

# IPv6 ADRESLEME VE BAŐLIK YAPISI

**Orhan Sümer** <sup>†</sup>  
Eser Telekom  
osumer@esertelekom.com

**Ege Kipman**  
Beykent Üniversitesi  
kipman@beykent.edu.tr

## 1. Giriş

Günümüzde hayatımızda Internet'in rolü artık tartışılmayacak bir noktadadır. Her çeşit uygulamada Internet'i kullanıyoruz. Şirketler Internet üzerinden ürünlerini satışı için sanal mağazalar açıyorlar, gezici satış elemanları ve şirketleri arasındaki bağlantılar Internet üzerinden gerçekleştiriliyor, üniversitelerde dersler sanal dersliklere doğru geçiyor, bankalar mudilerine tüm işlemleri için Internet'i kullanılmasını öneriyor, telefon görüşmeleri Internet üzerinden taşınarak indirimli görüşmeler sağlıyor. Bundan 10 sene önce Internet'in bu kadar gelişeceğini kimse düşünmüyordu. Ama artık Internet'i bu şekilde yeterli olmamaktadır. Internet'in yayılmasıyla yukarıda sayılanlardan başka bir çok farklı gereksinimler ortaya çıkmıştır. IPv4'e güvenlik ve ağ adres çevirimi eklentiler ile bugüne kadar gelinmiştir. Fakat gereksinimlerin artmasıyla IPv4 yetersiz gelmektedir. Bunu için 1992 yılından itibaren oluşturulan bir grupla IPv4'ün eksikliklerini giderecek yeni bir altyapı protokolü üzerinde çalışılmaya başlandı. Bu yeni alt yapı protokolüne IPv6 ismi verildi. IPv6 ilk olarak IPv4'ün 32 bitlik kısıtlı IP adres'i eksikliğini gidermek için oluşturulmuştu. Fakat zamanla IPv4'ün eksik kalan tüm yönleri IPv6 altında toplandı. IPv6 ile güvenlik, adres kısıtlaması ve yönlendirme gibi işlemlerini kendi üzerinde yapacak bir yapıya kavuştu.

Bu makalede gelecek nesil Internet Protokolünün (IPng) adresleme yapısı ve uzantı başlıkları hakkında bilgiler verilmiştir.

Anahtar Kelimeler : IPv6, Başlık, Adresleme, ESP ,AH , Sıçrama başlığı, Yönlendirme Başlığı, Parçalama Başlığı

## 2. IPv6'ya Genel Bakış

Internet Protokolü sürüm 6 (IPv6), Internet Protokolü'nün (IP) yeni bir sürümüdür. IPv6 tasarımı, kullanımdaki sürüm olan IPv4 evrimsel değişiminden ileri gelmektedir. IPv6, IPv4'ün doğal artırılmış halidir. IPv6'da adres sayısı artırılmıştır. IPv6 ile Internet yeteneğini, basit başlık biçimi, gizlilik ve doğrulama desteği, otomatik konfigrasyon ile adres verilmesi ve yeni servis kalitesi (quality-of-service QoS) yetenekleriyle arttırmıştır.

IPv6'nın özellikleri:

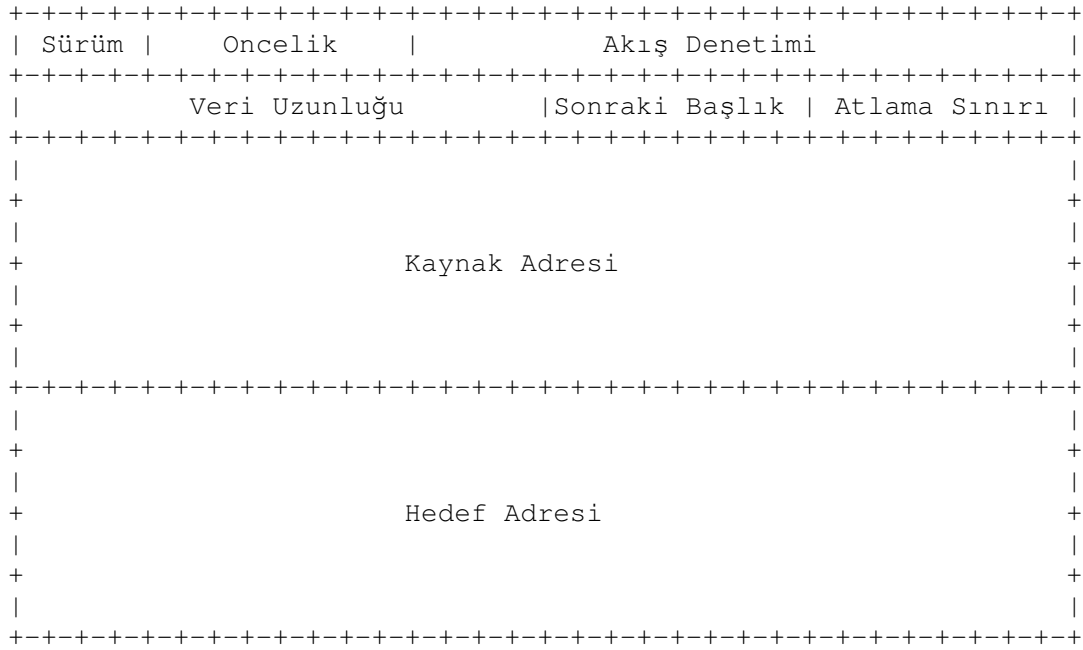
- Genişlemiş yönlendirme ve adresleme yeteneği
- Basitleştirilmiş başlık biçimi
- Gelişmiş seçenekler desteği
- Servis kalitesi yeteneği
- Doğrulama ve gizlilik yeteneği
- Mobil kullanıcıların bağlantı, güvenlik ve hız gereksinimlerini sağlayacak mimari

