İPv4'ten İPv6'ya Geçiş Süreci İçin İPv6 Tünel Ve Sanal Hedef İP Yöntemleri

Kenan ERDOĞAN[1] İrfan KARAGÖZ[2] Nursel AKÇAM[3]

[1]Türktelekom, Ankara

[2,3]Elektrik-Elektronik Mühendisliği Bölümü, Mühendislik-Mimarlık Fakültesi, Gazi Üniversitesi, Ankara

[1]e-posta: kenanerdogan2002@yahoo.com [2]e-posta:irfankaragoz@gazi.edu.tr [3]e-posta:ynursel@gazi.edu.tr

Özetçe

Bu çalışmada, günümüzde yaygın bir şekilde kullanılan ve internetin adresleme altyapısını oluşturan İnternet Protokolü'nün (İP) mevcut versiyonu İPv4, internetin gelişim hızı nedeniyle ortaya çıkarılan yeni versiyonu İPv6 ve bu iki versiyon arasındaki geçiş süreci anlatılmaktadır. İPv4'ten İPv6'ya geçiş mekanizması için bağımsız olarak çözüm üretmiş çalışmalardan ikili yığın, otomatik tünelleme, dinamik tünelleme ve anahtarlama yönlendiricisi çalışmalarına değinilmiş; bu çalışmalar üzerinde geçiş süreci için İPv6 Tünel ve Sanal Hedef İP yöntemleri geliştirilmektedir.

1. Giriş

İP, adres konfigürasyonu, yönlendirme esnekliği ve trafik desteği ile bütünsel bir ağ protokolü ortaya koymuştur. Bir İPv4 adres 32 bit yapıya sahiptir ve 4 milyarın üzerinde bilgisayarı adreslemeye imkan tanır. 1990'ların başından itibaren internetin hızla gelişmesi ile bu sayı yetersiz olmaya başlamıştır. Uluslararası organizasyon IETF (Internet Engineering Task Force)'nin çalışmaları, 2008 ile 2018 yılları arasında mevcut İPv4 adreslerin tamamen tükeneceği yönünde veriler sundu [1].

İPv6 için ilk öneriler Temmuz 1992'de IETF tarafından yapılmış; 1994'te de İPv6 adres yapısı için son tasarım oluşturulmuştur. Günümüzde ise, eski protokolden yeni protokole geçiş süreci yaşanmaktadır. Geçiş tamamlanıncaya kadar dünya üzerinde İPv4 ve İPv6 beraber kullanılacaktır. İPv6 protokolünün detayları olgunlaştırılırken mevcut internet altyapısının yeni altyapıya geçiş sürecinin optimize edilmesi ile ilgili çalışmalar da sürdürülmektedir. Geçişin nasıl olacağı ve nasıl fazlardan geçeceği tam olarak belirlenmemiştir, ancak yeni geçiş mekanizmaları ile İPv6'ya geçiş mümkün kılınmıştır. Bu mekanizmalar; ikili yığın yaklaşımı, tünel yaklaşımı ve dönüştürücü yaklaşımı olarak sıralanabilir.

2. İnternet Protokolleri

2.1.İnternet Protokol Versiyon 4 (İPv4)

Temel olarak İP, sunduğu global adresleme yapısı ile veri paketleri için bilgisayar ağlarında iletim yolu belirlemeye imkan tanır. Bir bilgisayarın milyonlarca bilgisayar arasından hedefini bulabilmesi, birimsel bir İP adrese sahip olmakla mümkün olmaktadır. Ayrıca IP'nin servis isteklerini sınıflandırma, paketleri iletim için uygun parçalara ayırma ve hedef alıcıda paketleri tekrar birleştirme, paketlerde hata kontrolü gibi fonksiyonları mevcuttur [2].

