Bu alan en fazla 65536 byte uzunluğuna izin vermektedir. Daha fazla byte gerektiren zamanlardan IPv6 jumbogram uzantısı kullanılır ve bu alan 32 bit ile ifade edilir. Yani jumbogram ile beraber 2^{32} byte kadar yük uzunluğu desteklenir hale gelmektedir [4].

Next Header(Sonraki Başlık): IPv6 başlığından sonra hangi başlığın geleceğini ifade etmek için kullanılan 8 bitlik alandır. Örneğin buradaki değer 58 ise IPv6 başlığından sonra ICMPv6 başlığı geleceği ifade edilir.

Şekil 3.2: Sonraki Başlık

Hop Limit(Sıçrama Limiti): Paketin bir hedefe giderken kaç tane yönlendirici üzerinden geçtiğini gösteren 8 bitlik bir alandır. Her bir yönlendirici buradaki değeri 1 azaltarak iletir. Bu değer sıfıra kadar düşerse paket düşürülür ve paketten yanıt bekleyen kaynak adrese ICMPv6 ile paketin zaman aşımından ötürü düşürüldüğü bilgisi gönderilir [4]. IPv4'te TTL (Time to Limit) adı verilen alana karşılık gelmektedir.

Source Address (Kaynak Adres) (128 bit):Paketi gönderen kaynak IPv6 adresini ifade eder.

Destination Adress(Varış yeri Adresi) (128 bit): Paketin gideceği yeri gösteren IPv6 adresini ifade eder.

3.2 IPv6 Uzantı Başlıkları

IPv6'da çeşitli özel ihtiyaçları karşılamak amacıyla farklı türde ek uzantı başlıkları vardır. Bu başlıklar IPv6 başlığından hemen sonra gelmektedir ve Sonraki Başlık alanında IPv6'dan sonra gelecek başlığa göre bilgilendirme yapılmaktadır. Aşağıdaki şekilde IPv6 başlıkları verilmiştir .

Sonraki Başlık Değeri	Başlık Adı
0	Hop-by-Hop Options(Sıçrama Seçenekleri Başlığı)
43	Routing Header (Yönlendirme Başlığı)
44	Fragment Header(Parçalama Başlığı)
50	ESP (Encapsulation Security Protocol)(Kapsüllenmiş Güvenlik Yük Başlığı)
51	Authentication Header (AH)(Doğrulama Başlığı)
59	Sonraki Başlık yok
60	Destination Options(Varış Yeri Seçeneği Başlığı)
6	TCP Başlığı
17	UDP Başlığı
58	ICMPv6 Başlığı

Şekil 3.3: Sonraki Başlık Değerleri [1]

Her bir başlık yapısı içerisinde sonraki başlığı belirten alan vardır ve kendisinden sonra gelecek olan başlık yapısını göstermektedir. IPv6 uzantı başlıkları aşağıda sırasıyla işlenmiştir.

3.2.1 Sıçrama Seçenekleri Başlığı

Hop-by-Hop Seçenekleri başlığı, bir paketin teslimat yolu boyunca her düğüm tarafından incelenmesi gereken opsiyonel bilgileri taşımak için kullanılır [11]. Örneğin yönlendiricilerin jumbogram desteği için Hop-BY-Hop seçeneği kullanılmak durumundadır. Hop-By Hop seçeneği için IPv6 başlığında next header alanı sıfır ile belirtilir. IPv6'ya seçeneğine birden fazla seçenek ekleneceği zaman Hop-By-Hop seçeneği IPv6 başlığından hemen sonra gelen başlık olacak şekilde planlanmıştır. NEXT Hope sıfır ile belirtilmesi bundan kaynaklanmaktadır.

3.2.2 Yönlendirme Başlığı

RFC 2460'ta tanımlanmıştır. Yönlendirme başlığı paket kaynağının hedefe giden yolu belirlemesine olanak tanır. Bu başlık, bir paketin varış yerine giden yolda bir veya daha fazla ara yönlendiricinin bir listesini içerir [4].

3.2.3 Fragment Başlığı

RFC 2460'ta tanımlanan ve IPv6'da paketi gönderen taraf ın paketleri fragmente ederek karşı tarafa yollaması ve alıcı tarafın ise bu paketleri tekrar birleştirerek işlemesini sağlar. Bu işlem IPv4 altyapısında yönlendiriciler üzerinde de yapılırken IPv6'da fragmentasyon gerektiği zaman sadece paketi gönderen cihaz yani kaynak IPv6'ya sahip cihaz gerçekleştirir. Yönlendiriciler paketi gönderen kaynak IP olmadıkları müddetçe fragmantasyona karışmazlar. Eğer yönlendirici arayüzlerin MTU(Maximum Transmission Unit) değerlerinden daha büyük bir paket alırlarsa paketi düşürürler ve kaynak adrese "ICMPv6 Packet Too Big error message" mesajı yollarlar [4].

3.2.4 IPSEC ESP ve AH Başlıkları

IPSEC işlemleri iki farklı başlık yardımıyla kimlik doğrulama, şifreleme ve bütünlük için kullanılır. Eski RFC tanımlarında IPSEC başlıkları zorunluluk olarak geçerken RFC 6434'ten sonra bu başlık "uygulanmalı" olarak değiştirildi. ESP başlığı özellikle şifreleme amacıyla kullanılmaktadır[4]. Bu başlık varsa taşınan verinin şifreli olduğu

anlaşılır[1]. AH başlığı ise kimlik doğrulama ve veri bütünlüğü için kullanılmaktadır. AH RFC 2402, ESP ise RC 2406'da tanımlanmaktadır.

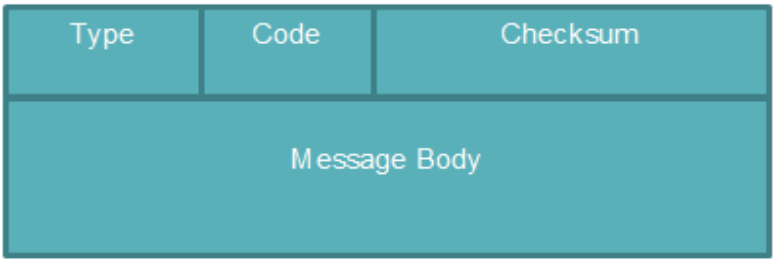
3.2.5 Hedef Seçenekleri Başlığı

Sadece hedef IPv6 adresine sahip cihaz tarafından işlenmesi istenen bilgiler gönderilecekse bu başlıkta kullanılmak zorundadır.

Bütün bunların yanında eğer IPv6 başlığında sonraki başlık alanı 59 ise IP başlığından sonra herhangi bir başlık gelmeyeceği belirtilir.

3.3 ICMPv6 Başlığı ve Yapısı

ICMPv4, ağ cihazlarının birbirleri ile haberleşmeleri sırasında kullandıkları kontrol amaçlı bir protokoldür. Bu özelliklerin yanında ICMPv6'da NDP mesajlarının da bu protokol ile iletilmesi ICMP mesajının kullanım alanını ve önemini arttırmıştır. ICMP cihazlar arası haberleşmelerde bilgi ve hata mesajları alınması açısından önem arz etmektedir. IPv6 başlığında sonraki başlık alanının "58" olması IPv6 başlığının ardından gelecek protokolün ICMPv6 olduğunu gösterir. ICMPv6 paket başlık yapısı RFC 4443'e göre yapısı aşağıdaki şekilde gösterilmiştir.



Şekil 3.4: ICMPv6 Başlık Yapısı [13]

Başlıktaki her bir alanın anlamlarını özetlemek gerekirse; Type(Tip)(1 byte), ICMPv6 mesajının tipini göstermektedir. Bu kısımdaki mesaj tipleri hata ve bilgi mesajları olmak üzere ikiye ayrılır. Bu kısımda 0-127 arasındaki değerler hata mesajlarını (128-255) arasındaki değerler bilgi mesajlarını göstermektedir[13]. Code(Kod)(1 byte), Tip alanında verilen hata veya bilgiye dair daha detaylı bilgi içerir. Örneğin tip alanında bir hata mesajı döndü ise bu hatanın sebebinin ne olabileceğine dair daha detaylı bilgi içerir [13]. Checksum(Sağlama)(2 byte), Diğer birçok paket başlığında da yer aldığı gibi paketin hedef noktaya ulaştığında herhangi bir bozulmaya uğrayıp

uğramadığını ortaya çıkarmak için kullanılır [13]. Aşağıdaki tabloda IANA'da belirtilen tip ve koduna göre bazı önemli ICMPv6 mesajları gösterilmiştir.

TİP	TİP AÇIKLAMASI	Kod ve Açıklaması
1	Hedefe ulaşılamıyor	0:Hedefe yönlendirme yok 1:Hedef ile iletişim yönetimsel olarak yasaklanmış
2	Paket çok büyük	0: Alıcı tarafından reddedildi
3	Zaman aşımı	0: Hop Limit sınırı aşıldı 1: Fragment parçalarının yeniden birleştirme zamanı aşıldı
4	Parametre hatası	0:Hatalık başlık alanı ile karşılaşıldı 1:Tanınmayan sonraki başlık alanı ile karşılaşıldı 2:Tanınmayan IPv6 seçeneği ile karşılaşıldı
128	Yankı talep mesajı	0:Alıcı tarafından önemsenmez
129	Yankı cevap mesajı	0:Alıcı tarafından önemsenmez
133	Yönlendirici talep mesajı	0:Alıcı tarafından önemsenmez
134	Yönlendirici duyuru mesajı	0:Alıcı tarafından önemsenmez
135	Komşu keşif talep mesajı	0:Alıcı tarafından önemsenmez
136	Komşu duyuru mesajı	0:Alıcı tarafından önemsenmez
137	Yeniden yönlendirme mesajı	0:Alıcı tarafından önemsenmez
148	Sertifika yolu talep mesajı	0:Alıcı tarafından önemsenmez
149	Sertifika yolu duyuru mesajı	0:Alıcı tarafından önemsenmez

Şekil 3.5: IANA ICMPv6 Parametreleri [14]

4. KOMŞU KEŞFİ PROTOKOLÜ(NDP)

Bilindiği gibi IPv4 altyapısında ARP (Adress Resolution Protocol) IP ve MAC eşleşmesi yapıp IP adresi bilinen bir cihazın MAC adresini bulmaya ve komşulukları oluşturmaya yaramaktadır. IPv4 ortamında bu görevleri gerçekleştiren ARP isteği sorguları broadcast çalışmaktadır. IPv6'da ise bu görevler ve DAD ve NUD(Neighbor Unreachability Detection) gibi ek bazı işlerin yapılması için ise NDP protokolü tasarlanmıştır. NDP protokolü istek sorguları ise çoklu gönderim adresi ile çalışmakta ve RFC 4861'de tanımlanan görevleri şu şekildedir [9]:

- Yönlendirici keşfi
- Önek keşfi
- Parametre keşfi (Sıçrama limiti, MTU vb.)
- Otomatik adres yapılandırması
- Sonraki atlama tespiti

- Komşu erişilemezlik keşfi (NUD)
- Adres çakışma tespiti
- Yeniden yönlendirme

NDP bu görevleri yerine getirmek için 5 farklı ICMPv6 tabanlı mesaj tipi kullanmaktadır. Bu mesajlar yine RFC 4861'de şu şekilde adlandırılmaktadır [9]:

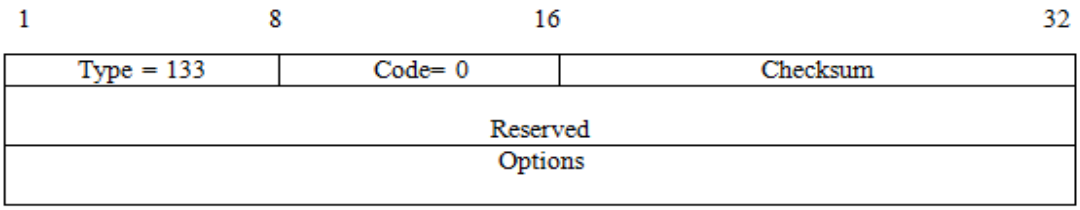
- Yönlendirici talep mesajı(RS)
- Yönlendirici duyuru mesajı(RA)
- Komşu talep mesajı(NS)
- Komşu duyuru mesajı(NA)
- Yeniden yönlendirme mesajı

Bu mesaj türlerine ait ICMPv6 tip numaraları önceki bölümlerde gösterilmiştir.

4.1 NDP Mesaj Türleri

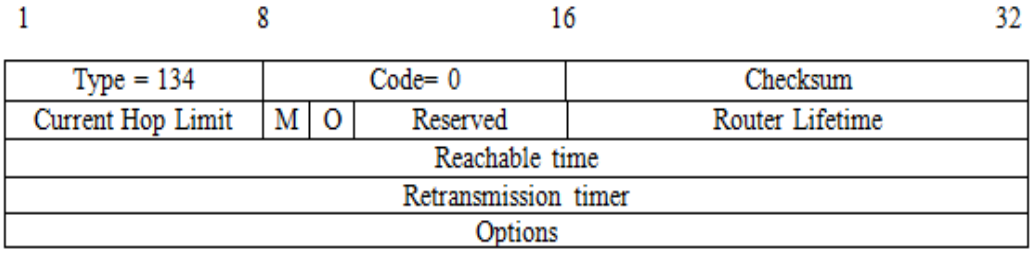
4.1.1 Yönlendirici Talep(RS) ve Duyuru Mesajları(RA)

İstemciler ağa bağlanmak ve IPv6 adresine sahip olabilmek için RS mesajları yayarak çevresinde bir yönlendirici ararlar, yönlendiriciler de gerek bu RS mesajlarına gerekse kendilerini bütün istemcilere bildirmek için periyodik olarak RA mesajları yayarlar. İstemcilerin yolladığı RS mesajları varış yeri adresi olarak yerel bağlantıdaki tüm yönlendiricileri gösteren çoklu gönderim adresini kullanırlar. Yönlendiricinin gönderdiği RA mesajında varış yeri adresi olarak ise yerel ağdaki bütün cihazları ifade eden çoklu gönderim adresi yer alır. Yönlendiriciler RA mesajları ile istemcilerin ihtiyaç duyduğu veya istediği önek, MTU vb. bilgileri istemcilere iletirler. RS mesaj başlığı aşağıda gösterilmiştir.