---

<sup>†</sup> Beykent Üniversitesinde Yarızamanlı görev almaktadır.

### 3. IPv6 Başlıkları

Bir IPv6 veri paketi başlığı, aşağıda gösterildiği gibi 32 bitlik 10 satırdan oluşmaktadır. [1][2]



Sürüm ( <i>Version</i> )	4-bit Internet Protokol sürüm numarasıdır. Bu sürümde her zaman 0110'dır.
Öncelik ( <i>Traffic Class</i> )	8-bit değer alan bu alan, paketin önceliğini belirler.
Akış Etiket ( <i>Flow Label</i> )	24-bitlik etiket trafik akışını belirtmek için kullanılır. Bu değer yönlendiricilerde gerçekleştirilen yönlendirme işlemini basitleştirdiğinden, yönlendirme tablosuna her paket için bakılması gerekliliğini ortadan kaldırır (MPLS).
Veriyükü Uzunluğu ( <i>Payload Length</i> )	16-bit işaretli tamsayı değeri alır. Bu değer taşınan asıl veri miktarını belirler.
Sonraki Başlık ( <i>Next Header</i> )	8-bit tamsayı değeri alır. Bir sonraki başlık türünün numarasını tanımlar.
Atlama Sınırı ( <i>Hop Limit</i> )	8-bit değer alır. Bir datagram'ın ne kadar uzağa gidebileceğini belirtir. Atlama Sınırı değeri sıfır olduğunda paket yok edilir.
Kaynak Adres ( <i>Source Address</i> )	128-bit paketin oluşturulduğu adresin değerini alır.
Hedef Adres ( <i>Destination Address</i> )	128-bit paketin gönderileceği adresin değerini alır.

#### 3.1. IPv6 Uzantı Başlıkları

IPv6'da seçimli internet katmanı bilgileri başlıklarla numaralandırılmayla birbirinden ayrılmıştır. Gelen numaraya ya IPv6 ek uzantı başlığı;ya da üst katman başlığı pakete eklenir. Bu 8-bitlik numara Sonraki Başlık (*Next Header*) değeri içerisindedir. Aşağıdaki şekilde sürecin nasıl gerçekleştirildiği gösterilmektedir.

IPv6 başlığı	TCP başlığı + veri		
Sonraki Başlık= TCP			
IPv6 başlığı	Yönlendirme Başlığı	TCP başlığı + veri	
Sonraki Başlık= Routing	Sonraki Başlık= TCP		
IPv6 Başlığı	Yönlendirme Başlığı	Parçalama Başlığı	TCP Parçalama başlık + veri
Sonraki Başlık= Yönlendirme	Sonraki Başlık= Parçalama	Sonraki Başlık= TCP	

Her uzantı başlığının bir 8 bit uzunluğunda tam sayı değeri vardır. Hangi başlığın geleceği hem IPv6 başlığındaki hem de uzantı başlığındaki “*Sonraki Başlık*” değerine göre belirlenir. Uygulamalarda karşımıza sıklıkla aşağıdaki uzantı başlıkları gelmektedir.