2.2. İnternet Protokol Versiyon 6 (İPv6)

1990'ların başında İPv4' ün çalışma deneyimine dayalı, ancak ondan daha güçlü ve işlevsel olan İP versiyon 6 tasarlanmaya başlandı. İPv6'nın getirdiği bir çok yenilikler mevcuttur. İPv6 adresleme de bir adres 128 bittir ve bu İPv6'nın İPv4'ten temel farkıdır. İPv6 alıcı ve verici arasında yüksek kalitede yol oluşturup paketleri bu yol üzerinden iletme imkanı sunar. Bu da daha kaliteli ve performanslı iletim isteyen ses ve görüntü iletimine altyapı hazırlar, ayrıca ucuz iletim imkanı da sağlar. İPv6 başlığı basitleştirilmiştir, bu nedenle işlem süresi kısalmıştır. Ayrıca paketlerin türü başlık içerisinde ayrıştırılarak gerçek zaman trafiği ile anlık iletim istemeyen trafik için yönlendiricilerin farklı davranması hedeflenerek servis kalitesi arttırılmıştır. İPv6 temel başlığının yanında ek başlık kavramını ortaya çıkarmıştır. Bu başlıklar, ilerde ihtiyaç duyulabilecek eklemelere imkan verirken İPv6'yı gelişmeye açık bırakmıştır [3].

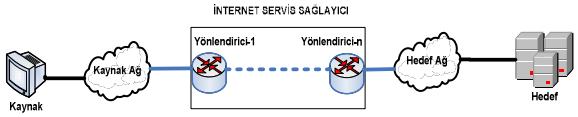
3. Geçiş Süreci

Tablo 1'de görülen RFC4852 dökümanında belirtilmiş kaynak, geçilen ağ ve hedef türleri matrisi Şekil 1'de genel haliyle görülmektedir. Geçilen beş ortamın

herbiri üç farklı İP yapısında olabileceğinden sıralama kuralına göre 3x3x3x3x3=243 farklı senaryo oluşmaktadır [4].

Tablo 1: Geçiş sürecinde kaynak, geçilen ağ ve hedef türleri matrisi

İstemci	İstemci Ağı	İnternet Servis Sağlayıcı	Sunucu Ağı	Sunucu
Sadece İPv4	Sadece İPv4	Sadece İPv4	Sadece İPv4	Sadece İPv4
Sadece İPv6	Sadece İPv6	Sadece İPv6	Sadece İPv6	Sadece İPv6
İkili Yığın	İkili Yığın	İkili Yığın	İkili Yığın	İkili Yığın



Şekil 1: Genel internet ağ şeması

3.1. İPv4-İPv6 Arası Geçiş Mekanizmaları

Tablo 2'de İPv4-İPv6 arası geçiş mekanizmaları görülmektedir [5].

Tablo 2: İPv4-İPv6 arası geçiş mekanizmaları

İsim	Bağlantı	Tip
İkili Yığın	4'ten 4'e , 6'dan 6'ya	İkili Yığın
Sııt	6'dan 4'e 4'ten 6'ya	Dönüştürücü
Bıs	4'ten 6'ya	Dönüştürücü
Bıa	4'ten 6'ya	Dönüştürücü
Nat-Pt	6'dan 4'e 4'ten 6'ya	Dönüştürücü
Mtp	6'dan 4'e 4'ten 6'ya	Dönüştürücü
Trt	6'dan 4'e	Dönüştürücü
Socks64	6'dan 4'e 4'ten 6'ya	Dönüştürücü
4 Üzerinden 6	4 Üzerinden 6'dan 6'ya	Tünel
Isatap	4 Üzerinden 6'dan 6'ya	Tünel
Dstm	6'dan 6'ya , 4'ten 4'e	Tünel
İP İçinde İP	6'dan 6'ya , 4'ten 4'e	Tünel
Dinamik Tünel	6 Üzerinden 4'ten 4'e	Tünel
6'dan 4'e Otomatik	4 Üzerinden 6'dan 6'ya	Tünel

3.1.1. İkili yığın yaklaşımı

İkili yığın yaklaşımı hem İPv4 hem de İPv6 uygulamalarını aynı cihazda toplama işlemidir. Bu durumda bir çok kod iki protokol tarafından paylaşılarak kullanılır. Bu cihaz her iki İP türüyle haberleşir.

3.1.2. Dönüştürücüler

Dönüştürücüler farklı ağların birbiriyle çalışmasını sağlaması amacıyla oluşturulmuş yazılımlardır. SIIT (Stateless IP/ICMP Translation Algorithm), BIS (Bump-In-The-Stack), BIA (Bump-In-The-API), NAT-PT (Network Address Translation - Protocol Translation), MTP (Multicast translator based on IGMP/MLD proxying), SOCKS64 TRT (Transport relay translator) gibi türleri mevcuttur.