Şekil 4.1: Yönlendirici Talep Mesajı (RS) [9]

Bunun yanında RA mesaj başlığı da aşağıda gösterilmektedir.



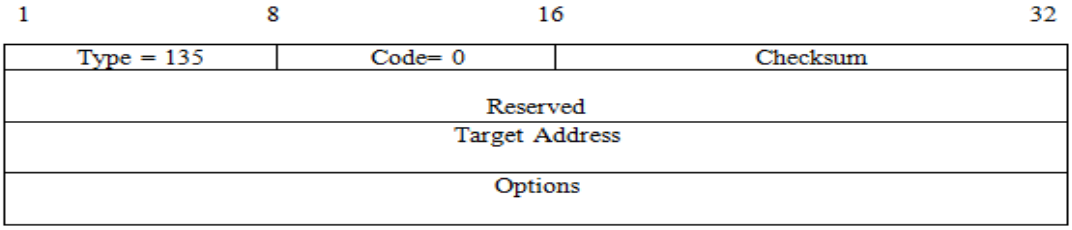
Şekil 4.2: Yönlendirici Duyuru Mesajı(RA) [9]

RFC 4861'e göre başlık bilgilerini şu şekilde özetleyebiliriz; Type(Tip), ICMPv6 tip 133 mesajın RS mesajı olduğunu, tip 134 RA mesajı olduğunu gösterir. Code(Kod), tip alanına dair detaylı bilgi içeren bu alan NDP mesajlarında sıfır değerini almaktadır. Checksum(Sağlama), mesajın sağlama değerini içeren 16 bitlik alandır. Reserved(Rezerve edilmiş),gelecekte doğabilecek ihtiyaçlar için rezerve edilmiş 16 bitlik değerdir. Alıcı tarafından ihmal edilen ve bütün bitleri sıfır olan alandır. Options(Seçenekler), RS veya RA başlığına eklenebilecek seçenekleri ifade etmektedir. NDP mesajlarında Target Link-Layer adress(Hedef Katman 2 Adres), Önek, MTU gibi seçenekler bu kısma örnek olarak gösterilebilir. Current Hop Limit(Mevcut Sıçrama Limiti), yönlendiriciye kaç sıçrama sonra erişilebileceğine dair bilgiyi içerir. Eğer yönlendirici bu kısımda bir şey belirtmemişse sıfır alınır [9].

M biti, istemcinin nasıl yapılandırılacağını gösterir. Bu bit 1 olursa istemciye DHCPv6 aracılığı ile durumlu yapılanması gerektiği söylenir. Sıfır ise istemciye yönlendiricinin gönderdiği önek bilgisine göre durumsuz IP numarasının yapılandırılması gerektiği söylenir. "O" biti, istemcilere durumlu olarak DHCPv6 sunucusundan alınması gereken başka bilgilerinde olduğunu göstererek istemcinin DHCPv6 ile iletişimini tetikler. Router Lifetime (Yönlendirici Hayat Süresi), alanı istemciye bu yönlendiricinin ne kadar süreliğine varsayılan yönlendirici olarak kabul edileceği bilgisi bildirilir. Eğer burası sıfır işaretlenmişse yönlendirici kendisinin varsayılan yönlendirici olmadığını ifade etmektedir. Reachable Time (Ulaşılabilir Süre),bir komşunun ne kadar süre ulaşılabilir varsayılacağının milisaniye cinsinden bilgisidir. Retransmission timer(Yeniden İletim Zamanlayıcısı), iki ardışıl NS mesajının arasında geçmesi gereken minimum sürenin milisaniye cinsinden değeridir [9].

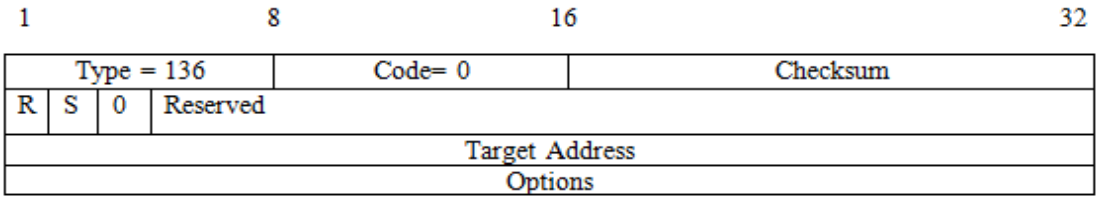
4.1.2 Komşu Talep(NS) ve Komşu Duyuru(NA) Mesajı

NS ve NA mesajları bir cihazın IP adresinden MAC adresini sorgulamak veya istenen MAC adresini sorgulayan istemciye iletmek için kullanılan komşu keşif mesajlarıdır. Bu anlamıyla IPV4'te ARP/RARP protokollerinin yaptığı işleri yaptığı söylenebilir. Bu adres çevirimi işleminin yanında adres çakışma tespiti(DAD) ve komşu erişilemezlik tespiti(NUD) için de kullanılmaktadır. Dolayısı ile NS mesajı çoklu gönderim, NA mesajı tekil gönderim adresler üzerinden çalışmaktadır. Aşağıda komşu talep mesaj yapısı gösterilmiştir.



Şekil 4.3: Komşu Talep Mesajı (NS) [9]

Bunun yanında aşağıdaki şekilde de komşu duyuru mesaj yapısı gösterilmiştir.



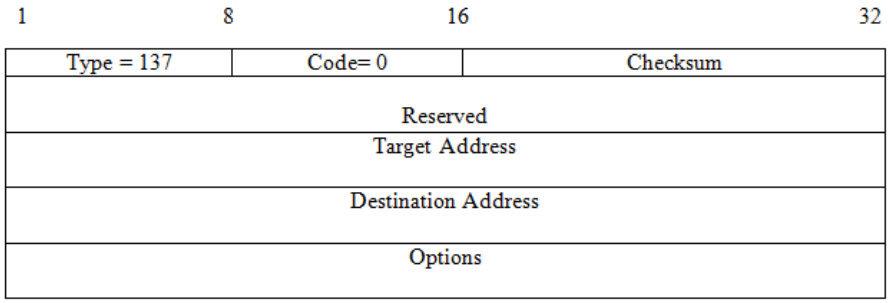
Şekil 4.4: Komşu Duyuru Mesajı (NA) [9]

Komşu duyuru mesajındaki alanlar şu şekilde özetlenebilir; Type(Tip) değeri NS mesajı için 135, NA mesajı için 136 değerini almaktadır. R(Router/Yönlendirici) biti, eğer bu bit 1 olarak işaretlenmişse gelen mesajın bir yönlendiriciden geldiği ifade edilmektedir. S(Solicitation/Talep) biti, eğer bu bit 1 olarak işaretlenmişse gelen mesajın bir NS mesajına cevap olarak gönderildiği ifade edilmektedir. Erişilebilirlik kontrollerinde gönderilen NS mesajlarına cevap olarak yollanan NA mesajlarında ayarlanır. O(Override/Geçersiz kılma) biti, 1 olarak ayarlandığında komşu önbelleğinde yer alan katman 2 adresinin güncelleştirilmesi, komşu önbelleğinin yenilenmesi gerektiğini ifade etmektedir. Eğer bu bir sıfır olarak ayarlanırsa komşu önbelleğinde var olan kaydın üstüne yazılmak yerine önbellekte yeni bir kayıt

oluşturulur [9]. Target Adress(Hedef Adres), katman 2 adresi sorgulanan IPv6 bağlantı yerel adresini belirtmektedir.

4.1.3 Yeniden Yönlendirme Mesajı

Bir istemci RS mesajı gönderdiğinde, ortamda birden fazla yönlendirici varsa, yönlendiricinin biri RA mesajı için kendisine gelen RS mesajını başka bir yönlendiriciye yeniden yönlendirme mesajı ile yönlendirebilir.



Şekil 4.5: Yönlendirme Mesajı (Redirect Message) [9]

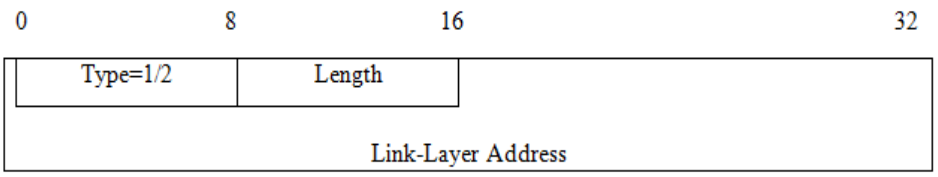
Burada Type(tip) alanında yer alan 137 sayısı mesajın bir yeniden yönlendirme mesajı olduğunu göstermektedir. Target Adress(Hedef Adres), paketin yönlendirildiği yönlendiricinin IPv6 adresini ifade etmektedir. Destination Adress(Varış Yeri Adresi) ise yönlendirilen paketin sahibini gösteren IPv6 adresini ifade etmektedir.

4.2 NDP Seçenekleri

ND süresinde RS/RA, NS/NA ve yeniden yönlendirme mesajlarında bir takım seçenekler kullanılmaktadır. Bu seçenekler aşağıda sırasıyla incelenmektedir.

4.2.1 Kaynak/ Hedef(Source/Target) Katman 2 Adresi

Bu seçenek genelde yeniden yönlendirme mesajının seçeneği olarak kullanılır [9]. İstemci bir NS mesajı ile yönlendirildiği yönlendiricinin katman 2 MAC adresini tekrar sorgulamasın diye, ilk yönlendirici tarafından MAC adresi istemciye bu seçenek ile bildirilir.

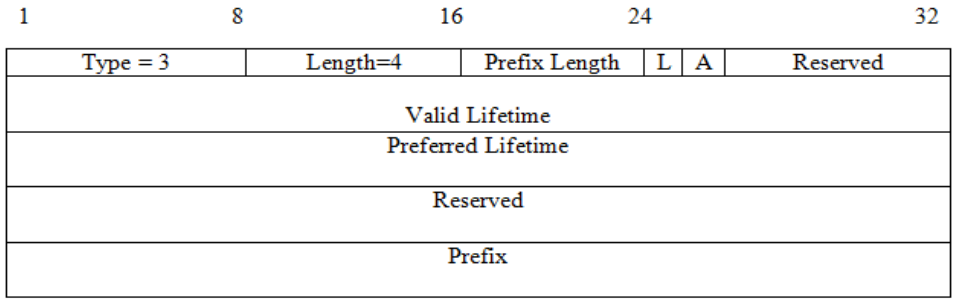


Şekil 4.6: Kaynak/Hedef Katman 2 Adres Seçeneği [9]

Burada; Type(Tip),kısmında 1 varsa kullanılan katman 2 adresinin bir kaynak adres olduğu, 2 varsa bir hedef adres olduğu ifade edilmektedir. Length(Uzunluk) alanı tip ve uzunluk alanları da dahil olmak üzere tüm kaynak/hedef katman 2 seçeneğinin uzunluğunu ifade eder.

4.2.2 Önek (Prefix) Seçeneği

Önek başlık yapısı aşağıda gösterilmiştir.



Şekil 4.7: Önek Başlığı [9]

RFC 4861'e göre Önek Seçeneği'nin alanları şu şekilde özetlenebilir[9]; Type(Tip): Bu alanın 3 olması bu başlığın bir önek başlığı olduğunu ifade etmektedir. Length(Uzunluk): Bütün önek başlığının uzunluğunu göstermektedir. Prefix Length(Önek Uzunluğu): Gönderilen önekin uzunluğunu göstermekte olan alandır.

L (Link/Bağlantı) Biti: Bu bitin 1 olarak ayarlanması gönderilen bu öneki istemci lokal networkünü belirlemek için kullanabilir anlamına gelmektedir. A(Autonameous/Otonom) Biti: Bu bitin ayarlanması gönderilen önekin durumsuz yapılandırma için kullanılabileceğini gösterir.

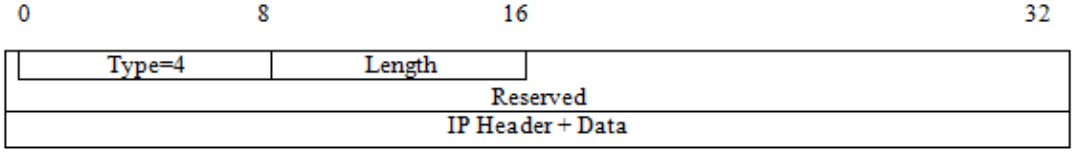
Valid Lifetime(Geçerli Hayat Süresi): L biti ayarlanmışsa bu alanda belirli bir süre belirtilir. Bu alan yerel ağ belirlenmesi için gönderilen önek bilgisinin geçerlilik süresini saniye cinsinden göstermektedir. Bu süre sonunda ya yönlendirici önek bilgisini yeniler veya istemci RS ile önek bilgisini ister.

Preferred Lifetime/Tercih Edilen Hayat Süresi): Gönderilen önek durumsuz adres üretmek için kullanılacaksa bu adres için tercih edilen geçerlilik süresi ifade eder.

Prefix(Önek): Yönlendiricinin istemcilere bildirdiği önek bilgisini ifade etmektedir.

4.2.3 Yönlendirilmiş Seçenek (Redirected Option)

Yönlendirilmiş Seçenek yapısı aşağıda gösterilmiştir.



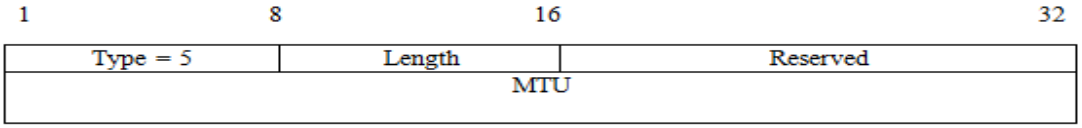
Şekil 4.8 : Yönlendirilmiş Seçenek[9]

Bu seçenek yeniden yönlendirme mesajında yer alır ve gönderilen paketi içerir. Type(Tip) =Bu alanın 4 olması bu başlığın bir yönlendirilmiş başlık olduğunu ifade etmektedir.