0	Sıçrama Seçenekleri Başlığı <i>Hop-by-Hop Options Header</i>
60	Hedef Seçenekleri Başlığı <i>Destination Options Header</i>
43	Yönlendirme Başlığı <i>Routing Header</i>
44	Parçalama Başlığı <i>Fragment Header</i>
51	Doğrulama Başlığı <i>Authentication Header</i>
50	Kapsüllenmiş Güvenlik Veriyükü Başlığı <i>Encapsulation Security Payload Header</i>
60	Hedef Seçenekli Başlık <i>Destination Options Header</i>
	Üst katman Başlığı (TCP – UDP)

Eğer IPv6 başlığında bir fazla uzantı başlığı aynı paket içerisinde kullanılacak ise, başlıklar yukarıdaki sıraya göre sıralanacaktır.

Her bir başlık paket içerisinde yalnızca bir defa kullanılır. Sadece “Hedef Seçenekleri Başlığı” bunun dışındadır. İlk “Hedef Seçenekleri Başlığı” IPv6 paketi içerisindeki Hedef Adresi alanının ve sonraki başlık olan Yönlendirme Başlığı’nın seçeneklerini içermektedir. Üst Katman Başlığından önce kullanılan ise en son hedef’in seçenekleri içindir.

### 3.2. Sıçrama Seçenekleri Başlığı

Sıçrama Seçenekleri Başlığı, seçenekler teslim yolu boyunca tüm düğümlere taşımak için kullanılır. Başlık, IPv6 başlığındaki “Sonraki Başlık” alanının sıfır değeri ile tanımlanmıştır. Başlık yapısı aşağıdaki gibidir:

Sonraki Başlık	Uzn Bşl Uzun	
Seçenekler		

Sonraki Başlık (Next Header)	8-bit tamsayı değeri alır. Sıçrama Seçenekleri Başlığından bir sonraki başlık türünün numarası ile tanımlanır.
Uzantı Başlık Uzunluğu (Header Extension Length)	8-bit değer alır. Sıçrama Seçenekleri Başlığının kaç adet 8'lik oktet'den oluştuğunu gösterir. İlk 8 oktet dahil değildir.
Seçenekler (Options)	Değişken uzunlukta alan. Toplam uzunluğu 8 oktet'in tamsayı katıdır.

### 3.3. Yönlendirme Başlığı

Yönlendirme Başlığı, IPv6 kaynağında bir veya daha fazla sayıda listelenmiş olan yoldaki hedef düğümleri ziyaret eder. Yönlendirme başlığı, Sonraki başlıkta 43 değerinde tanımlanmış başlıktır.

Sonraki Başlık	Uzn Bşl Uzun	Yönl. Tür=0	Kalan Bölümler
Ayrılmış			
Adres [1]			
Adres [2]			
.			
.			
Adres [n]			

Sonraki Başlık (Next Header)	8-bit tamsayı değeri alır. Yönlendirme Başlığından bir sonraki başlık türünün numarası ile tanımlanır.
Uzantı Başlık Uzunluğu (Header Extension Length)	8-bit değer alır. Yönlendirme Başlığının kaç adet 8'lik oktet'den oluştuğunu gösterir. İlk 8 oktet dahil değildir.
Yönlendirme Türü (Routing Type)	8-bit ile tanımlanmış belirli Yönlendirme Başlığı değişkeni. Tanımlamalarda sıfır kabul edeceğiz.
Kalan Bölümler (Segment Left)	8-bit işaretli tamsayı. Kaç adet yönlendirme bölümü kaldığını gösterir. Paketin içerisinde gideceği toplam düğüm sayısından ziyaret ettikleri çıkarıldıktan sonraki değerdir.
Ayrılmış (Reserved)	32-bit'lik ayrılmış alan. Başlangıç gönderimde sıfırdır.
Adres [1....n] (Address [1....n])	1'den n'e kadar 128 bit'lik düğüm adresleri.

Yönlendirme Başlığı, IPv6 paketi Hedef Adres'i alan tanımını inceleme veya işleme süreçlerine sokmaz.

Yönlendirme Başlığında oluşturulan algoritmadaki sürecin nasıl geliştiğini bir örnekle görelim: İstanbul düğümünün, Rize düğümüne Yönlendirme Başlığında Sinop, Samsun, Trabzon ara düğümlerini kullanarak bir paket göndereceğini varsayalım. IPv6 başlığı ve Yönlendirme Başlığının her bölüm taşıma yolundaki değerleri aşağıdaki gibi olacaktır.