3.1.3. Tünel metodu

Tünel metodu İPv6 paketinin İPv4 tarafından kaplanması ve İPv4 ağı üzerinden gönderilmesidir. Bu durumda İPv6 bilgisayarlar aradaki İPv4 ağı İPv6 yapılmasa da haberleşir. Tünel metodu türleri;

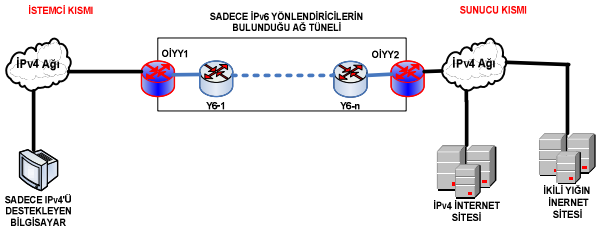
- 4 üzerinden 6 tünelleme,
- ISATAP tünelleme,
- İP içinde İP tünel konfigürasyonu,
- Dinamik tünelleme,
- 6'dan 4'e otomatik tünelleme'dir [5].

4. İPv4'ten İPv6'ya Geçiş Süreci İçin İPv6 Tünel Ve Sanal Hedef İP Yöntemleri

4.1. İPv6 Tünel Tekniği

Günümüze kadar yapılan tünel çözümlerinden dinamik tünelleme dışında kalanlar İPv4 üzerinden İPv6 haberleşmesine yoğunlaşmıştır. Sadece dinamik tünelleme yöntemi İPv6 üzerinden İPv4 bilgisayarların haberleşmesine çözüm getirmiştir. Ancak dinamik tünelleme metodu kaynak bilgisayarın ikili yığın yapıda olmasını gerektirmektedir. İkili yığın bilgisayar kendi ürettiği İPv4 paketini İPv6 başlık ile kaplayıp İPv6 ağ üzerinden İPv4 hedefe göndermekte ve onun servisinden yaralanmaktadır. Dinamik tünelleme yönteminde ikili yığın yönlendirici sadece tünelin çıkışında bulunmaktadır.

Geçiş sürecinde internet servis sağlayıcı İPv6'ya geçtiği halde kendi ağını İPv6'ya yükseltemeyen istemciler de bulunacaktır. İstemcinin bilgisayarları ve ağ altyapısı sadece İPv4 desteği sunabildiğinden bu bilgisayarların İPv4 internete erişmesi problemi doğacaktır. Bu problemi çözmek için burada İPv6 tünelleme tekniği geliştirilmiştir. Şekil 2'de çözüm geliştirilen yapı görülmektedir.



Şekil 2. İPv6 ağ tüneli yapısı

Tablo 3. Cihazların İP adres dağılımı

Cihaz	İPv4 Adres	İPv6 Adres
Sadece İPv4 Destekleyen Bilgisayar	a.b.c.d	-
OİYY1	x.y.z.t	2002:0x0y:0z0t::
OİYY2	u.v.y.z	2002:0u0v:0y0z::
İPv4 İnternet	d.e.f.g	-
İkili Yığın İnternet	k.l.m.n	2001::0k0l:0m0n

OİYY cihazı daha önce anlatılan otomatik ikili yığın yönlendiricidir. Sadece İPv4 destekleyen bilgisayar ve İPv4 ağı, altyapısı henüz İPv6'ya geçememiş istemcileri belirtir. İPv4 internet sitesi sadece İPv4 desteği olan internet sitesini ve ikili yığın internet sitesi ise hem İPv4 hem de İPv6 desteği olan internet sitesini belirtmektedir.

Kaynak bilgisayar a.b.c.d, hedef bilgisayarlar ise d.e.f.g ve k.l.m.n İPv4 adreslere sahiptir (Tablo 3). Teknikte ikili yığın internet sitesinin de İPv4 adresi kullanıldığından işlem süreci İPv4 internet sitesinin çözümü ile aynıdır. a.b.c.d kaynak İPv4 adrese sahip bilgisayar d.e.f.g veya k.l.m.n hedef adresine erişmek için önce İPv4 paket oluşturur. Oluşan bu İPv4 paket İPv4 ağdan geçerek OİYY1'e gelir. OİYY1 paketin İPv6 ağda iletilebilmesini sağlamak amacıyla İPv4 başlığı İPv6 başlığı ile kaplar. İPv6 başlığın kaynak adresi OİYY1'in 2002:0x0y:0z0t:: şeklindeki İPv6 adresi; hedef adresi ise OİYY2'nin 2002:0u0v:0y0z:: şeklindeki İPv6 adresidir. Paket İPv6 ağı tünelinde böylece iletilir. Tünelin sonunda OİYY2 paketin İPv6 başlığını kaldırır ve orjinal İPv4 paketine ulaşır. Daha sonra bu paketi başlıktaki hedef adrese yani d.e.f.g veya k.l.m.n hedef adresine yollar. Böylece haberleşme gerçekleşmiş olur.