Length(Uzunluk) : Bu alan bütün başlığın uzunluğunu göstermektedir. IP Header(IP Başlığı) + Data**:** Başlıktaki bu alan ise yönlendiricinin başka bir yönlendiriciye yeniden yönlendirme mesajı ile yönlendirdiği paketi içermektedir [15].

4.2.4 MTU(Maximum Transmission Unit/Maksimum İletim Birimi) Seçeneği

MTU Seçeneği başlık yapısı aşağıda gösterilmiştir.



Şekil 4.9: MTU Seçeneği

Tip alanının 5 olması bu başlığın bir MTU başlığı olduğunu göstermektedir. MTU seçeneği RA mesajları içerisinde ağa gönderilip ağdaki istemcilerin MTU bilgisine sahip olmalarını sağlar [9]. RA mesajları ile bu değer bütün bağlantıya iletilir. İstemciler kendi aralarında MTU keşfi yaparsalar o zaman yine bu başlık ile MTU değeri gönderilir.

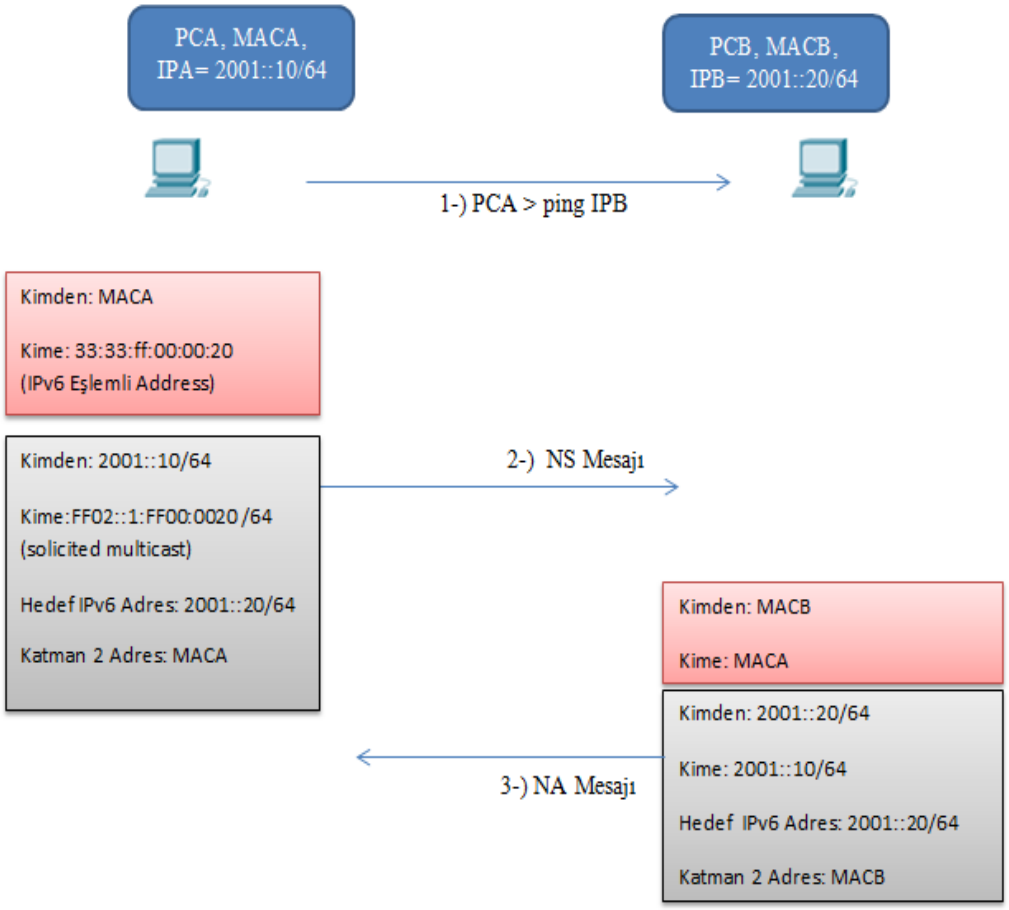
4.3 NDP Kullanım Alanları

Bu bölümde ND Protokolünün en fazla kullanılan uygulamaları işlenecektir. Bu uygulamalar Adres çözümleme, cihazların otomatik yapılandırılması, adres çakışma tespiti(DAD), komşu erişilemezlik tespiti(NUD), yönlendirici keşfi. Bunların bir

kısmına bir önceki bölümlerde kısaca değinilmiş olsa da bu bölümde daha detaylı işlenecektir.

4.3.1 Adres Çözümleme

Aynı ağdaki bir bilgisayar başka bir bilgisayar ile haberleşmek istediği zaman ilk önce kendi önbelleğinden haberleşmek istediği bilgisayarın MAC adresini sorgular. Eğer burada bir ilgili MAC adresi mevcut ise anahtarlar marifetiyle diğer bilgisayarla haberleşebilir. Yoksa ilk önce bu MAC adresini tespit etmesi gerekmektedir. Bunun için varış yeri adresi olarak solicited multicast adres yer almaktadır. Daha önce ifade edildiği üzere solicited multicast adresse sahip cihazlar bu çoklu adrese gelen cevapları dinlerler ve paket kime gelmişse o cevap verir. Ayrıca MAC adresi sorgulanmak istenen IPv6 bağlantı yerel adresi de gönderilen pakete hedef seçeneğine eklenerek burada belirtilir. Aşağıdaki şekilde adres çözümleme süreci özetlenmiştir.



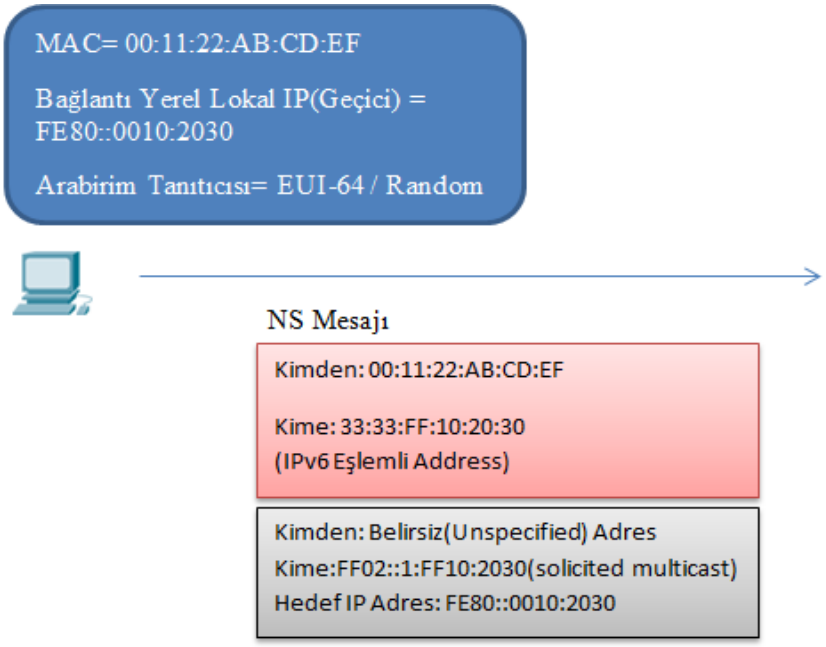
Şekil 4.10: NDP Adres Çözümleme

4.3.2 Adres Çakışma Tespiti (DAD)

Bir istemci bir arabirim tanıtıcısı ürettiği veya aldığı zaman bu adresin ağda başkaları tarafından kullanılıp kullanılmadığını bilmemektedir. Özellikle durumsuz adres yapılandırmalarında kullanılan IPv6 adresleri herhangi bir yerde tutulmadığı için bunu tespit etmek istemciye kalmıştır. İstemci bir IPv6'yı kullanmadan önce ağda böyle bir IPv6 olup olmadığını DAD süreci ile anlamaktadır. RFC 4861, bütün tekil gönderim adresler için (bağlantı yerel veya küresel adres olmasına bakılmaksızın) yapılandırmanın durumsuz veya durumlu olmasına bakılmaksızın (DHCPv6, SLAAC veya manuel yapılandırma olsa bile) DAD sürecinin her durumda istemcilere uygulanmasını önermektedir [4]. DAD süreci aşağıda özetlendiği şekilde işlemektedir.

- Kendi IPv6 adresini durumlu veya durumsuz olarak üreten bir istemci, bu adresi kullanmadan önce geçici olarak işaretler ve yerel ağına bir NS mesajı ile DAD isteğinde bulunur. İstekte kaynak adres olarak belirsiz adres yer almaktadır. Çünkü üretilen adres istemciye DAD sürecinden önce atanmamaktadır. Varış yeri adresi olarak da yine kendi ağdaki cihazları gösteren solicited multicast adres yer almaktadır. Yani bu mesaj bu gruptaki IP adreslerini dinleyen herkese gidecektir.
- Bu NS DAD mesajına eğer belli bir süre içerisinde cevap gelmezse, istemci bu IP adresinin başkası tarafından kullanılmadığı düşünüp kendisine atar ve kullanmaya başlar.
- Eğer bu IP adresi başka bir istemci tarafından kullanılıyorsa bu istemci bu adresi kullandığı bir NA adresi ile bildirir. Bu NA adresinde kaynak olarak kendi IP adresi, varış yeri olarak ise yine solicited adress yer alacaktır. Çünkü karşı tarafın daha IP adresi geçici olarak işaretlendiği için paketi kime göndereceğini bilmemektedir.
- Kendisine gelen NA mesajında kullanmak istediği IP adresinin başka bir istemci tarafından kullanıldığını gören istemci ise yeni bir IP adresi üretip süreci tekrarlayacaktır.

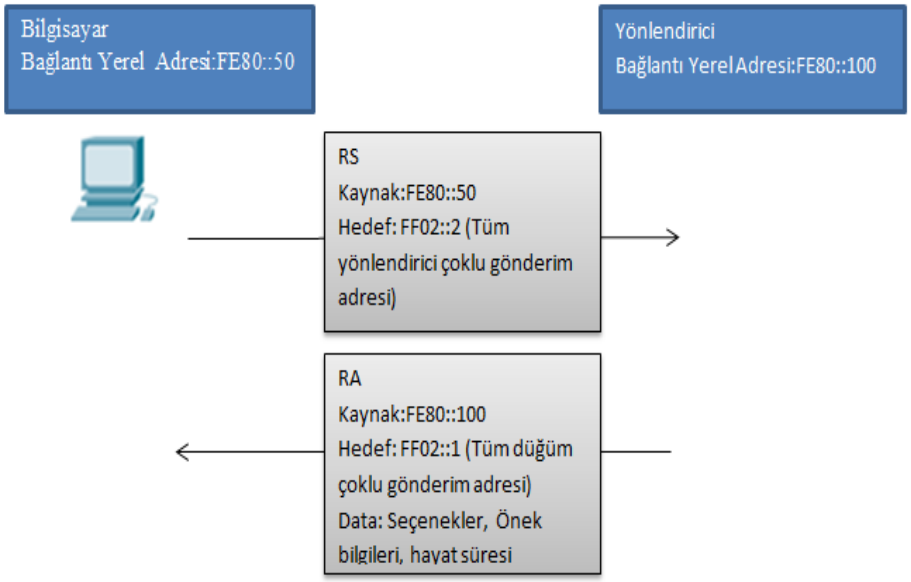
Yukarda anlatılan DAD sürecini özetleyen şekil aşağıda verilmiştir.



Şekil 4.11: NDP DAD Süreci

4.3.3 Yönlendirici Keşfi

Bir istemci bir ağa bağlanmadan önce o ağ ile ilgili önek bilgisi, IPv6 adresini nereden alacağı gibi bazı bilgilere sahip olması gerekir. İstemci bu bilgilere ortamda bulunan bir yönlendirici sayesinde sahip olur. İstemci yönlendirici aramak için ağa bir RS mesajı yayar. Ağdaki yönlendirici ise bu mesajı RA mesajı ile karşılık vererek istemciyi önek, durumlu veya durumsuz IP alması gerektiği vb. gibi konularda bilgilendirir. Bu süreç aşağıdaki şekilde özetlenmiştir.



Şekil 4.12: Yönlendirici Keşif Süreci

4.3.4 Komşu Erişilemezlik Tespiti(NUD)

Bu mesajın amacı ağa daha önce erişilmiş olan ve istemcinin önbelleğinde yer alan IP adresinin halen daha erişilebilir olup olmadığını tespit etmektedir [9]. İstemci bunun için ilgili IP adresine sahip cihaza bir NS mesajı yollar. Eğer cevap alamazsa o istemci ile alakalı bilgileri önbelleğinden siler. Cihazlar bu şekilde başka komşularına erişilebilirliği arada bir test etmektedirler.

4.3.5 Cihazların Otomatik Yapılandırılması

Daha önceki bölümlerde de anlatıldığı üzere NDP mesajları, istemcilerin durumsuz IP yapılandırılması kullanarak kendi kendilerine IP adresi üretmesi için kullanılmaktadır. Bu süreç şu şekilde özetlenebilir;

- Bir istemci ilk açıldığı zaman kendi bağlantı yerel adresini oluşturur.
- Ardından bu bağlantı yerel adresin ağda olup olmadığını anlamak için DAD sürecini başlatır.
- DAD sürecinde kendi IP adresi başkası tarafından kullanılmadığı anlaşıldığında bu adresi kullanarak RS mesajı ile ağda bir yönlendirici arar.
- Yönlendirici RA mesajı ile önek bilgisini ve otomatik yapılandırma ile adresini üretmesi gerektiğini istemciye iletir.
- İstemci kendisine elen önek bilgisine göre küresel tekil IPv6 adresini de random olarak üretir.
- Ürettiği küresel tekil adresi için de yeniden bir DAD süreci başlatır.