Paket İstanbul'dan Sinop'a giderken:

Kaynak Adres = İstanbul	Uzn Bşl Uzun = 6
Hedef Adres = Sinop	Kalan Bölümler = 3
	Adres[1] = Samsun
	Adres[2] = Trabzon
	Adres[3] = Rize

Paket Sinop'tan Samsun'a giderken:

Kaynak Adres = İstanbul	Uzn Bşl Uzun = 6
Hedef Adres = Samsun	Kalan Bölümler = 2
	Adres[1] = Sinop
	Adres[2] = Trabzon
	Adres[3] = Rize

Paket Samsun'dan Trabzon'a giderken:

Kaynak Adres = İstanbul	Uzn Bşl Uzun = 6
Hedef Adres = Trabzon	Kalan Bölümler = 1
	Adres[1] = Sinop
	Adres[2] = Samsun
	Adres[3] = Rize

Paket Trabzon'dan Rize'ye giderken:

Kaynak Adres = İstanbul	Uzn Bşl Uzun = 6
Hedef Adres = Rize	Kalan Bölümler = 0
	Adres[1] = Sinop
	Adres[2] = Samsun
	Adres[3] = Trabzon

### 3.4. Parçalama Başlığı

Parçalama başlığı, IPv6'da kaynak hedefin istediği MTU'dan daha büyük boyutta bir paket gönderdiğinde kullanılır (IPv4'dekinden farklıdır, IPv6'daki parçalama sadece kaynak düğümde yapılır). Parçalama başlığı, Sonraki başlıkta 44 değerinde tanımlanmıştır. Başlık yapısı aşağıdaki gibidir.

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Sonraki Başlık | Ayrılmış | Parçalama Kayıklığı | Res|M|
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Tanıtıcı                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

Sonraki Başlık (Next Header)	8-bit tamsayı değeri alır. Parçalama başlığından bir sonraki başlık türünün numarası ile tanımlanır.
Ayrılmış (Reserved)	8-bit'lik ayrılmış alan. İletimde sıfır değeri ile karşılaşıldığında alan gözardı edilir.
Parçalama Kayıklığı (Fragment Offset)	13-bit'lik işaretli tamsayı değeri alır. Parçanın datagram içerisindeki yerini gösterir.
Res	2-bit ayrılmış alan. İletimde sıfır değeri ile karşılaşıldığında alan gözardı edilir.
M bayrağı (M flag)	1-bit'lik alan. 1 = parçalanma devam ediyor ; 0 = son parça
Tanıtıcı (Identification)	32-bit'lik alan. Parçaları birleştirmek için kullanılır. Aynı datagramın bütün tanıtıcıları aynıdır.

Kaynak her paket parçalama için bir tanıtıcı değer oluşturur. Tanıtıcı değer, aynı kaynak ve hedef adresleri değerlerine sahip olan diğer parçalanmalardan farklı olmalıdır.

İlk büyük, parçalanmamış paket "asıl paket" olarak adlandırılır ve aşağıda gösterildiği gibi iki bölümden oluştuğu düşünülür.

```
Asıl paket :
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Parçalanmayacak |                               Parçalanacak                               |
|      kısım      |                               kısım                               |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

Parçalanmayacak kısım, düğümlerde ve yönlendiricilerde işleme girecek IPv6 başlığı ve diğer uzantı başlıklarından oluşmaktadır. Gelebilecek olan uzantı başlıkları, eğer kullanılacaksa, Yönlendirme ve Sıçrama Seçenekleri başlıklarıdır. Bunlardan başka kullanılmaz.

Parçalanacak kısımda, paketin geri kalanı , sadece hedef düğümde işleme girecek olan diğer uzantı başlıkları, üst katman başlığı ve veriden oluşmaktadır.

Asıl paketteki parçalanacak kısım, bölümlere parçalanır. Her parça, sağdan başlayarak, 8 oktet uzunluğuna kadar bir tamsayı alır. Bölümler birbirlerinden ayrı olarak aşağıdaki şekildeki gibi gönderilir:

```
asıl paket :
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Parçalanmayacak | ilk | ikinci | ... | son |
|      kısım      | parça | parça | ... | parça |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

parçalanmış paket:

Parçalanmayacak kısım	Parçalama başlığı	ilk parça
Parçalanmayacak kısım	Parçalama başlığı	ikinci parça
Parçalanmayacak kısım	Parçalama başlığı	son parça

Her bir parça paket aşağıdakileri oluşturdu:

1. Asıl paketteki parçalanmayacak kısımda, IPv6 paketindeki Veriyükü Uzunluğu her parçanın uzunluğuyla (IPv6 başlığının kendisi dışında) ve Parçalanmayacak Kısımdaki son başlıkta Sonraki Başlık alanı 44 ile değiştirildi
2. Parçalama başlığının içerdikleri:

Asıl pakette Parçalanacak Kısım'ın içerdiği ilk başlıktaki Sonraki Başlık değeri.