4.2. İPv4 ve İPv6 Tüneller Üzerinde Sanal Hedef İP İle Haberleşme Tekniği

İPv4 tünel metodu İPv6 bilgisayarları İPv4 ağ üzerinden haberleştirmek amacıyla, İPv6 tünel metodu ise İPv4 bilgisayarları İPv6 ağ üzerinden haberleştirmek amacıyla tasarlanmıştır. Bu tüneller İPv4 ile İPv6 bilgisayarların nasıl haberleşeceği konusunda yöntem içermemektedir. Burada geliştirilen sanal İP tekniğiyle İPv4 veya İPv6 tünel üzerinden İPv4 ve İPv6 bilgisayarları haberleştirme gerçekleştirilmiştir.

4.2.1. Sanal hedef İP kavramı ve teknik ile çözülen problemin ağ mimarisi

Global birimsel İPv6 adresleri 2000:0:0:0:0:0:0:0'den başlayıp
3FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
adresine kadar gider. Bu adresler internete bağlanacak her bilgisayarın birimsel İP adresi olacaktır. İPv4 adresin İPv6'ya haritalandırılması yöntemi, İPv4 adresten yola çıkılarak bir İPv6 adresi belirler. İPv4 adres onaltılık sayı sisteminde yazılır. Daha sonra oluşan adres ikişerli birleştirilerek dörtlü gruplar oluşturulur ve İPv6 adresin son kısmına yerleştirilir. Örneğin, 3.0.0.1 İPv4 adresinin onaltılık yapısı 03.00.00.01'dır. İkişerli birleşince 0300:0001 değeri oluşur. Bu değer herhangi bir İPv6 adres üzerindeki son 32 bite yerleştirilince 2001:0000:0000:0000:0000:0000:0300:0001 şeklinde İPv6 adres elde edilmiş olur.

Burada geliştirilen teknikte global İPv6 adreslerdeki 2001:: bloğu kullanılmış ve bu bloğun son 32 biti İPv4 adresin İPv6 adrese haritalanması şeklinde seçilmiştir. Geliştirilen teknikte 32 bitin oluşturduğu İPv4 adresler ve otomatik 6'dan 4'e İPv6 adreslerin içerdiği İPv4 adresler herhangi bir İPv4 sınıfından seçilebilir. Tablo 4'de, teknik için seçilen İPv6 altyapısı görülmektedir.

Tablo 4. Teknik için seçilen İPv6 altyapısı

İPv6 Adres Türü	İlk 16 Bit	Sonraki 32 Bit	Sonraki 48 Bit	Son 32 Bit
Otomatik 6'dan 4'e İPv6	2002	x.x.x.x İPv4 Adres	Değişken	Değişken
Global İpv6	2001	Değişken	Değişken	x.x.x.x İPv4 Adres

Burada oluşturulan sanal İP tekniğinde her bir İPv4 adrese sanal olarak nitelenen bir İPv6 adresi, her bir İPv6 adrese de yine sanal olarak nitelenen yeni bir İPv4 adresi üretilmektedir. Şekil 3'de geliştirilen tekniğin ağ mimarisi görülmektedir. Bu yapıda bulunan cihazların tanımları ve işlevleri aşağıda sıralanmıştır.

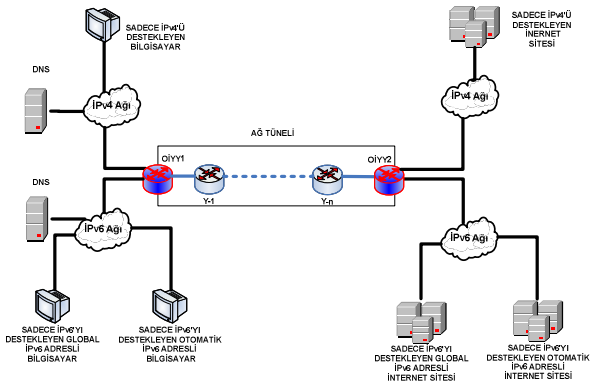
Sadece İPv6'yı Destekleyen Global İPv6 Adresli Bilgisayar: Üzerinde sadece İPv6 yığını ve desteği bulunan bilgisayarı temsil eder. 2001:: şeklinde global tekli-yayın İPv6 adrese sahiptir.