Şimdiye kadar işlenen konularda NDP sürecinin birçok aşaması ağ analizi açısından incelenmiştir. Bunun yanında güvenlik konularına değinilmemiştir. Aynı IPv4 ortamında ARP protokolünün saldırılara açık olması gibi NDP de doğası gereği bazı ataklara karşı zafiyet içermektedir. Bundan sonraki bölümlerden NDP' ye yönelik ataklara ve bu ataklara karşı alınabilecek önlemlere değinilecektir.

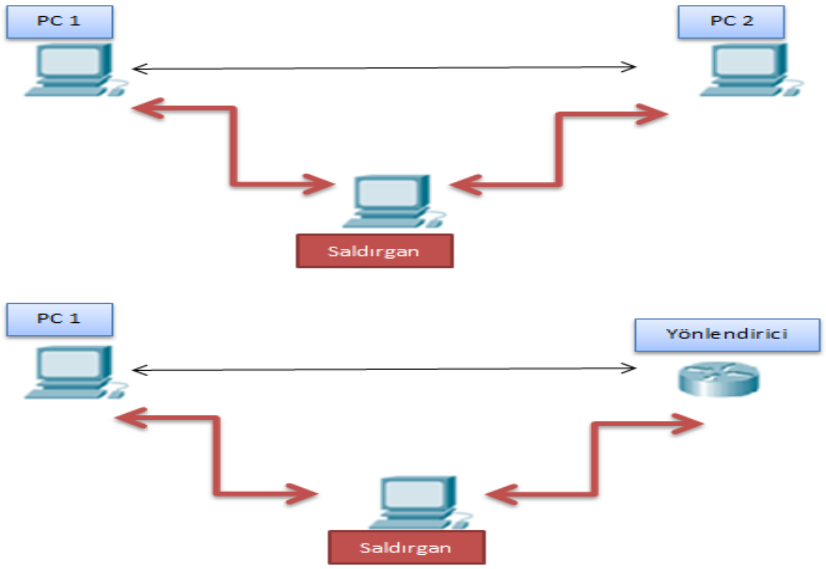
4.4 NDP'ye Yönelik Ataklar

NDP, ağda dolaşan paketleri şifrelemediği, verinin bütünlük kontrolü ve kimlik doğrulama gibi güvenlik önlemlerine sahip olmadığı için çeşitli saldırılara karşı

savunmasızdır. RFC 3756'de de tanımlanan NDP atakları [16] aşağıda sırasıyla incelenmiştir.

4.4.1 Komşu Sahtekarlığı

Saldırgan sahte NDP mesajları ile ağdaki başka birini taklit ederek istediği iki cihaz arasına girebilir. Böylelikle örneğin kendi MAC adresini kurbanın varsayılan ağ geçidinin MAC adresi gibi göstererek kurbanın trafiğinin kendi üzerinden geçmesine neden olabilir. Bu saldırı aslında bir ortadaki adam saldırısına örnektir ve IPv4 ortamında Arp sahtekarlığına karşılık geldiği düşünülebilir. Bu saldırının temel sebebi cihazlar arasındaki iletişimin şifresiz gitmesi ve bütünlük kontrolünün olmamasıdır. Aşağıdaki şekillerde bu saldırı iki farklı örnek ile gösterilmektedir.



Şekil 4.13: Komşu Sahtekarlığı

4.4.2 DAD DOS Atakları

DOS ataklarındaki temel mantık kurbanın kaynaklarını tüketerek yapmak istediği yapmasına engel olmak olarak açıklanabilir. Bu ataklara DAD DOS atağı örnek olarak verilebilir. DAD DOS atağını açıklamak gerekirse, bir istemcinin bir IP aldığında DAD süreci ile bu IP adresinin ağda kullanılıp kullanılmadığını kontrol etmekte olduğu belirtilmişti. Bu işlem gerçekleştirilirken eğer saldırgan kendisine gelen DAD NS mesajlarına "bu IPv6 adresini ben kullanıyorum" diye DAD NA mesajı ile cevap dönerse istemci yeniden IP adresi üretip bu süreci tekrar etmek zorunda kalacaktır.

Kendisine gelen her NS DAD isteğine sahte bir NA DAD isteği dönen saldırgan kurbanın IP almasına ve ağa bağlanmasına engel olabilir. Bu atağın gerçekleştirilebilmesinin temel sebebi gelen DAD NA mesajlarının istemci tarafında doğrulanamamasıdır.

4.4.3 Sahte RS/RA Mesajı Atakları

Bu ataklar birkaç çeşit olarak işlenebilir. Bunların ilki saldırganın bir yönlendirici gibi davranıp sahte RA mesajları ve önek bilgisi yollamasından kaynaklanır. Bu önek bilgisine göre IP adresini üretecek olan istemci DAD sürecini işlettiğinde de kendisine herhangi bir cevap almayacağı için bu IP adresini kullanmaya başlar fakat ağdaki diğer bilgisayarlarla haberleşemez, yönlendirici üzerinden internete çıkmak zorunda kalabilir veya internete hiç çıkamayabilir.

Diğer bir RS/RA mesajı saldırısında, saldırgan istemcilere gönderdiği RA mesajlarında önek hayat süresi kısmını sıfır olarak ayarlar ve kısa periyodik aralıklarla bu mesajı tekrarlarsa bu mesajı alan istemciler küresel tekil IP adreslerini ürettikten sonra bu önekin süresinin sıfır olduğunu düşünüp kullanamayacaklardır. Yani bu durumda istemciler sadece yerel ağda çalışabileceklerdir.

Bunun yanında bir diğer RS/RA atağına ise farklı öneklere sahip periyodik RA mesajlarının istemcilere gönderilmesi örnek olarak verilebilir. Bu durumda istemciler kendilerine gelen farklı önek bilgilerine göre IP adreslerini yeniden üretmek zorunda kalacak ve bu da istemcinin kaynak tüketimine sebep olabilecektir. Bu atak bir DOS atağı gibi de düşünülebilir.

Bu ataklarda ki ortak problem ise yönlendiriciden gelen RA mesajlarının doğruluğunun, bir diğer ifadeyle yönlendiricinin güvenilirliğinin istemci tarafında doğrulanmamasıdır.

4.4.4 Yeniden Yönlendirme Atakları

Saldırgan istemcilerin kullandığı yönlendiricinin IP adresinden geliyormuş gibi bir RA mesajı üreterek kurbana gönderir. Bu paket içerisinde yer alan yeniden yönlendirme başlığında kurbanın bundan sonraki varsayılan ağ geçici yazar. Bu yeniden yönlendirme mesajı ile istemciye “artık şu yönlendiriciyi kullan” şeklinde bir istek yollanmış olur. Kurban bu mesajı kabul ettikten sonra artık yönlendirici olarak yeniden yönlendirme mesajında gönderilen yönlendiriciyi kullanmaya başlar. Kurban

kendisine gelen mesaj içerisinde kaynak IP adresi olarak kendi yönlendiricisinin IP adresini gördüğü için bu yeniden yönlendirme paketini kabul eder [17]. Bu atağın gerçekleştirilebilmesinin temel sebebi istemcinin kendisine gelen bütün RA paketlerini kabul etmesi, yönlendiriciyi bir şekilde doğrulayamamasıdır.

4.4.5 Yeniden Yayınlama Atakları

Yeniden yayınlama ataklarında saldırgan iki istemci arasındaki trafiği dinleyip değiştirebilir. Örneğin PC1, PC2 ile haberleşmek istediğinde PC2'nin MAC adresini öğrenmek için bir NS mesajı yollar. Kurban ise araya girip bu istekleri dinleyerek değiştirip trafiğin kendi üzerinden akmasını sağlayabilir. Aslında bu da bir ortadaki adam saldırısına örnek olarak gösterilebilir. Saldırgan bu saldırıyı RA mesajlarını yeniden yayımlayarak ederek de yapabilir. Yönlendiriciden aldığı RA mesajlarının parametrelerini değiştirerek yerel ağa yollayabilir [18]. Yeniden yayınlama ataklarında temel mantık gelen mesajların parametrelerinin değiştirilerek hedefe gönderilmesidir. Bu atakların yapılabilmesinin temel sebebi yine araya birilerinin girebilmesidir.

4.4.6 Birleşik Ataklar

Bu ataklar yukarı da yazılan atakların birden fazlasının bir araya getirilip gerçekleştirilen senaryoları içermektedir. Örnek olarak sahtekarlık ve DOS atağı beraber kullanılabilir. Saldırgan sahte kaynak IP'lere sahip paketler üreterek DOS atağı gerçekleştirebilir[19].

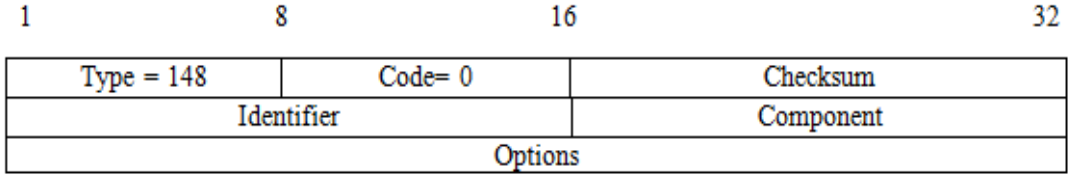
5. GÜVENLİ KOMŞU KEŞFİ (SEND)

IPv6 ND protokolündeki zafiyetlere yönelik ataklara karşı önlem alabilmek için kimlik doğrulama, istemcinin sahip olduğu adresi kanıtlaması, mesajların bütünlüğünün sağlanması ve yönlendiricilerin yetkilendirilebilmesi gibi çeşitli önlemlerin alınması gerekmektedir. Bu noktada bu işlemleri gerçekleştiren bir mekanizma, güvenli komşu keşfi (SEND), RFC 3971'de tanımlanmıştır. RFC 3971'de SEND için 4 yeni başlık yapısı ve 2 farklı mesaj tipi tanımlanmaktadır. Bunlar; CGA, RSA imza, Tek seferlik değer(Nonce) ve zaman damgası(Timestamp) seçenekleri ile, CPS(Certification Path Solicitation) ve CPA(Certification Path Advertisement)

mesajlarıdır. CPS ve CPA mesajları da kendi içerisinde TA ve Sertifika seçeneklerini kullanmaktadır.

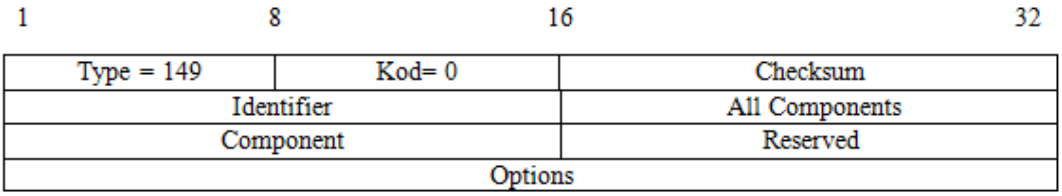
5.1 SEND Mesajları

SEND ile gelen CPS ve CPA mesajları başlık yapıları RFC 3971' e göre aşağıdaki gibi tanımlanmaktadır. CPS başlık yapısı aşağıda gösterilmiştir.



Şekil 5.1: Sertifika Yolu İstek Mesajı(CPS) [20]

Bunun yanında CPA başlık yapısı da aşağıdaki şekilde gösterildiği gibidir.



Şekil 5.2: Sertifika Yolu Duyuru Mesajı (CPA) [20]

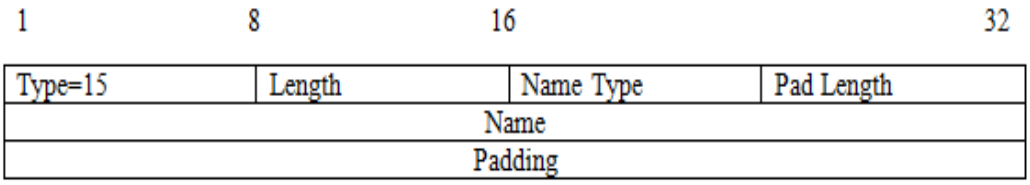
Tip, Kod, Rezerve alanlarının ne ifade ettiği daha önce açıklanmıştı. ICMPv6 paketinde tip 148 mesajın bir CPS mesajı olduğunu, tip 149 mesajın bir CPA mesajı olduğunu ifade etmektedir. Bunun yanında mesajlarda yer alan diğer alanlar şu şekilde açıklanabilir;

Identifier(Tanımlayıcı): CPS ve CPA mesajlarının eşleşmesini sağlayan bir değerdir. Her iki seçenekte de aynı değere sahiptir.

Component(Bileşen): İstemcinin ilgilendiği sertifika yoluna bir dizin sağlamaktadır. Yani istemci "ben şu sertifika yolu ile ilgileniyorum" şeklinde bir mesaj yollamaktadır. İstemci güvendiği TA sunucusuna ait bilgileri içeren TA seçeneğini de ekleyebilir. Bu durumda istemci kendisinin sertifika yoluna güvenmesi için ilgili sertifika yolunun bu TA ile imzalanmış olması gerektiğini bildirir. Bu alan CPS mesajında da CPA mesajında da mevcuttur. CPA mesajında yer aldığında sertifika seçeneği ile gönderilen sertifikanın sertifika yolundaki dizinini göstermektedir. Yani hangi sertifika yolundaki sertifikanın gönderileceğini istemciye bildirir [21].

All Component(Bütün Bileşenler): Bu alan TA sunucu bilgisine kadar uzanan tüm sertifika yolundaki toplam sertifika sayısını göstermektedir. CPA mesajı bir veya birden fazla sertifika yolunu ve o sertifika yolundaki sertifikaları istemcilere göndermek için kullanılmaktadır. Sertifikaları göndermek için sertifika seçeneği CPA mesajına ek olarak gönderilir. [21]

Options(Seçenekler): CPS mesajına TA seçeneği, CPA mesajına ise TA seçeneği ve sertifika seçeneği gelebilmektedir. Bu seçeneklerden ilki TA seçeneğinin başlık yapısı RFC 3971'e göre aşağıda gösterilmiştir.



