

IPv6

Prof. Dr. Resul KARA

IPv6

- 1990'lı yılların başlarından itibaren İnternet'in hızla genişlemesi, eklenen uç sayısı ve çeşitliliğinde gözlenen artış nedeniyle, İnternet protokolü sürüm 4 (IPv4)'ün İnternet'e bağlanacak cihazların adreslemesi için yetersiz kalacağı ve yeni bir adresleme sistemine geçişin zorunlu olacağı vurgulanmaya başlanmıştır.
- Bu kapsamdaki çalışmalar IETF (Internet Engineering Task Force) önderliğinde başlamış ve yeni protokolün IPng (Internet Protocol next generation) veya İnternet protokolü sürüm 6 (IPv6) olarak adlandırılması kararlaştırılmıştır. Yeni İnternet protokolünün standartları 1998 yılı sonunda yayınlanan RFC 2460 belgesinde tanımlanmıştır.
- IPv4'ün 32-bitlik adres yapısı teorik olarak 4 milyardan fazla ($2^{32}=4.294.967.296$) kullanılabilir adres sunmaktadır. Ancak pratikte verimsiz adres atama mekanizmalarından dolayı etkin adres sayısı bu sayıya hiçbir zaman ulaşamamaktadır.
- 128-bitlik bir adres yapısına sahip olan IPv6 ise teorik olarak 340 trilyondan fazla ($2^{128}=340.282.366.920.938.463.463.374.607.431.768.211.456$) İnternet adresi sunmaktadır.

IPv4'ün Eksiklikleri

- İnternetin her geçen gün artan bir hızla büyümesi ve İnternet'e bağlı cihaz sayısının artması nedeniyle IPv4 adres uzayı yetersiz kalmıştır. Bu sıkıntıyı aşmak için pek çok kurum Ağ Adresi Çevirimi (Network Address Translation - NAT) gibi adres dönüştürücü mekanizmaları kullanmayı seçmiştir. Uçtan uca adresleme sağlayamayan IPv4, İnternet üzerinden sunulan servis çeşitliliğinin artması ve bazı servislerin NAT arkasındaki kullanıcılara ulaştırılmasında yaşanan işletim zorlukları gibi nedenlerle ihtiyaçları karşılamakta yetersiz kalmıştır.
- IPv4 adres uzayı hiyerarşik adresleme yapılmasına olanak sağlayamamıştır. Bu durum yönlendirici cihazlarının yönlendirme tablolarının büyümesine yol açmıştır.
- IPv6 için geliştirilen ancak daha sonra IPv4 için de uyarlanan IPsec standardının kullanımı ile güvenlik altyapısı sağlanabilmektedir. Ancak özellikle NAT kullanılan IPv4 ağlarında, bu standardın kullanımı sorunlara sebep olmaktadır.

IPv4'ün Eksiklikleri

- IPv4 adres yapılandırması statik olarak veya DHCP kullanarak yapılabilmektedir. Ancak IP adresleri gereksiniminin artması nedeniyle yeni bir otomatik yapılandırma yöntemi geliştirilmesine ihtiyaç duyulmuştur.
- Gerçek zamanlı veri aktarımında, IPv4 paket başlığında bulunan “Servis Tipi” (Type of Service) TOS alanı kullanılarak belli bir servis kalitesi (Quality of Service) sağlanabilmektedir. Ancak TOS alanı kullanımı kısıtlıdır ve şifreli aktarımlarda sorun yaratmaktadır.

IPv6'nın Avantajları

- **Genişletilmiş adres alanı:** IPv6'nın en önemli özelliklerinden biri 128 bitlik adres uzunluğu ile IPv4'e göre daha büyük bir adres alanı sunmasıdır. IPv6'daki bu geniş adres alanı, hiyerarşik adresleme yapılmasına olanak sağlayarak, yönlendirme tabloları boyutlarının küçülmesini sağlayacaktır.
- **Yeni Güvenlik Özellikleri:** IPv6 güvenlik konusunda da bazı üstünlüklere sahiptir. Öncelikle İnternet Protokol Güvenliği (Internet Protocol Security - IPsec) desteği IPv6'da bütünleşik olarak gelmektedir. Bu bütünleşme ile servislerin daha sorunsuz ve etkin çalışması sağlanmaktadır.
- Güvenlik için tanımlanmış ek başlıklar ile yetkilendirme ve şifreleme yapılabilmektedir. Ayrıca IPv6'da ara düğümlerde paketlerin parçalanmadan aktarılması, yeni başlık yapısı ile ağ üzerinde paketlerin izlenmesinin kolaylaşması gibi güvenlik bütünlüğünü sağlayan yeni özellikler de mevcuttur.