Sadece İPv6'yı Destekleyen Otomatik İPv6 Adresli Bilgisayar: Üzerinde sadece İPv6 yığını ve desteği

bulunan ve 2002:İPv4 Adres: :/16 şeklinde otomatik İPv6 adrese bilgisayardır.

Sadece İPv4'ü Destekleyen Bilgisayar: Üzerinde sadece İPv4 yığını ve desteği bulunan bilgisayarı temsil eder.

DNS (Domain Name Server): DNS sunucusu internet sitelerinin isim-İP eşleştirmelerini tutan sunucudur. Sanal hedef İP tekniğinde DNS cihazı kayıtlarında özel olarak, gerçek İP adresi yerine sanal hedef İP adresini tutulur (Tablo 5).



Şekil 3 Geliştirilen tekniğin ağ mimarisi

Tablo 5. Sanal Hedef İP adresler için DNS kayıtları

Cihaz Adı	İP Adres
Sadece İPv4'ü Destekleyen İnternet Sitesi	2002:x.x.x.x::
Global İPv6 Adresli İPv6 İnternet Sitesi	x.x.x.x
Otomatik İPV6 Adresli İPV6 İnternet Sitesi	x.x.x.x

OİYY (Otomatik İkili YığınYönlendirici): Daha önce bahsedilen ve çözümlerde kullanılmış olan, otomatik 6'dan 4'e yönlendirme desteği bulunan, hem İPv4 hem de İPv6'yı destekleyen ikili yığın yönlendiricidir. Paket başlıkları üzerinde kaplama, çıkarma ve yeniden ekleme gibi işlemler yapabilmektedir.

Ağ Tüneli: İPv4 veya İPv6 altyapısında daha önce bahsedilen tünel türlerinden biridir.

Y-1---Y-n: 1'den n'e kadar belirsiz sayıda tünel türüne göre İPv4 veya İPv6 yönlendiricilerdir.İletim paketleri üzerinde değişiklik yapmazlar. Sadece iletim tünelini oluşturup paketi bir sonraki hedefe gönderme işlemi yaparlar.

Sadece İPv4'ü Destekleyen İnternet Sitesi: İPv4 altyapısında kurulmuş internet sitesidir.

Sadece İPv6'yı Destekleyen Global İPv6 Adresli İnternet Sitesi: İPv6 altyapısında kurulmuş global İPv6 adrese sahip internet sitesidir.

Otomatik İPv6 Adrese Sahip İPv6 İnternet Sitesi: İPv6 altyapısında kurulmuş özel 6'dan 4'e İPv6 adrese sahip internet sitesidir.

4.2.2. İPv6 kaynakların İPv4 ve İPv6 tüneller üzerinden İPv4 hedefle haberleşmesi için geliştirilen teknik

Burada İPv6 kaynakların İPv4 ve İPv6 tüneller üzerinden İPv4 hedefle haberleşmesi gerçekleştirilmektedir (Şekil 4). Kullanılan genel İP adres yapısı ve sanal İP adresler Tablo 6'da verilmiştir.

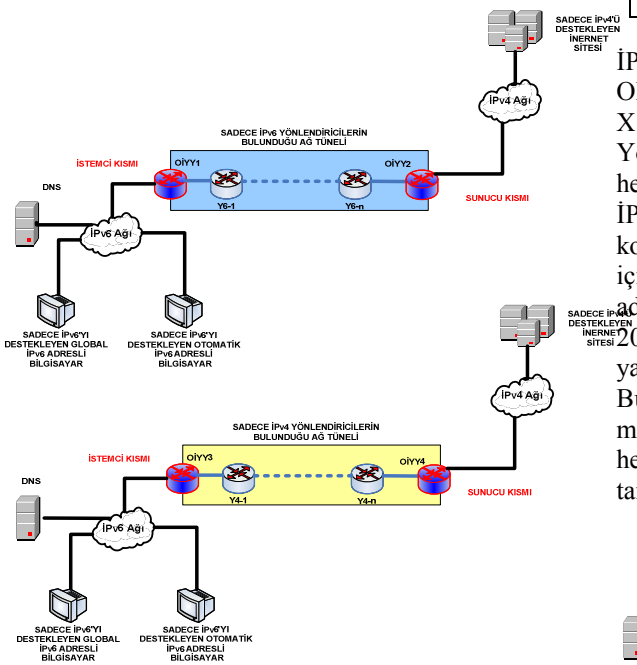
Tablo 6. Kullanılan genel İP adres yapısı ve sanal İP adresler