Şekil 5.3: TA(Trust Anchor) Seçeneği [20]

Başlık yapısı gösterilen TA seçeneği, sertifika yolu ile ilgili isim bilgilerini içermektedir. Başlık yapısındaki her bir alanın kısa açıklaması aşağıda gösterildiği gibidir.

Name Type(İsim Tipi): Bu alan Name(İsim) alanında yer alacak ismin türünü bildirmektedir. İki çeşit olabilir. Buraya 1 gelirse isim türünün DER ENCODED X.501 olduğunu 2 gelirse FQDN(Fully Qualified Domain Name) türünde olduğunu bildirmektedir [20].

Name(İsim): Bu alanda TA sunucusunu gösteren isim, İsim Tipi alanında belirtilen formatta yer alır. Örneğin İsim Tipi kısmı "2" olarak ayarlandıysa buraya TA sunucusunun FQDN isim karşılığı gelir. Buna örnek olarak "Trustanchor.example.com" vb. verilebilir [20].

Pad Length(Dolgu uzunluğu): Uzunluk alanında belirtilen başlık uzunluğunu tamamlayacak şekilde gelmesi gereken oktet sayısını belirtmektedir. Gönderici ve alıcı tarafından dikkate alınmayan sıfırlardan oluşur [20].

CPA mesajına gelebilecek bir diğer seçenek olan sertifika seçeneği başlık yapısı RFC 3971'e göre aşağıda gösterilmiştir.

Şekil 5.4: Sertifika Seçeneği [20]

Sertifika seçeneği CPA mesajı ile bilgisayarlara gönderilen sertifikaları içeren başlıktır. Bir sertifika yolu göstermek için tek bir sertifikaya sahiptir. [21]. Sertifika seçeneği başlık yapısında gösterilen alanların açıklamaları özet olarak aşağıdaki gibi ifade edilebilir.

Cert Type(Sertifika Tipi) : Bu alanda sertifika alanında ne tür bir sertifika olduğunu göstermektedir. Şu an için tek bir yasal sertifika türü olan X.509.v3 sertifikasını göstermek için bu alana "1" değeri gelmektedir [20].

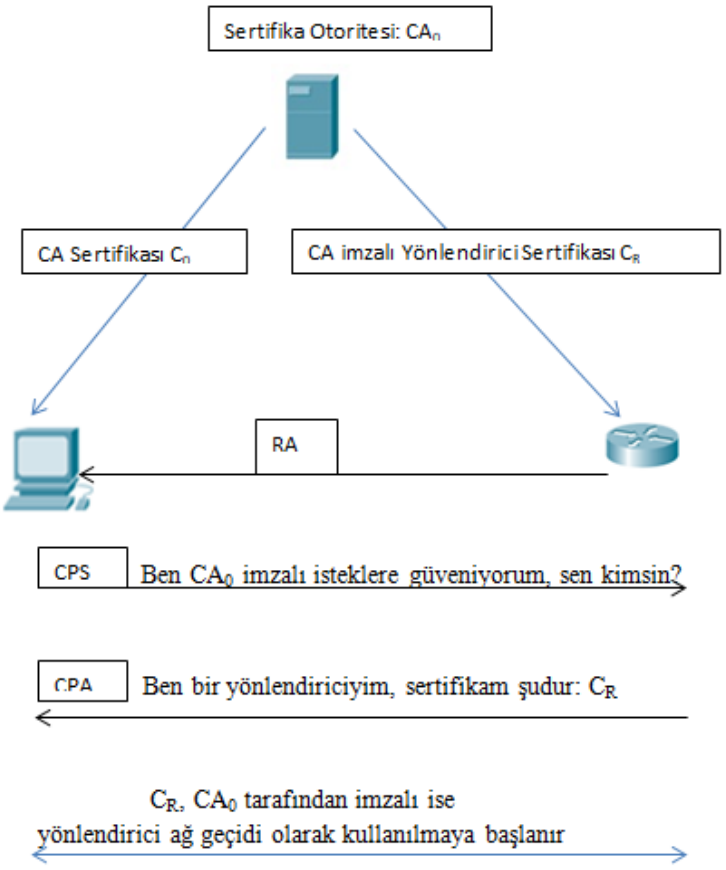
Certificate(Sertifika): Sertifika tipi alanı 1 olarak ayarlandığında bu alan bir X.509v3 sertifikası içermektedir [20].

SEND yapısında kullanılan CPS ve CPA mesajları ve bunların seçenekleri kullanılarak sahte yönlendirici ve sahte RS/RA ataklarına karşı önlem alınabilmektedir. Bu önlem temelde RA mesajı gönderen yönlendiricilerin sertifikalarının güvenilir olup olmadığının teyit edilmesi ve paketin ona göre kabul edilip edilmemesini ifade etmektedir. Bu yönteme yetkilendirme delegasyon keşfi (ADD) denilmektedir. Şekil 5.5'te ADD süreci gösterilmiştir ve şu şekilde özetlenebilir.

- İstemciler yalnızca güvenilir bir sertifika otoritesi tarafından imzalanan sertifikalara güvenmektedirler.
- Bir yönlendirici istemcilere RA mesajı yolladığında istemci yönlendiricinin sertifikasının kendi güvendiği sertifika otoritesi tarafından imzalanıp imzalanmadığına bakar
- Bir yönlendirici RA mesajı yaydığında, bilgisayar "Ben şu TA sunucusuna güveniyorum, sen kimsin, sertifika yolunu gönder" şeklinde CPS mesajı yollar
- Yönlendirici CPA mesajı ile sertifika zincirini ve sertifika yolunu gönderir

- Bilgisayar bu sertifika zincirini adım adım kontrol eder, zincirin herhangi bir noktasında imza hatası varsa RA mesajını düşürür, sertifika zincirinde herhangi bir hata yoksa RA mesajını kabul eder.
- Eğer sertifika yolundaki sertifikalar geçerli x.509 imzasına sahipse istemci bu yönlendiriciyi güvenilir kabul eder ve bu yönlendiriciden gelen paketlere güvenir. Güvenilir bir sertifika otoritesi tarafından imzalanmamış paketlere ise güvenmeyecek ve böylelikle yönlendiriciler üzerinden gelebilecek olan saldırılara karşı önlem alınabilecektir.

Bunun yanında ADD sürecinde DOS ataklarına maruz kalınmaması için sertifika yolu bilgisayarlarda depolanmadan evvel doğrulanmalı. Çünkü doğrulanmadan depolanırsa DOS ataklarına açık hale gelir. Bir saldırgan bir bilgisayara doğrulayamayacağı sertifikalar göndererek o bilgisayarın hafızasının dolmasına sebebiyet verebilir [20].



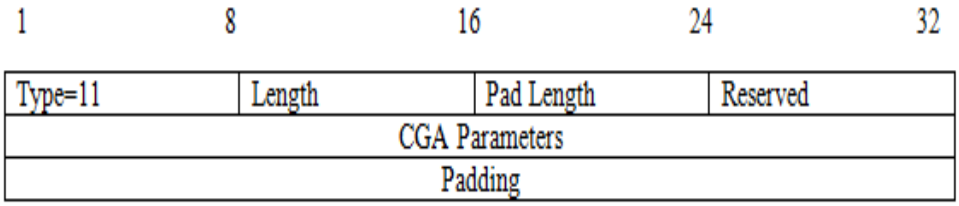
Şekil 5.5: ADD Süreci

5.2 SEND Seçenekleri

ND protokolünü güvenli hale getirmek için SEND ile birlikte 4 farklı seçenek tanımlanmıştır. Bu seçenekler aşağıda incelenmiştir.

5.2.1 CGA (Cryptographically Generated Address) Seçeneği

CGA, adres hırsızlığının yani bir saldırganın bir istemcinin adresini taklit etmesinin önüne geçmek için kullanılan tahmin edilip kırılması zor bir algoritmaya göre üretilip istemcinin özel anahtarı ile imzalandıktan sonra hedefe yollanan paketlerde kullanılan kriptografik IPv6 adreslerini ifade etmektedir. Bu adresler ve istemcinin özel anahtarı ile paketin hedef adrese bozulmadan gitmesi sağlanmaktadır. Bir diğer ifadeyle CGA, istemcinin özel anahtarı ile beraber mesajların bütünlük kontrolünde kullanılmaktadır. CGA seçeneği ise CGA parametrelerinin alıcı tarafa taşınması için kullanılmaktadır. Alıcı taraf bu parametreleri kullanarak üretilen adresin doğru üretilip üretilmediğini, yani kendisine gelen adresin gerçek bir adresten gelip gelmediğini kontrol edecektir. Başlık yapısı aşağıda gösterilmektedir.

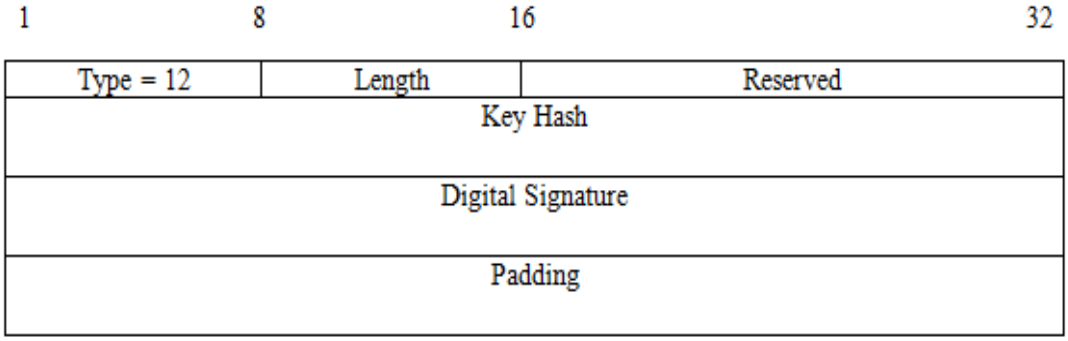


Şekil 5.6: CGA Option [20]

Bu başlık yapısında gösterilen bölümleri açıklamak gerekirse; Tip=11 başlığın bir CGA tanımladığını; Uzunluk, CGA başlık yapısının toplam uzunluğunu; Dolgu Uzunluğu(Pad Length), dolgu kısmının uzunluğunu gösteren; Dolgu(Padding), başlık yapısını tamamlamak için konulan sıfırlardan oluşan kısımdır.Alıcı tarafından ihmal edilmektedir. CGA Parametreleri ise Genel anahtar, Niteleyici(Modifier), Alt ağ öneki, CC(Collision Counts/Çarpışma sayısı) değerleri olup, CGA üretilmesi ve doğrulanmasında kullanılan parametreleri ifade etmektedir [20].

5.2.2 RSA İmza Seçeneği

SEND'de göndericinin kimliğinin doğruluğunun ispatı için RSA imza seçeneği kullanılmaktadır. Her cihaz kendi RSA genel/özel anahtar çiftlerini üretir. Genel anahtar CGA üretiminde, özel anahtar ise ND mesajlarının imzalanmasında kullanılmaktadır. Özel anahtar ile imzalama işlemi saldırganların iki cihaz arasına girip NP mesajlarının aldatılmasını engellemektedir. RSA imza seçeneğinde, gönderilecek olan her ND mesajının RSA imzası taşınmaktadır [15]. Aşağıda bir RSA imza seçeneğinin yapısı gösterilmiştir.

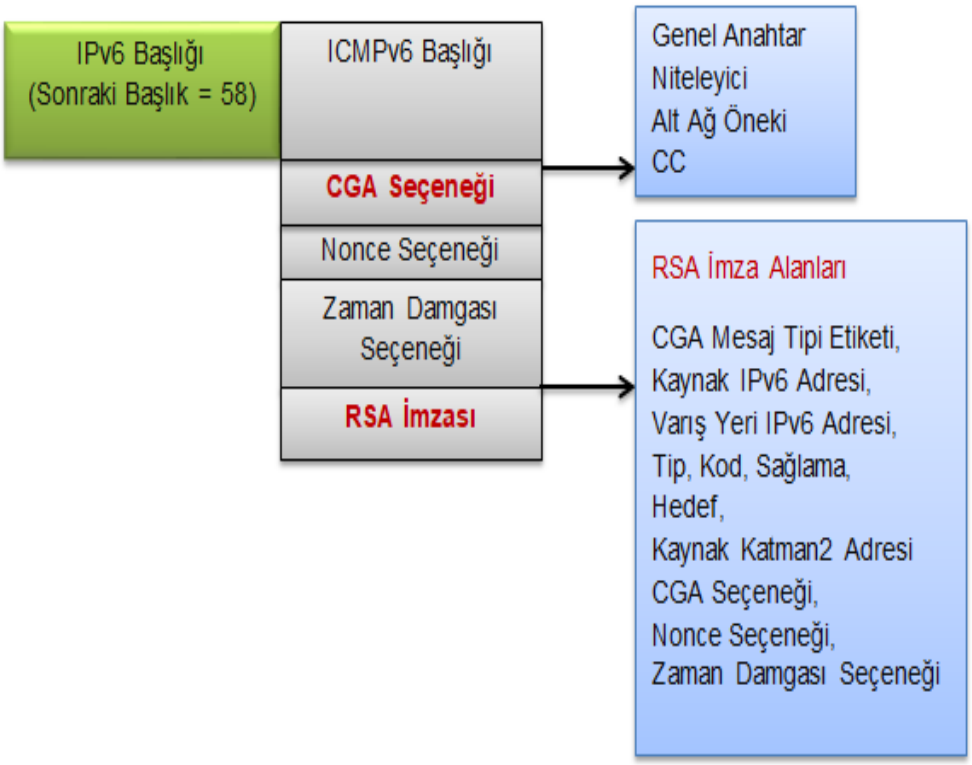


Şekil 5.7: RSA İmza Seçeneği [20]

Bu seçenekte gösterilen Digital Signature(Dijital imza) alanında göndericinin dijital imzası yer almaktadır. Key Hash(Anahtar Hash değeri) değeri ise imza oluşturulurken kullanılan genel anahtarın sha-1 hash değerinin soldan 128 bitlik kısmını içermektedir[21]. RFC 3971'e göre özel anahtar ile imzalanan alanlar şu şekilde ifade edilebilir [20]:

- CGA Message Type Tag(CGA Mesajı Tip Etiketi)
- ICMPv6 başlığında Tip, Kod ve Sağlama alanları
- ICMPv6 başlığında Sağlama alanından sonraki ND seçeneklerine kadar olan kısım (Hedef ve Kaynak Katman 2 adresi gibi)
- IPv6 başlığında kaynak ve varış yeri IPv6 adresi

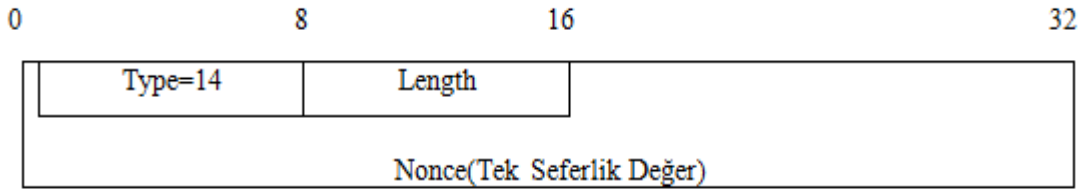
CGA, Tek Seferlik Değer, Zaman Damgası seçeneği de dahil RSA seçeneğinden önceki bütün ND seçenekleriBurada CGA Mesaj Tip Etiketi değeri aynı anahtarı kullanan başka protokol mesajları ile bir çakışma yaşanmaması için kullanılan, IANA tarafından tahsis edilen 128 bitlik bir değerdir [22]. Bu imza alanlarını aşağıdaki şekilde daha detaylı olarak görebiliriz.