Parçalama Kayıklığı, 8 oktet'lik parçalama kısımlarıyla ilişkili olarak asıl paket'e yazar. İlk parçalama kayıklığı parçasının değeri 0'dır.

Paketin parçalarının devamının geleceğini göstermek için M=1 yapar, son pakette M'e 0 değeri atanır.

Asıl pakette Tanıtıcı değer oluşturuldu.

Hedef düğümde, parçalanmış kısımlar orijinaline ve gelen değerlere göre aşağıdaki şekle uygun olarak birleştirilir.

Birleştirilmiş asıl paket:

Parçalanmayacak kısım	Parçalanacak kısım
--------------------------	-----------------------

Aşağıdaki kurallara göre birleştirildi:

Asıl paket'in birleştirilmesi ancak parçalanmış paketlerin tümü aynı Kaynak Adresine, Hedef Adresine ve Parçalama Kayıklığına sahip olduğunda yapılır.

Asıl paketteki Parçalanmayacak Bölüm birleştirildiğinde, Parçalama Kayıklığı 0 olan aşağıdaki işlemlerden geçtikten sonra Parçalama Başlığı olarak konur.

Veriyükü uzunluğu son parça geldikten sonra hesaplanarak alana eklenir. Sonraki başlık değeri ilk parçalanmış kısım içeri incelendikten sonra alana eklenir.

### 3.5. Doğrulama Başlığı

Doğrulama Başlığı bağlantısız bütünlük ve veri kaynağından IP datagramıyla doğrulama yapılmasını sağlar. Bunların dışında verinin tekrarına karşı güvenlik sağlar (*Anti-Reply Service*). Doğrulama Başlığı, üst katmana verilerin taşınmasında IP başlığından daha güvenli bir doğrulama sağlar. Doğrulama başlığı, Sonraki Başlıkta 51 değerinde tanımlanmıştır. Başlık yapısı aşağıdaki gibidir:[3][6]

```
+-----+
| Sonraki Başlık | Veriyükü Uzun. | Ayrılmış |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Güvenlik Parametresi Dizini (GPD) |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Sıra Numarası Alanı |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Doğrulama Verisi (değişken) |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

Sonraki Başlık ( <i>Next Header</i> )	8-bit tamsayı değeri alır. Doğrulama başlığından bir sonraki başlık türünün numarası ile tanımlanır.
Veriyükü Uzunluğu ( <i>Payload Length</i> )	8-bit işaretli tamsayı değeri alır. Bu değer taşınan asıl veri miktarını belirler.
Ayrılmış ( <i>Reserved</i> )	16-bit ayrılmış alan. İletimde sıfır değeri ile karşılaşıldığında alan gözardı edilir.
Güvenlik Parametresi Dizini ( <i>Security Parameters Index</i> )	32-bit ayrılmış alan. Güvenli tanımlama için ortak bir değer.
Sıra Numarası Alanı ( <i>Sequence Number</i> )	
Doğrulama Verisi ( <i>Authentication Data</i> )	

AH, Kapsüllenmiş Güvenlik Veriyükü (Encapsulation Security Payload – ESP) gibi iki yöntemle kullanılır: Taşıma modu veya tünelleme modu. Taşıma modu birincil olarak üst katman (TCP ve UDP gibi) protokollerinin korunması için tasarlanmıştır. Tünelleme modu ise bir IP paketi başka bir IP paketinin taşıma verisi olmaktadır. Bu yöntemde içerdeki IP paketi, başlığı ile birlikte kriptolanmakta, dış başlık ise bu kriptolanmış paketin ağ üzerinde, yönlendirilmiş olduğu ağa ulaştırılmasını sağlamaktadır. Uçlar hem taşıma ve hem de tünel çalışma şekillerinde işletilebilirken, güvenlik geçitleri sadece tünel çalışma şeklinde yapılandırılabilirler (Geçit uç rolünü üstlendiğinde her iki çalışma şeklini de destekleyebilir).

AH Uygulamadan Önce - Taşıma modu

```
+-----+-----+-----+-----+-----+-----+-----+-----+
| Asıl IP | Varsa Uzantı | | |
| Başlığı | Başlığı | TCP | Veri |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