	1.Kaynak Global İPv6	2.Kaynak Otomatik İPv6	Hedef İPv4
Gerçek İP Adres	2001::X.Y.Z.T	2002:K.L.M.N::	A.B.C.D
Sanal İP Adres	X.Y.Z.T	K.L.M.N	2002: A.B.C.D::

2001::X.Y.Z.T ve 2002:K.L.M.N:: yapıda (X,Y,Z,T,K,L,M ve N 0 ile 256 arası değişen sayılardır) İPv6 adreslere sahip kaynak bilgisayarlar sadece İPv6 paket oluşturabilirler. Hedef İPv4 olduğundan doğrudan hedef yapılamaz. Sanal hedef yöntemi ile bu İPv4 adresin DNS'teki kaydı olan 2002:A.B.C.D:: şeklindeki sanal İPv6 adresi kullanılarak bu sorun aşılır. Bu adresi hedef yapan İPv6 paketi oluşturulup İPv6 ağa verilir. Ağdan geçen paket her iki durumda da OİYY1'e ve OİYY3'e değişmeden gelir.

İPv6 tünel başındaki OİYY1'e gelen İPv6 paketi değişmeden OİYY2'ye geçer. OİYY2 paketin 2002:A.B.C.D:: şeklindeki sanal İPv6 hedefine bakar. Yönlendirme tablosunda böyle bir İPv6 hedef yoktur. Bu durumda hedef tablosunda bu İPv6 adresin içerdiği İPv4 adresin olup olmadığı kontrol edilir. Yönlendirme tablosunda bu hedef olduğu için paketin İPv6 başlığı açılır ve kaynağın sanal İPv4 adresini kaynak adres, hedefin A.B.C.D adresini hedef adres yapan yeni bir İPv4 başlık oluşturulup pakete eklenir. Bunu sağlamak için OİYY2'de bir hedef kontrol mekanizması konulmuştur. Oluşan bu paket A.B.C.D adresli bilgisayara gönderilir ve haberleşme tamamlanır.

İPv6 paketin İPv4 tünelde ilerleyebilmesi, OİYY3'te daha önce anlatılan tünel mantığıyla İPv4 başlık ile kaplanması ile mümkündür. Bu başlık OİYY4'te açılır ve İPv6 paketi elde edilir. OİYY4 paketin 2002:A.B.C.D:: şeklindeki sanal İPv6 hedefine bakar. Yönlendirme tablosunda böyle bir İPv6 hedef olmadığından paketin İPv6 başlığı açılır ve kaynağın sanal İPv4 adresini kaynak adres, hedefin A.B.C.D adresini hedef adres yapan yeni bir başlık oluşturulup A.B.C.D adresli bilgisayara gönderilir. Haberleşme tamamlanır. Bunu sağlamak için OİYY4'e bir hedef kontrol mekanizması konulmuştur.



Şekil 4. İPv6 kaynakların İPv4 ve İPv6 tüneller üzerinden İPv4 hedefle haberleşmesi

4.2.3. İPv4 kaynağın İPv4 ve İPv6 tüneller üzerinden İPv6 hedeflerle haberleşmesi için geliştirilen teknik