Şekil 5.8: CGA parametreleri ve RSA imza Alanları

5.2.3 Tek Seferlik Değer(Nonce) Seçeneği

Nonce seçeneği duyuru ve talep mesaj çiftlerinin sırasını belirlemede kullanılan rastgele bir değerdir [23]. Bir NA mesajının, bir NS mesajına çok yeni bir cevap olduğunu göstermek için kullanılır. Bir NS mesajında yer alan Nonce değerinin aynısı bu NS mesajına giden NA mesajında da yer alır. Böylelikle NS ve NA mesajlarının eşleşmesi sağlanır.

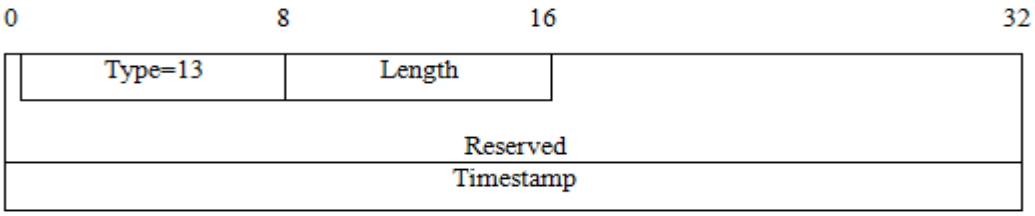


Şekil 5.9: Nonce Seçeneği [20]

Burada gösterilen Nonce alanı en az 6 byte uzunluğunda rasgele bir değer içermektedir. Mesajların arasına giren birisi Nonce değerini çok kısa sürede tutturması güç olduğu için potansiyel yeniden yayınlama ataklarına karşı koruma sağlamaktadır.

5.2.4 Zaman Damgası Seçeneği(Timestramp)

Zaman damgası seçeneğinin amacı, istenmeyen duyuruların ve yönlendirmelerin tekrar yayınlanmadığından emin olmaktır [20]. Kısacası istenmeyen duyuru ve yönlendirme çoklu gönderme adresleri ile gelen yeniden yayınlama ataklarına karşı koruma sağlar. Mesajı gönderen cihaz tarafından bilinen gün saatini içerir. Bu anlamda SEND'e yönelik yeniden yönlendirme ataklarına karşı koruma sağlamaktadır. Aşağıda yapısı gösterilen Zaman Damgası Seçeneğinde, Zaman Damgası alanının ilk 48 biti, 1 Ocak 1970 00:00 UTC zaman diliminden beri geçmiş zamanı saniye cinsinden göstermektedir. Geri kalan bitler ise bir saniyenin (1/64K) kesirli haliyle tutulmasını sağlamaktadır [21].

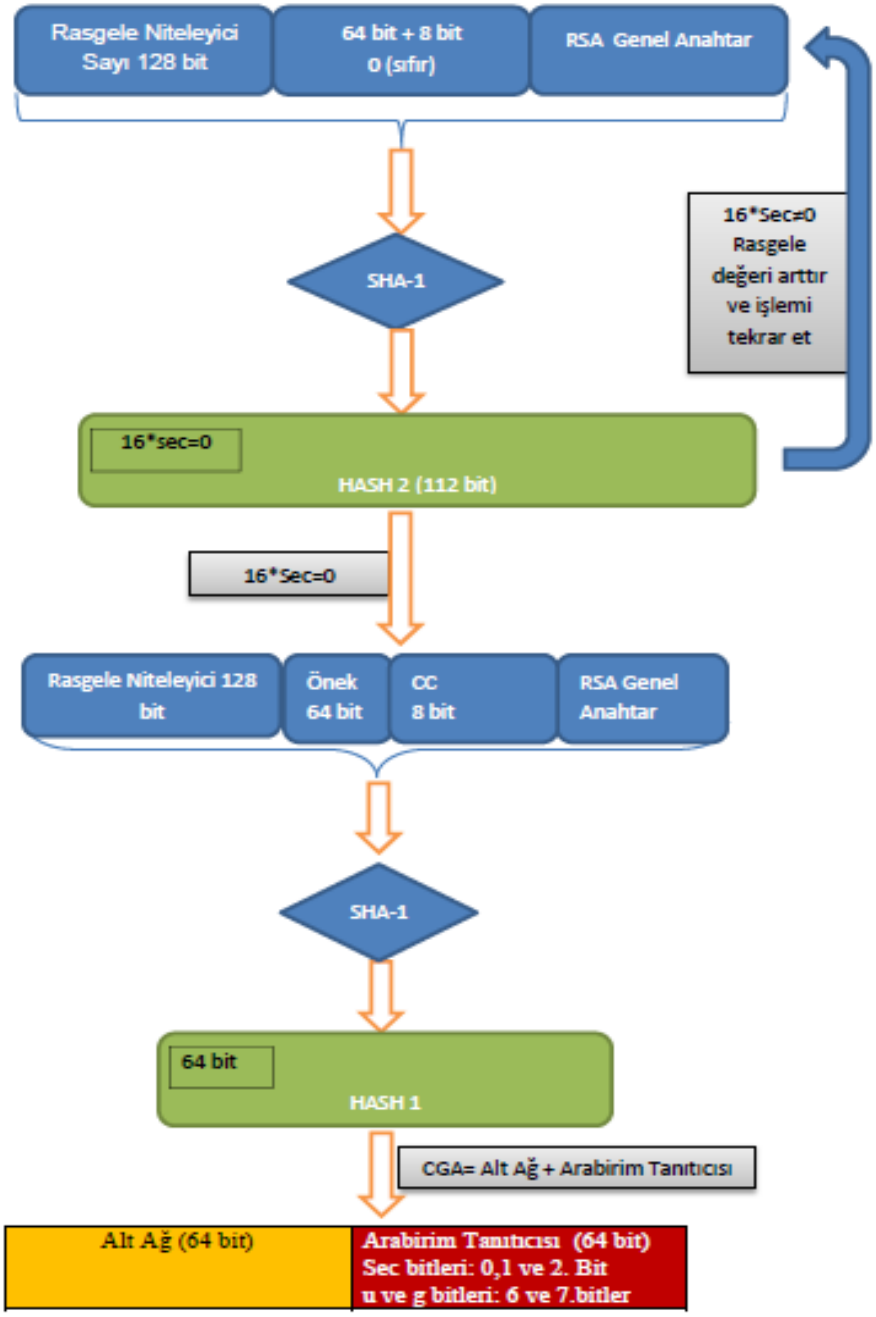


Şekil 5.10: Timestamp Option [20]

5.3 SEND Süreci

5.3.1 CGA Üretimi

CGA üretim sürecini aşağıdaki şekil ile özetlenmektedir. Üretim sırasında kullanılan Rasgele değer bilgisayar tarafından üretilir. RSA anahtarları ise bilgisayara ürettirilebilir veya başka bir ortamda üretilip bilgisayara yüklenebilir.



Şekil 5.11: CGA Üretim Algoritması

Şekilde anlatılmaya çalışılan CGA üretim aşaması RFC 3972'ye göre adım adım aşağıdaki gibi gerçekleşmektedir [22] :

1- İşletim sistemi tarafından bir SEC değeri seçilir. SEC değeri (0-7) arasında olabilecek şekilde tasarlanmış olup işletim sistemleri tarafından tanınmaktadır.

2- Gönderici tarafta işletim sistemi tarafından 128 bitlik bir rasgele bir sayı üretilir. Rasgele sayının yanında RSA genel/özel anahtar çifti de üretilmeli

veya işletim sistemine bir yerden sağlanmalıdır. Genel anahtar CGA üretiminde, özel anahtar ise CGA'nın kullanılmadan önce imzalanmasını sağlamaktadır.

3- 128 bit rasgele sayı değeri, 72 bit sıfır (64 bit önek alanı, ardından 8 bit CC alanı yerine) ve bilgisayarın RSA Genel Anahtarı(DER-Encoded) yan yana koyularak ortaya çıkan değerin SHA1 algoritmasına göre Hash değeri alınır. Bu hash, HASH2 olarak adlandırılır.

4- Ortaya çıkan HASH2 değerinin yalnızca soldaki 112 biti alınır. Bu değerin son 16*SEC kadar bit sayısı sıfır ile karşılaştırılır. Sıfıra eşitse diğer aşamaya geçilir. Eşit değilse rasgele sayı değeri bir arttırılarak işlem tekrar edilir. Bu işlem 16*SEC kadar bitin sıfır olmasına kadar devam eder. Dolayısı ile bu süre. CGA üretiminde en çok zaman gerektiren işlem yoğunluğunun fazla olduğu süreçtir. Bu süreçteki iyileştirmeler CGA üretim süresini kısaltacaktır.

5- CC değeri sıfıra ayarlanır.

6- Bir sonraki adımda en son kullanılan rasgele sayı, 64 bit önek, 8 bit CC ve bilgisayarın RSA genel anahtarı(DER-Encoded), ve uzantı alanları varsa o da yan yana konularak, yani CGA parametleri yan yana konularak bu değerin SHA1'e göre hash değeri alınır ve çıkan sonuç HASH1'dir.

7- Elde edilen Hash1 değerinin soldaki 64 biti alınır ve önekin yanına arabirim tanıtıcısı olarak konulur. Arabirim tanıtıcısı ilk üç biti SEC değerleri ile değiştirilir. Çünkü SEC değerinin karşı tarafa gönderilmesi gerekmektedir. Bunun yanında U ve G bitleri ilgili değerlerine set edilir. Arabirim tanıtıcısının ilk byte değerinin son iki biti sırasıyla U ve G bit olarak bilinmektedir. U biti küresel/yerel(universal/local) biti olmakla beraber ayarlandığında adresin yerel olarak yönetildiği anlamına gelmektedir. G bit grup biti olarak bilinmektedir ve ayarlandığında ilgili adresin bir grup adresi veya çoklu gönderim adresi tipinde olduğunu da bildirmektedir [21].

8- Bu şekilde bilgisayarın CGA'sı hesaplanmış olur.

9- Ardından üretilen CGA'nın ağda kullanılıp kullanılmadığının kontrolü için DAD süreci başlar. DAD süreci sonunda eğer çakışma meydana gelirse CC değeri 1 arttırılarak HASH1 ve arabirim tanıtıcısı yeniden hesaplanır ve tekrar DAD süreci çalışır. CC değeri en fazla 2'ye kadar çıkabilir. 3 kereden daha fazla

çakışma meydana gelmesi demek CGA üretimi yapan cihaza, ortamda bir saldırı olma ihtimalini düşündürecek ve üretimi durdurup kaynak tüketiminin önüne geçecektir.

CGA üretimi sırasında HASH2 değerinin hesaplanmasının sebebi kaba kuvvet saldırılara karşı CGA'yı güçlendirmektedir. Önek zaten içerdeki bir saldırgan tarafından tahmin edilebileceği veya bilineceği için aslında CGA'nın kaba kuvvet saldırılarına karşı dayanığı 2^{64} kabul edilebilir. Çünkü IPv6 ID kısmı 64 bittir. Bu 64 bitin ilk üç biti SEC değerini ifade etmek için kullanılmaktadır. SEC değeri buraya yazılıp karşı tarafta doğrulama için kullanılır. Dolayısı ile SEC değeri bilinmektedir. Bunun yanında U ve G bitleri de bilindiği için CGA bu dayanıklılığı 2^{59}'a düşmektedir. Yani bir CGA 2^{59} adet tahmin içeren bir kaba kuvvet saldırısı ile bulunabilmektedir. İşte burada önceden belirlenen ve işletim sistemlerinde yer alan SEC değerleri ve HASH2 algoritması bu dayanıklılığı arttırmaktadır. Örneğin SEC=1 olduğunda dayanıklılık 2^{16} kadar artıp 2^{75} olacaktır. SEC değerinin her bir artışında CGA kaba kuvvetleri karşısında 2^{16} kadar daha güçlenecektir.

SEC değerinin her artışı HASH2'nin üretimini zorlaştırmaktadır. Çünkü HASH2'nin 16xSEC değeri kadar soldan ilk bitleri sıfır olarak üretilmek zorundadır. SEC değerinin artışları güvenliği arttırsa da HASH2 üretimini zorlaştırdığı için CGA üretim süresini uzatmaktadır. Yani HASH2 üretimi, CGA üretiminde işlem kapasitesinin en yoğun olduğu kısımdır denebilir. A. AlSa'deh ve C. Meinel'ın [24],[25], [26]' dan aktardığına göre SEC değeri ile CGA üretim sürelerinin karşılaştırmasını gösteren şekil aşağıdadır.