AH Uygulamadan Sonra - Taşıma modu

```
+-----+-----+-----+-----+-----+-----+-----+-----+
| Asıl IP | hedef, sıçrama, | | Hedef | | |
| Başlığı | yönlendirme, parçalama | AH | Seçen. | TCP | Veri |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

IPv6'daki AH genel durumu, AH noktadan noktaya veriyükü incelemesi yapılması ve böylece sıçrama seçenekleri, yönlendirme ve parçalama uzantı başlıkları izlenmesini sağlar. Hedef seçenekleri uzantı başlığı ihtiyaca göre AH'den önce veya sonra yerleştirilir.

Tünel çalışma modunda asıl IP paketi, kapsülleyen IP paketinin taşıma verisi olur; kapsülleyen IP paketi başlığı ve taşıma verisi arasına taşıma modunda olduğu gibi bir güvenlik başlığı eklenir. Tünel çalışma modunda, iç IP başlığı kaynak ve hedef adreslerini taşır, buna karşın dış IP başlığı farklı IP adreslerini içerir (güvenlik geçidi adresi gibi). Bu modda, AH bütün iç IP paketini IP başlıkları dahil tüm içeriklerini korur. Aşağıdaki şekilde AH tünel modundaki durumu gösterilmiştir.

AH Uygulamadan Sonra - Tünelleme modu

```

+-----+
| Yeni IP | Varsa Uzantı|   | Asıl IP | Varsa Uzantı|   |   |
| Başlığı | Başlığı      | AH| Başlığı | Başlığı      |TCP|Veri |
+-----+

```

### 3.6. Kapsüllenmiş Güvenlik Veriyükü Başlığı

Kapsüllenmiş Güvenlik Veriyükü (Encapsulation Security Payload – ESP) başlığı IPv6'da güvenlik servisi sağlaması için tasarlanmıştır. ESP bazen tek başında bazen de AH ile beraber kullanılır. Güvenlik servisi, iletişimdeki iki düğüm arasında, iki güvenlik geçityolu arasında veya bir düğüm bir güvenlik geçityolu arasında sağlanabilir.[4]

ESP başlığı IP başlığından sonra, üst katman (TCP, UDP gibi) başlığında önce kullanıldığında taşıma modu veya kapsüllenmiş IP başlığından sonra kullanıldığında tünelleme modunda kullanılmış olur. ESP, Sonraki başlıkta 50 değerinde tanımlanmıştır. Başlık yapısı aşağıdaki gibidir.

```

+-----+
|           Güvenlik Parametresi Dizini (SPI)           |
+-----+
|           Sıra Numarası                               |
+-----+
|           Veriyükü (varsa)                           |
.                                                     .
|                                                     |
+-----+
|           |           Dolgu Verisi (0-255 byte)       |
+-----+
|           |           Dolgu Boyu   |Sonraki Başlık   |
+-----+
|           Doğrulama Verisi (varsa)                   |
.                                                     .
|                                                     |
+-----+

```

Güvenlik Parametresi Dizini ( <i>Security Parameters Index</i> )	32-bit ayrılmış alan. Güvenli tanımlama için ortak bir değer
Sıra Numarası Alanı ( <i>Sequence Number</i> )	32-bit'lik artan sayıda sıra numarası değeridir.
Veriyükü Verisi ( <i>Payload Data</i> )	Değişken uzunlukta alan. Sonraki başlığın içeriği bu alanda bulunmaktadır.
Dolgu ( <i>Padding</i> )	16-bit ayrılmış alan. İletimde sıfır değeri ile karşılaşıldığında alan gözardı edilir.

Dolgu Uzunluğu ( <i>Padding Length</i> )	8-bit'lik alan, dolgunun boyunu 0-255 byte ölçüsünde değerini koyar
Sonraki Başlık ( <i>Next Header</i> )	8-bit tamsayı değeri alır. Doğrulama başlığından bir sonraki başlık türünün numarasını tanımlanır.
Doğrulama Verisi ( <i>Authentication Data</i> )	Değişken uzunluktaki bu alan, paketin Bütünlük Denetim Değerini (Integrity Check Value – ICV) içermektedir.

AH başlığı gibi, ESP iki yöntem kullanılır: taşıma modu veya tünelleme modu. Taşıma modu, ESP IP başlığından sonra ve üst katman protoklünden (TCP, UDP gibi) sonra geldiğinde geçerli olur. ESP noktadan noktaya veriyükü incelemesi yapılması ve böylece sıçrama seçenekleri, yönlendirme ve parçalama uzantı başlıkları izlenmesini sağlar. Hedef seçenekleri başlığı ESP başlıklarının arasında olduğundan şifrelenir. Aşağıdaki şekilde gösterilmiştir.[8]

ESP uygulanmadan önce - Taşıma modu