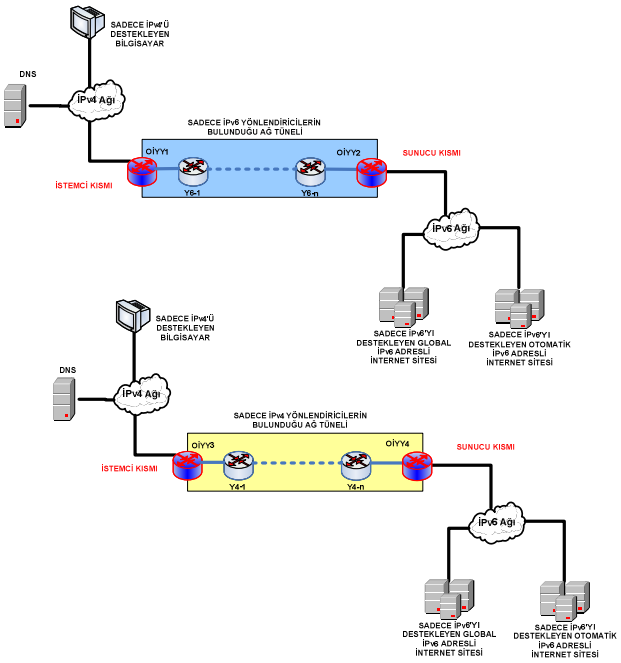
Burada İPv4 kaynağın İPv4 ve İPv6 tüneller üzerinden İPv6 hedeflerle haberleşmesi sağlanmaktadır (Şekil 5). Kullanılan genel İP adres yapısı ve sanal İP adresler Tablo 7'de verilmiştir.

Kaynak İPv4 bilgisayar sadece İPv4 paket oluşturabilir. Bu nedenle 2001::X.Y.Z.T veya 2002:K.L.M.N:: yapıda (X,Y,Z,T,K,L,M ve N 0 ile 256 arası değişen sayılardır) İPv6 adreslere sahip bilgisayarları doğrudan hedef yapamaz. Sanal hedef yöntemi ile bu İPv6 adreslerin DNS'teki kayıtları olan K.L.M.N veya X.Y.Z.T şeklindeki sanal İPv4 adresleri kullanılarak bu sorun aşılır. Bu adresleri hedef yapan İPv4 paketleri oluşturulup İPv4 ağa verilir. Ağdan geçen paket her iki durumda da OİYY1'e ve OİYY3'e değişmeden gelir.

Tablo 7. Kullanılan genel İP adres yapısı ve sanal İP adresler

	Kaynak İPv4	1.Hedef Otomatik İPv6	2.Hedef Global İPv6
Gerçek İP Adres	A.B.C.D	2002:K.L.M.N::	2001:: X.Y.Z.T
Sanal İP Adresler	2002: A.B.C.D:	K.L.M.N	X.Y.Z.T

İPv4 tünel başındaki OİYY1'e gelen paket değişmeden OİYY2'ye geçer. OİYY2 paketin K.L.M.N veya X.Y.Z.T şeklindeki sanal İPv4 hedefine bakar. Yönlendirme tablosunda bu adreslere sahip İPv4 hedefler yoktur. Bu durumda hedef tablosunda bu İPv4 adresleri içeren İPv6 adreslerin olup olmadığı kontrol edilir. Bu adresler hedef tablosunda var olduğu için paketin İPv4 başlığı açılır ve kaynağın sanal İPv6 adresini kaynak adres, hedeflerin 2001::X.Y.Z.T veya 2002:K.L.M.N:: İPv6 adresinlerinden birini hedef adres yapan yeni bir İPv6 başlık oluşturulup pakete eklenir. Bunu sağlamak için OİYY2'de bir hedef kontrol mekanizması konulmuştur. Bu paket bahsedilen hedeflerden birine gönderilerek haberleşme tamamlanır.