Bilgisayar Özellikleri	Sec=0	Sec=1	Sec=2	Sec=3
Modern PC (AMD 64 [24]	-	0.2 s	3.2 saat	24 yıl (Teorik olarak)
2.67 Ghz CPU PC [25]	93.41 ms	401.99 ms	1.65 saat	12 yıl (Teorik olarak)
Duo2 (2.53 Ghz) Workstation [26]	100 us	60 ms	2 saat	> 30000 saat (Teorik olarak)

Şekil 5.12: Farklı Sec değerleri için CGA üretim Süreleri [18]

CGA üretim süresinin kısaltılması için Ahmad AlSa'deh ve Christoph Meinel şu önerilerde bulunmuşlardır [18];

- CGA'yı daha hızlı üretebilmek için kriptografik hızlandırıcı kartlar kullanmak
- Günümüz bilgisayarları ve uygulamaları için pratik olmadığından dolayı SEC değerinin 1'den büyük kullanılmaması
- Sıfırdan büyük bir SEC değeri için belli bir süre sonra CGA üretiminin duracağının bir garantisi olmadığı için zaman bazlı CGA kullanılması önerilmektedir. Yani belli bir süre CGA üretilemezse üretiminin durması ve ardından farklı parametrelerle yeniden başlaması
- CGA üretiminin paralelleştirilmiş CGA algoritması ile yapılması
- Bilgisayar kaynaklarına uygun SEC değerlerinin seçilmesi
- Güvenlik seviye arttırıcı katsayının 16'dan 8 'e düşürülmesi [27]

Bunların yanında S.Jiang ve S.Xia CGA yönetiminin DHCPv6 sunucu kullanılarak yapılmasını önerdi. Burada İstemci DHCPv6'ya kendisi için CGA üretmesi için bir istekte bulunur.DHCPv6'nın ürettiği CGA istemci tarafından kullanılır [28].

CGA mobil cihazlarda da kullanılacaktır. Mobil cihazların kaynakları daha kısıtlı olduğundan üretim performansa daha fazla önem arz etmektedir. Kaldı ki mobil cihazların farklı ağlara bağlanma sıklığı normal cihazlara göre çok daha fazladır. Farklı ağlara bağlanan mobil cihazların önek değeri sürekli değiştiği için üretim aşaması yenilenmektedir. Bu da daha kısıtlı kaynaklara sahip mobil cihazlarda kaynak ve şarj tüketimine sebep olmaktadır. Bunun önüne geçmek için mobil cihazlarda işlem gücü gerektiren HASH2 hesaplanması kısmının yeni bir alt ağa girildiğinde hesaplanmaması, yeni alt ağlar ve önekler için sadece HASH1 ile arabirim tanıtıcısı üretilmesi düşünülmüştür. Buradaki tek endişe ise genel anahtara göre cihazın izlenip izlenemeyeceği ihtimalidir. Fakat genel anahtar ile bir mobil cihazın izlenebilmesi kolay değildir ve bu zaten çerezler ve IP adresleri vasıtasıyla yapılabilmektedir [18].

Bütün bunların yanında CGA süresinin üretim süresi işletim sisteminin genel/özel anahtar çiftini üretmek için seçeceği anahtar uzunluğuna göre de değişebilecektir. Örneğin RSA-1024 anahtar çifti ile üretilen CGA ile RSA-512 ile üretilen CGA'nın üretim süreleri aynı olmayacaktır. Bununla ilgili Pentium 4 ve 2593 Mhz CPU ya

sahip bir cihaz üzerinde yapılan bir çalışma da farklı uzunlukta ki RSA üretim süresi gösterilmiştir.

RSA Anahtar Uzunluğu (bit)	1024	2048	3072	7680
RSA Anahtar Üretim Süresi (sn)	0.163959	1.055806	3.457661	92.610627

Şekil 5.13: Farklı Anahtar uzunluklarına göre Anahtar üretim süresi [15]

Bütün bu performans geliştirmeleri göz önünde bulundurularak CGA üretim algoritması daha az kaynak tüketilmesi ve daha hızlı üretim için işletim sistemlerine en uygun şekilde düzenlenmelidir.

5.3.2 CGA İmzası

Bir cihaz bir mesajı imzalamak istediğinde RSA kullanarak üretmiş olduğu özel anahtar, CGA ve bu CGA ile ilişkili CGA data yapısı ve 128 bitlik "tip etiket" değerine ihtiyaç duymaktadır. 128 bitlik tip etiket değeri ve imzalanacak mesaj birleştirilir. Etiket değeri sola mesaj sağa yazılır. Oluşan bu yeni bileşke yapı ile özel anahtar girdi kabul edilerek RSASSA-PKCS1-v1_5 imzalama algoritması ve SHA-1 hash kullanılarak imza üretilir [22].

Mesaj imzalandıktan sonra; mesajın kendisi, imzası, CGA ve CGA data yapısı alıcı tarafa gönderilir. Alıcı tarafta imza doğrulanmadan evvel ilk önce CGA doğrulama algoritması gerçekleşir. İmzayı doğrulamak için mesajın imzası, kendisi, CGA ve CGA data yapısı, 128-bitlik tip etiket değeri birleştirilir. Bu yeni oluşan bileşke, mesajın imzası ile genel anahtar girdi kabul edilerek SHA-1 algoritması ile birlikte RSASSA-PKCS1-v1_5 imza algoritması çalışır ve imza doğrulanır [22].

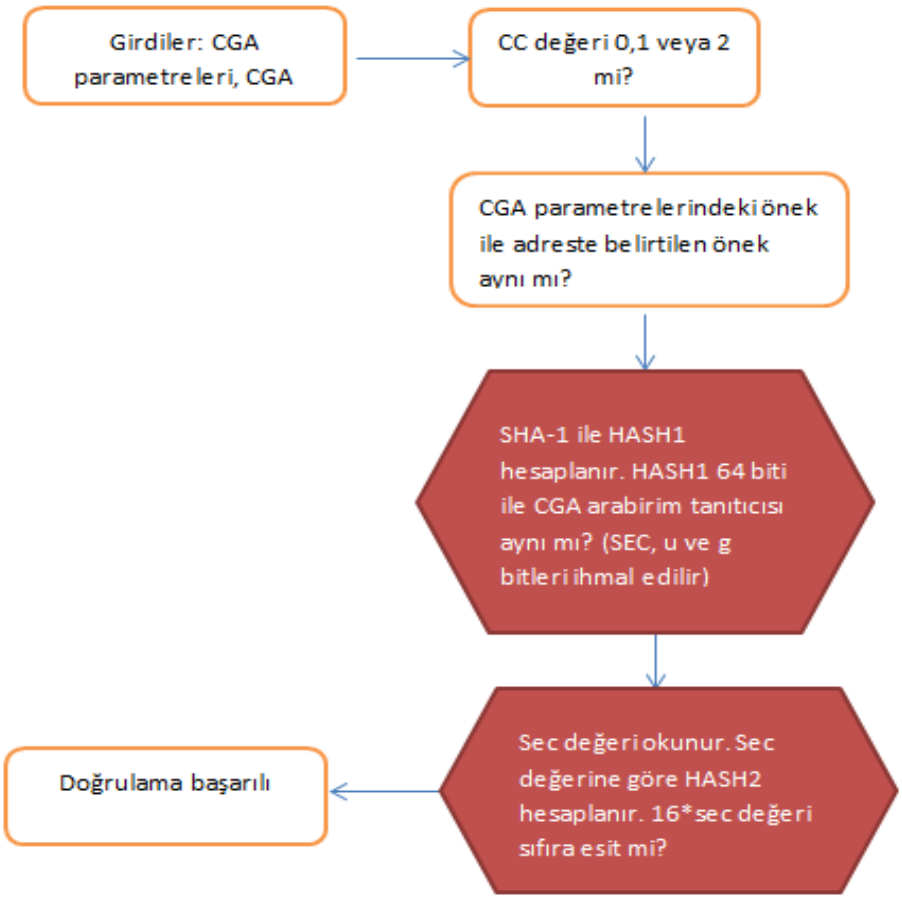
5.3.3 CGA Doğrulanması

CGA, RFC 3972' e göre mesajı alan bilgisayar tarafından aşağıdaki adımlar izlenerek doğrulanmaktadır [22]:

1- CC değerinin 0,1 veya 2 olup olmadığı kontrol edilir.
2- CGA'nın önekinin, CGA parametreleri ile gelen önek ile aynı olup olmadığı kontrol edilir.

3- CGA parametrelerini kullanarak HASH1 hesaplanır. Çıkan hash değerinin soldaki 64 hanesi CGA adresinin arabirim tanıtıcısı kısmı ile karşılaştırır. Bu karşılaştırma sırasında SEC bitleri, U ve G bitleri ihmal edilir.

4- Arabirim tanıtıcısının ilk 3 biti yani SEC değeri alınır. Sec değerine göre CGA yapısında bulunan niteleyici, 9 byte sıfır ve genel anahtar yan yana koyularak SHA1 algoritmasına sokulur ve HASH2 hesaplanır.HASH2'nin 16*SEC kadar bitinin sıfır olup olmadığı karşılaştırılır. Bütün bu işlemler hatasız olarak tamamlanırsa doğrulama başarıyla sonuçlanır. Doğrulama işleminin herhangi bir adımında hata alınırsa doğrulama işlemi durur ve başarısız olur. Aşağıda CGA doğrulama algoritmasını özetleyen şekil gösterilmiştir.



Şekil 5.14: CGA Doğrulama Algoritması

SEND üretim, imzalanma ve doğrulanma aşaması yukarıda belirtildiği gibi tasarlanmıştır. Bunların yanında her işletim sistemi ve SEND yapısını kendi ihtiyaç ve altyapılarına uyacak şekilde yeniden tasarlama yoluna gidebilirler. Örneğin Windows

kendi işletim sistemine özgü WinSEND veya çeşitli Linux sürümleri DoComo SEND, Easy SEND gibi SEND tasarımları kullanmaya başlamışlardır.

5.4 SEND Güvenlik Problemleri

CGA'ların SEND yapısında kullanılmasının birçok saldırı metodunu engellediği söylenebilse de CGA kendi içerisinde bir takım güvenlik problemleri barındırmaktadır. Bu güvenlik problemlerini şu şekilde özetleyebiliriz;

- SEND mesajları özel anahtar ile imzaladığı için bir cihazın IP adresinin bir saldırgan tarafından çalınmasını engellemektedir. Yani bir saldırgan ortamda kullanılan bir IP adresini kendi üzerine alamaz. Çünkü o IP adresini kullanan istemcinin özel anahtarına sahip olması gerekmektedir. CGA bu türlü bir adres hırsızlığının önüne geçse de bir istemcinin kimliğini doğrulamakta yetersizdir. CGA' da kullanılan anahtarların güvenilirliği doğrulanmadığı için bir saldırgan RSA genel/özel anahtar çifti üretip özel anahtarı ile imzalayıp iletişimi başlatabilir. Bunun önüne geçebilmek için anahtarların bir sertifika otoritesi tarafından doğrulanması gerekmektedir [19].
- Bilindiği gibi CGA parametreleri alıcı tarafa açık olarak gitmektedir. Saldırgan araya girip bu açık giden parametreleri değiştirirse mesajı alan taraf bu parametreler ile CGA'yı doğruladığı için doğrulama işlemini gerçekleştiremez. Dolayısı ile saldırgan iki cihaz arasındaki iletişime bu parametreleri değiştirerek engel olabilir [18].
- Bütün bunların yanında CGA kullanımında gizlilik konusunda da bir takım güvenlik problemleri doğabilir. Örneğin bir cihaz bir CGA ürettiği zaman uzun bir süre onu kullanmaya devam edecektir. Dolayısı ile cihaz ile kullandığı CGA arasında gizlilik tabanlı ataklar oluşturulabilir. Bunun üstesinden gelmek için ise üreticiler tasarımlarında CGA' ya bir geçerlilik zamanı atamalıdır. Bu süre sonunda CGA' nın yeniden üretilmesini sağlayacak şekilde CGA üretim algoritması genişletilmelidir [19]. Burada dikkat edilmesi gereken husus ise hukuksal gerekliliklerin yerine getirilmesi için her yeni CGA adresinin hangi cihaz ve kişi tarafından kullanıldığının kaydının tutulmasıdır. Burada her cihaz için kullanılan CGA

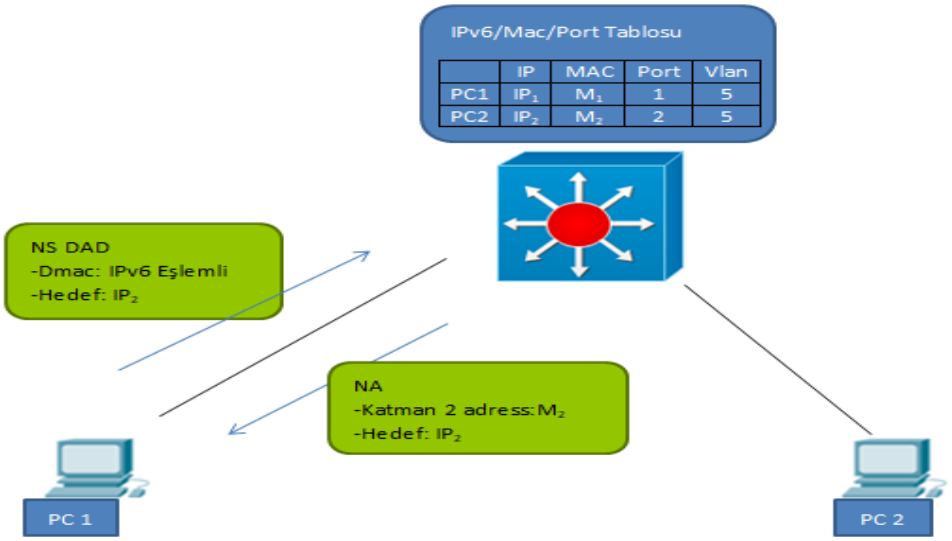
sürekli yenileneceği için bir kayıt mekanizmasının çalışması gerekmektedir. Tavsiye olunan çözüm ise ortamda DHCP benzeri IP, MAC, kişi ve zaman eşleştirilmiş bilgilerini tutan bir veritabanı bulundurulması ve CGA üretim aşamasında, DAD sürecinden hemen sonra yeni CGA'nın bu veritabanına istemci tarafından otomatik yazdırılmasını sağlayacak bir genişlemeye gidilmesidir. Burada istemci yeni CGA' sını kullanmaya başlamadan hemen evvel "Bu CGA adresini artık ben kullanıyorum" diye veritabanına mesaj yollamalı, veri tabanı bu mesaj içeriğini diğer bilgilerle eşleştirerek tutmalıdır. Bunun için yeni bir SEND mesajı veya seçeneği ve bunlara ait tip ve kod alanını içeren başlık yapılarının tanımlanması gerekmektedir.