```

+-----+
| Asıl IP   | Varsa Uzantı|           |           |
| Başlığı  | Başlığı      | TCP | Veri |
+-----+

```

ESP Uygulandıktan sonra - Taşıma modu

```

+-----+
| Asıl IP | hedef, sıçrama,           | hedef |   |   | ESP | ESP |
| Başlığı | yönlendirme, parçalama|ESP|seçe. |TCP|Veri| Eki | Doğr|
+-----+
|<----taşıma verisi---->|
|<----- doğrulanmış ---->|

```

Tünelleme modunda ESP, hem düğümde hem de güvenlik geçitinde kullanılabilir. Eğer ESP güvenlik geçiti olarak tanımlandığında tünelleme modu kullanılması gerekir. Tünelleme modunda, iç IP başlığı kaynak ve hedef adreslerini taşır, dış IP başlığı ise farklı bir IP adresi içerir( güvenlik geçiti adresi gibi). Tünelleme modunda ESP, bütün iç IP paketini ve iç IP başlığını korur. Aşağıdaki şekilde ESP'nin tünelleme modundaki durumu gösterilmiştir.

```

+-----+
| Yeni IP |Yeni Uzntı |   |Asıl IP|Asıl Uzantı|   |   | ESP | ESP |
| Başlığı | Başlığı   |ESP|Başlığı|Başlığı   |TCP|Veri| Eki | Doğr|
+-----+
|<-----taşıma verisi----->|
|<----- doğrulanmış ----->|

```

#### 4. Adresleme Yapısı

IPv6, arabirimler için 128-bit'lik adres yapısında tanımlanmıştır. Üç çeşit adresleme yapısı vardır:[5][7]

Unicast: Tek bir arabirim için tanımlanmıştır. Bir veri paketi unicast adres'e gönderildiğinde adresin tanımlı olduğu arabirim paketi alır.

Anycast : Birkaç arabirim için tanımlanması belirlenmiştir. Genellikle uygun olan farklı bir düğüm içindir. Bir veri paketi anycast adres'e gönderildiğinde adresin tanımlı olduğu bir düğüm paketi alır.

Multicast: Birkaç arabirim için tanımlanmıştır. Bir veri paketi multicast adres'e gönderildiğinde, bu adres'e tanımlı tüm düğümler paketi alır.

IPv6 broadcast adres yoktur, bu fonksiyonun yerine multicast adres tanımlaması geçmiştir.

#### 4.1. Adres Modeli

IPv6'nın tüm adresleri, çeşitleri düğümler için tanımlanmaz, arabirimler için tanımlanır. Bir IPv6 Unicast adres tipi tek bir arabirim ile ilgilidir. Her arabirim bir düğüm için kullanılmaktadır.

Tüm arabirimlerin en az bir tane link-local unicast adresine sahip olması gerekmektedir. Bir arabirim çeşitli IPv6 tiplerine (unicast, anycast, multicast) veya bunların anlama yeteneğine sahip olabilir.

Güncel olarak IPV6 ,IPv4 modeline altağ öntakısı ile birleştirilerek bağlantıda kullanılıyor. Birçok altağ öntakıları ayrılmış aynı bağlantıda kullanılıyor.

#### 4.2. Adreslerin Gösterilişi

IPv6 adres yapısının dizisinde üç çeşit geleneksel biçim gösterilişi bulunmaktadır:

1. x:x:x:x:x:x:x:x sunulmasında ,x'lerin yerine sekiz tane 16-bit'lik hexadesimal değeri verilmektedir.

Örnek:

```
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417A
```

Önemli bir nokta da her alanda temel olarak bulunan sıfırların yazılması zorunlu değildir; ama her alanda nümerik bir değer girilmesi gerekmektedir (2. bölümde detaylı olarak anlatılacaktır).

2. IPv6'da adresleme yapısında kolaylıkla kullanılması için bazı metotlara sahiptir. IPv6'da uzun adres dizilerinde sıfırlar bulunmaktadır. Adres yapısındaki düzende sıfırları yazmaktansa sıkıştırılmış bir sıfır sözdizimi özelliği getirilmiştir. Sıfırların yerine ":", bir veya daha fazla 16 bitlik grupların yerine kullanılır. "::" sözdizimi adreste sadece bir kez kullanılır. "::" 'i temel veya izleyen sıfırları sıkıştırmak için kullanılır.

Örnek:

```
1080:0:0:0:8:800:200C:417A bir unicast adresi
FF01:0:0:0:0:0:0:101 bir multicast adresi
0:0:0:0:0:0:0:1 bir loopback adresi
0:0:0:0:0:0:0:0 tanımsız adres
```

Gösteriliş Şekli:

```
1080::8:800:200C:417A bir unicast adresi
FF01::101 bir multicast adresi
::1 bir loopback adresi
:: tanımsız adres
```

3. IPv6'ya geçişin aşamalar halinde olması öngörüldüğünden bazı durumlarda IPv4 ile IPv6'nın birleştirilmesini gerektiren ortamlar olacaktır. Bu durumlarda uygun bir yapı olan x:x:x:x:x:x:d.d.d.d kullanılması gerekmektedir. Burada 'x'ler adreslerde altı adet 16-bitlik hexadesimal değer almaktadır ve 'd'ler ise adreslerde dört adet 8-bitlik desimal adres değeri (öngörülen IPv4 değeri)almaktadır.

Örnek:

```
0:0:0:0:0:0:13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38
```

değiştirilmiş durumda;

```
::13.1.68.3
::FFFF:129.144.52.38
```

### 4.3. Adres Öntakılarının Gösterilişi

IPv6'daki adres öntakı gösteriliş şekli, IPv4'deki adres öntakı gösterilişindeki CIDR sistemiyle aynıdır. IPv6'daki adres öntakı gösteriliş sistemi:

```
ipv6-adresi/öntakı-uzunluğu
```

şeklindedir.

ipv6-adresi	herhangi bir IPv6 adres gösterilişi
öntakı-uzunluğu	bir desimal değerdir, adresin soldan kaç adet bit öntakısından oluştuğunu gösterir.

Örnek olarak, aşağıdaki uygun gösterilişli öntakısı 60-bit 12AB00000000CD3 (hexadesimal) ele alalım:

```
12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30:0:0:0:0/60
12AB:0:0:CD30::/60
```

kurallara uymayan öntakı gösterilişleri:

12AB:0:0:CD3/60	temel sıfırları kesmektedir;ama gerekli sıfırları değil
12AB::CD30/60	adres sola doğru genişlemektedir.
12AB:0000:0000:0000:0000:000:0000:CD30	
12AB::CD3/60	adres sola doğru genişlemektedir.
12AB:0000:0000:0000:0000:000:0000:0CD3	

Eğer bir düğüm adresi ve bir düğümün öntakı adresi birlikte yazılmak istenirse (ör: düğümün altağ öntakısı), aşağıdaki iki yöntem de kullanılabilir:

12AB:0:0:CD30:123:4567:89AB:CDEF	düğüm adresi
12AB:0:0:CD30::/60	düğümün altağ adresi
12AB:0:0:CD30:123:4567:89AB:CDEF/60	kısaltılmış şekli

#### 4.4. Adres Türü Tanımlamaları

IPv6 adres türleri tanımlamasında adres bitlerindeki en anlamlı bit'e göre yapılır.

Adres türü	İkili öntakı	IPv6 notasyonu
Tanımsız	00...0 (128 bit)	::/128
Loopback	00...1 (128 bit)	::1/128
Multicast	11111111	FF00::/8
Link-local unicast	1111111010	FE80::/10
Site-local unicast	1111111011	FEC0::/10
Genel unicast	Geri kalan tümü	

Anycast adres boşluğu, her alanda unicast adres boşluğundan alır ve sözdiziminde unicast'den ayırt edilmez.

#### 5. Referanslar

- [1] R. Hinden, S. Deering, RFC 2460 Internet Protocol version 6 (IPv6) Specification
- [2] R. Çölkesen, B. Örencik, Bilgisayar Haberleşmesi ve Ağ Teknolojileri 3.Baskı
- [3] S. Kent, R. Atkinson, RFC 2402 IP Authentication Header (AH)
- [4] S. Kent, R. Atkinson, RFC 2406 IP Encapsulation Security Payload (ESP)
- [5] R. Hinden, S. Deering, RFC 3513 Internet protocol Version 6 (IPv6) Address Architecture
- [6] W. Stallings, Network Security Essentials Application and Standards
- [7] P. Grossetete, IPv6 Protocols and Standards presentation
- [8] Y. Kaplan, Veri Haberleşmesi Temelleri