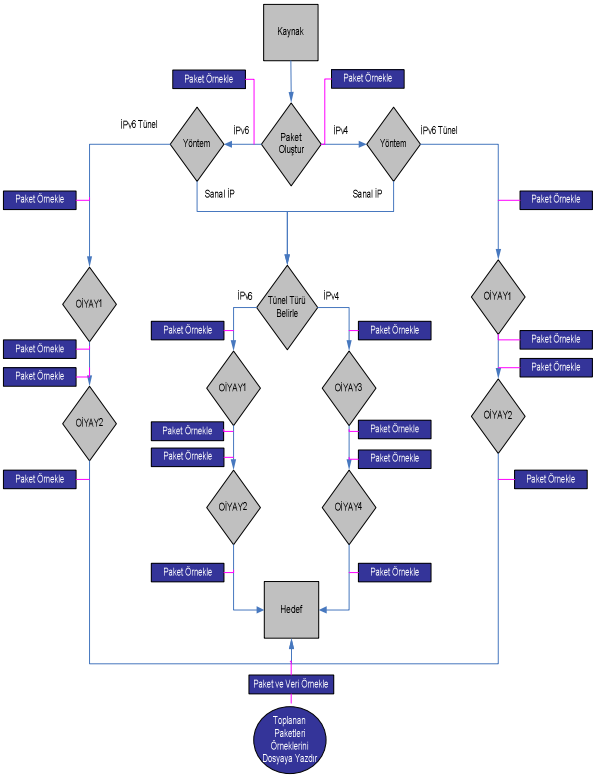


Şekil 5. İPv4 kaynağın İPv4 ve İPv6 tüneller üzerinden İPv6 hedefler ile haberleşmesi

İPv4 paketin İPv6 tünelde ilerleyebilmesi, OİYY3'te daha önce anlatılan tünel mantığıyla İPv4 başlık ile kaplanması ile mümkündür. Bu başlık OİYY4'te açılır ve baştaki İPv6 paketi yeniden elde edilir. OİYY4 paketin K.L.M.N veya X.Y.Z.T şeklindeki sanal İPv4 hedefine bakar. Yönlendirme tablosunda bu adreslere sahip İPv4 hedefler yoktur. Bu durumda hedef tablosunda bu İPv4 adresleri içeren İPv6 adreslerin olup olmadığı kontrol edilir. Bu adresler hedef tablosunda var olduğu için paketin İPv4 başlığı açılır ve ve kaynağın sanal İPv6 adresini kaynak adres, hedeflerin 2001::X.Y.Z.T veya 2002:K.L.M.N:: İPv6 adresinlerinden birini hedef adres yapan yeni bir İPv6 başlık oluşturulup pakete eklenir. Bunu sağlamak için OİYY4'e bir hedef kontrol mekanizması konulmuştur. Bu paket bahsedilen hedeflerden birine gönderilerek haberleşme tamamlanır.

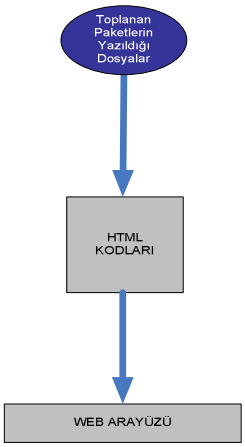
4.2.4. Geliştirilen uygulama

Bahsedilen her teknik için İP paketlerinin ağdaki seyri java kadroları ile simule edilmiştir ve webe aktarılmıştır. Programın genel işleyiş algoritması Şekil 6'da verilmiştir.



Şekil 6. Bağlantıları simule eden java programlarının genel işleyiş algoritması

Şekil 7'de ise sonuçlardan tasarlanan web arayüzünün algoritması verilmiştir.



Şekil 7. Sonuçlardan tasarlanan web arayüzünün algoritması

5. Sonuçlar

Bu çalışmada, günümüzde yerel ağlarda ve geniş ağlarda yaygın bir şekilde kullanılan ve internetin altyapısını oluşturan internet protokolünün (İP) bugünü ve geleceği üzerine bilgiler sunulmuştur. İPv6'ya geçiş süreci için, günümüze kadar yapılan çalışmalar anlatılmış ve İPv6 tünel ve sanal hedef İP teknikleri geliştirilmiş ve sunulmuştur. Bu teknikler java kodları ile simule edilip webden aktarılmıştır.

Kaynakça

[1] Buckhanan, B., "Handbook of Data Communication and Networks 1999 ed.", ***Kluwer Academic Publishers*** , Boston, 211-212 (1999).

[2] Krose, J. F. and Ross, K. W., "Computer Networking A top-down Approach Featuring The İnternet 2nd ed.",***Addison Wesley,*** Pearson, 369-375, 334-33 (2003).

[3] Stallings, W., "Computer Networking with İnternet Protocols And Technology İnternational ed.",***Prentice Hall***, Pearson, 290-300 (2004).

[4] Bound J., Pouffary Y., Klynsma S, Chown T. and Green D., "IPv6 Enterprise Network Analysis-IP Layer 3 Focus", **RFC-4852,** 1-29 (2007).

[5] Gilligan, R., and Nordmark, E. "Transition Mechanisms for IPv6", ***İnternet Engineering Task Force Magazine*** **RFC-2893,**1-29(2000).