- Saldırgan bir CGA' nın DAD sürecine DOS atak yapabilir. Kurban yeni bir CGA üretip DAD sürecini başlattığında ağa NS DAD mesajları yollar. Saldırgan bu mesajlar içerisinden kurbanın IP adresini, CGA parametrelerini ve imzasını alıp kopyalar ve DAD NA için beklenen süre içerisinde kurbana geri dönerse kurban kendisine gelen parametre ve imzaların doğru olduğunu görüp ürettiği CGA'nın kullanıldığını düşünür. Saldırgan aynı işlemi iki kere daha tekrarlarsa kurban artık CGA üretimini durdurur ve hata verir. Burada saldırgan sadece DOS atağı yapabilmekte bunun dışında herhangi bir zarar oluşturamamaktadır. Fakat yine de bu saldırının engellenebilmesi için DAD NS mesajı gönderen istemcinin kendisine gelen DAD NA mesajını CC değerini arttırmadan evvel doğrulayabilmesi gerekmektedir [19].
- Saldırgan DAD sürecine CGA olmayan bir IP adresi ve NA mesajı ile "Sorgulanan adrese sahibim" mesajı yollayabilir. CC değeri 2'ye ulaştığında ise CGA üretim aşaması başarısızlığa uğrar. Dolayısı ile CGA algoritması CC değeri arttırmadan evvel gelen DAD NA mesajını doğrulayacak şekilde geliştirilmelidir. Bu durumda ağdaki bütün cihazların CGA'yı desteklemesi ve CGA olmayan IP adreslerinden gelen DAD NA mesajlarının düşürülmesi gerekmektedir [18].

- CGA üretimi için SHA-1 algoritması kullanılsa da SHA-1'e yönelik çarpışma saldırıları mevcuttur. Fakat bu saldırının gerçekleşmesi en az sec değerinin sağladığı güvenlik seviyesi kadar değerin incelenmesini gerektirmektedir. Ayrıca SHA-1 nispeten eski bir güvenlik algoritması olduğundan dolayı yavaş yavaş sistemlerden desteği çekilmektedir. Örneğin Microsoft SHA-1 imzalı TLS sertifikalarına desteğini kaldırdı. Dolayısı ile CGA üretiminde ileriki yıllarda SHA-1 yerine başka bir şey kullanılması konusunda değişikliğe gidilebilir.

6. DAD PROXY

SEND, NDP yapısını daha güvenli hale getirse de kendi içerisinde birtakım güvenlik ve gizlilik açıklıkları içermektedir. Belirtilen bu tür güvenlik sorunların üstesinden gelebilmek için farklı bir çözüm yolu olan DAD Proxy geliştirilmiştir. Farklı üreticilerin ağ anahtarlarına entegre edilen bu çözüm ile ağ katmanında NDP'ye yönelik saldırılara karşı önlem alınabilmektedir.



Şekil 6.1: DAD Proxy [29]

Bu çözümün çalışması için istemcilerin bağlı olduğu ağ anahtarının katman3 paketlerini de açıp inceleyebilecek kapasitede olması gerekmektedir. Sistem aşağıda belirtildiği şekilde çalışmaktadır [30];

- İstemcilerin bağlı olduğu ağ anahtarları kendi içerisinde istemcilerin port, IPv6 ve Mac bilgilerini tutmaktadırlar.
- Bir istemci bir NS DAD isteğinde bulunduğu zaman bağlı olduğu anahtar gelen NS mesajı içerisinde Hedef adres seçeneğinde yer alan istemcinin sorgulamak istediği Ipv6 adresi ile kendi tablosundaki adresleri karşılaştırır. Eğer sorgulanan adres kendi tablosunda varsa bir NA mesajı ile adresin kendinde olduğunu bildirir. Eğer kendisinde yoksa kendi tablosuna kaydeder, NS paketini düşürür ve cevap vermez.
- Kısacası IPv6 DAD Proxy özelliği bir adres kullanımdayken ağ anahtarlarının o adres adına cevap vermesini sağlar. Anahtarlar istemciler için birer vekil konumundadırlar.

DAD Proxy kaynak adres aldatmasını engellemek için SAVI(RFC: 6959 Source Address Validation Improvement) mekanizması gibi özelliklerle beraber kullanılırsa kaynak adres aldatmasına yönelik NDP saldırılarının önüne geçer [31]. Bunun yanında 802.1x ve port-security gibi önlemlerde ağ katmanında güvenliği arttırmaktadır. IPv6 DAD proxy özelliğini kullanabilmek için ağdaki tüm anahtarlar katman 3 özelliklerini desteklemeli ve bu özellikleri destekleyecek modlarda çalıştırılmalı. Bu da fazladan kaynak tüketimine ve maliyet açısından daha yüksek rakamların ortaya çıkmasına sebebiyet verebilir.

DAD Proxy şu an için SEND ile beraber çalışmamaktadır. Çünkü vekil görevi görecek olan katman 2 anahtarlar CGA ile ilişkili özel anahtara sahip olmadığı için vekil ND mesajlarını imzalayamamaktadırlar [31]. Ayrıca DAD Proxy için bütün anahtarların katman 3 paketlerini açabilmesi ve kendi içerisinde bir eşleşme tablosu tutması gerekmektedir. Pratikte eşleşme tablolarının ağdaki sadece tek bir katman 3 destekleyen cihazda tutulacağı ve ağda diğer güvenlik önlemlerin alınmadığı varsayılıp düşünülürse vekil anahtar ve istemci arasına girilebileceği düşünülmelidir. Bu eksikliği giderilmesi vekil anahtar cihazının özel anahtar içermesi ve CGA' yı destekleyip mesajları imzalaması gerekmektedir. Bunun için şu an RFC6496'da deneysel aşamada olan SEND için güvenli vekil desteği tanımlanmıştır. SEND için güvenli vekil desteği çalışmasında "proxy imza seçeneği" adında yeni bir seçenek tasarlanıp denenmektedir [32].

Şu ana kadar yazılan bütün önlemler özetlenirse, güvenli bir yapı oluşturulması için bir ağda aşağıdaki gereklilikler sağlanmalıdır.

- ND Vekil Anahtarı kullanılmalı
- CGA kullanılmalı
- SEND altyapısında kullanılan bütün sertifikalar bir sertifika otoritesine doğrulatılmalı
- Bunların yanında ağ katmanında EAP-TLS gibi 802.1x metotları kullanılarak ağdaki herhangi bir cihaz ve kullanıcının kimliği doğrulanmalıdır.

KAYNAKLAR

[1] IPv6 El Kitabı, ULAKBİM, 2012, http://ulakbim.tubitak.gov.tr/tr/hizmetlerimiz/ipv6-el-kitabi, (Erişim Tarihi: 20 Mart 2017), s.9-14.

[2] R. Hinden, S.Deering ve E. Nordmark, "IPv6 Global Unicast Address Format," RFC 3587, Ağustos 2013, https://tools.ietf.org/html/rfc3587, s.2.

[3] IANA, https://www.iana.org/assignments/ipv6-unicast-address assignments/ipv6-unicast-address-assignments.xml, (Erişim Tarihi: 4 Ocak 2017).

[4] Graziani, R., IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6, Cisco Press, ABD, 2012, s.27-180.

[5] R. Hinden ve B.Haberman, "Unique Local IPv6 Unicast Addresses," RFC 4193, Ekim 2005, https://tools.ietf.org/html/rfc4193, s.3-5.

[6] R. Hinden ve S.Deering, "IPv6 Multicast Address Assignments," RFC 2375, Temmuz 1998, https://tools.ietf.org/html/rfc2375, s.2.

[7] Donald Eastlake, "IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters," RFC 5342, Eylül 2008, https://tools.ietf.org/html/rfc5342, s.7.

[8] T.Narten,R.Draves ve S.Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, Eylül 2007, https://tools.ietf.org/html/rfc4941, s.10-12.

[9] T.Narten vd., "Neighbor Discovery for IP version 6 (IPv6)," RFC 4861, Eylül 2007, https://tools.ietf.org/html/rfc4861

[10] Das K., IPv6 Stateless Auto Configuration, http://ipv6.com/articles/general/Stateless-Auto-Configuration.html (Erişim Tarihi:8 Mart 2017)

[11] S. Deering ve R.Hinden, "Internet Protocol, Version 6 (IPv6)Specification," RFC 2460, Aralık 1998, https://tools.ietf.org/html/rfc2460, s.4-11.

[12] S. Amante vd., "IPv6 Flow Label Specification," RFC 6437, Kasım 2011, https://tools.ietf.org/html/rfc6437, s.4.

[13] A.Conta, S. Deering ve M.Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," RFC 4443, Mart 2006, https://tools.ietf.org/html/rfc4443, s.3.

[14] IANA, Internet Control Message Protocol version 6 (ICMPv6) Parameters, https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml, 27 Ocak 2017.

[15] A.Boudguia, T.Cheneau ve M.Laurent., "Usage and performance of cryptographically generated addresses," Eylül 2008, https://hal.archives-ouvertes.fr/hal-01373433, s.8-51

[16] P.Nikander, J.Kempf ve E.Nordmark., "IPv6 Neighbor Discovery (ND) Trust Models and Threats," RFC 3756, Mayıs 2004, https://tools.ietf.org/html/rfc3756, s.9-12.

[17] J. Arkko vd., "Securing IPv6 Neighbor and Router Discovery", **1.ACM Workshop on Wireless Security**, Atlanta,ABD, 29 Eylül 2002, s.77-86.

[18] A. AlSa'deh ve C. Meinel, "Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations", IEEE Security & Privacy, 7 Şubat 2012, s.26-34

[19] A. AlSa'deh, H. Rafinee ve C. Meinel, "Secure Neigbor Discovery: A Crytocraphic Solition for Securing IPv6 Local Link Operations", Theory and Practice of Cryptography Solutions for Secure Information Systems, ed. A.Elçi vd., IGI Global, 2013,s.183-190)

[20] J.Arkko vd.,"Secure Neighbor Discovery (SEND)," RFC 3971, Mart 2005, https://tools.ietf.org/html/rfc3971, s.15-40.

[21] Fall K.R. ve Stevens W.Richard, TCP IP Illustrated, Person Education, 2.b., ABD, 2012, s.45-418

[22] T.Aura," Cryptographically Generated Addresses (CGA)," RFC 3972, Mart 2005, https://tools.ietf.org/html/rfc3972, s.7-15.

[23] AlSa'deh A, Meinel C; "Secure Neighbor Discovery", 2012, Aktaran: Akın G., Uysal M.B. ve Sarı T., **Secure Neighbor Discovery Protokolü**, Akademik Bilişim Konferansı Bildirileri, Akdeniz Üniversitesi, Antalya,2013, s.3

[24] J.W. Bos, O. Özen, ve J.-P. Hubaux, "Analysis and Optimization of Cryptographically Generated Addresses," LNCS 5735, Springer, 2009, pp. 17–32., Aktaran: AlSa'deh A., **Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations,** IEEE Security & Privacy, 7 Şubat 2012, s.31

[25] A. AlSa'deh, H. Rafee, ve C. Meinel, "Stopping Time Condition for Practical IPv6 Cryptographically Generated Addresses," *Proc. 26th IEEE Int'l Conf. Information Networking* (ICOIN 12), IEEE, 2012, pp. 257–262, Aktaran: AlSa'deh A., **Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations,** IEEE Security & Privacy, 7 Şubat 2012, s.31

[26] S. Jiang, "Analysis of Possible DHCPv6 and CGA Interactions," draf, 12 Mar. 2012; htp://tools.ietf.org/html/draf-ietf-csi-dhcpv6-cga-ps-09, Aktaran: AlSa'deh A., **Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations,** IEEE Security & Privacy, 7 Şubat 2012, s.31

[27] AlSa'deh ve C. Meinel, "Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations", IEEE Security & Privacy, 7 Şubat 2012, s.26-34, Aktaran: A. AlSa'deh, H. Rafee, ve C. Meinel, Stopping Time Condition for Practical IPv6 Cryptographically Generated Addresses, *26.Int'l Conf. Information Networking* (ICOIN 12), IEEE, 2012, s. 257–262.

[28] Jiang S. Ve Xia S., "Configuring Cryptographically Generated Addresses (CGA) Using DHCPv6", IETF, , http://tools.ietf.org/html/draft-ietf-dhc-cga-config-dhcpv6-02, 11 Nisan 2012.

[29] Cisco,IPv6 First-Hop Security Configuration Guide, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-3e/ip6f-xe-3e-book/ip6f-xe-3e-book_chapter_0101.html, (Erişim tarihi:20 Haziran 2017).

[30] Costa F. vd.,"Duplicate Address Detection", https://tools.ietf.org/html/rfc6957, RFC 6957, Haziran 2013, s.7-9.

[31] Costa F. vd.,"Duplicate Address Detection draft-costa-6mn-dad-proxy-01", IETF internet-draft,https://tools.ietf.org/html/draft-costa-6man-dad-proxy-01#page-11, 20 Eylül 2010, s.10-11.

[32] Krishnan S. vd., "Secure Proxy ND Support for Secure Neighbor Discovery (SEND)", RFC 6496, Şubat 2012, s.5.