IPv6'nın Avantajları

- ❑ **Sadeleştirilmiş Başlık Yapısı:** IPv6 paketleri yönlendiriciler tarafından daha hızlı işlenebilmelerine olanak sağlayan sabit uzunlukta yeni bir başlık yapısına sahiptir. IPv4 başlığındaki gereksiz bazı alanlar atılmış, bazıları ise isteğe bağlı kullanım için uzantı başlıkları kısmına kaydırılmıştır.
- ❑ **Gelişmiş Servis Kalitesi Özellikleri:** İnternet Protokolü, doğası gereği farklı uygulamaların hepsini en iyi çaba (best effort) yaklaşımı ile fark gözetmeksizin ele alır. Bu durum, uçtan uca gecikme veya paket kayıpları gibi parametrelere karşı duyarlı olan trafik için problemlere yol açabilmektedir.
- ❑ **Otomatik Adres Yapılandırılması:** Otomatik adres yapılandırılması IPv6'nın getirmiş olduğu önemli yeniliklerdendir. IPv6, ağ üzerinde adres atama sunucusu olmaksızın, ağa bağlı arabirimlerin adres edinmelerine olanak tanır. Bu özelliğin temelinde ağdaki yönlendiricilerin gerekli adres önekini anons etmeleri ve istemcilerin de bu bloğa 64 bitlik bir değer ekleyerek kendi adreslerini oluşturmaları yatar. Bu şekilde oluşturulan adreslerin kullanılmadan önce '*tekillik testi*'nden (Duplicate Address Detection Mechanism) geçirilmesi gerekir. Düğümler başkaları tarafından kullanılmadığına kanaat getirdikleri adresi kullanıma alabilir.

IPv6'nın Avantajları

- ❑ **Dolaşılabilirlik:** Dolaşılabilirlik, bir istemcinin farklı ağlardan “gerçek ev adresi” ile bağlantı yapabilmesidir.
- ❑
- ❑ **Genişletilebilirlik:** IPv6'da zorunlu başlık alanının dışında bulunan ve isteğe bağlı kullanılabilen uzantı başlıkları bölümü, ileride ihtiyaç duyulabilecek yeni özellikler için kullanılabilir.
- ❑
- ❑ **Komşu Düğümlerle Etkileşim İçin Yeni Protokol:** IPv6 Ağlarında aynı bağlantı üzerindeki komşu düğümlerin etkileşimini yönetmek için yeni bir protokol olan Komşu Keşfi (Neighbor Discovery) Protokolü kullanılır. Bu protokol, “Internet Control Message Protocol for IPv6” (ICMPv6) mesajlarını kullanır.

IPv6 Adres Mimarisi

- 128 bitlik IPv6 adresleri onaltılık sayı düzeni kullanılarak gösterilir
- Örnek bir adres:
0010000000000000100001101101110000000000000000000000000000000000
0000000000010101010100000000111111111111100010100010011100
01011010
- 128 bit olan bu IPv6 adresi öncelikle 16 bit uzunluğunda 8 gruba ayrılmıştır:
- | | | |
|-------------------|------------------|------------------|
| 00100000000000001 | 0000110110111000 | 0000000000000000 |
| 0000000000000000 | 0000001010101010 | 0000000011111111 |
| 1111111000101000 | 1001110001011010 | |
- Her grup onaltılık sayı düzenine dönüştürülür ve IPv6 adresi “:” ile ayrılan 16 bitlik bloklar halinde yazılır:
- 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A

IPv6 Adreslerinin Kısaltılması

- ❑ Her 16 bitlik blokta solda kalan sıfırlar adresten atılabilir:
- ❑ 2001:DB8:0:0:2AA:FF:FE28:9C5A
- ❑
- ❑ Tamamı sıfırdan oluşan bloklar fazladan bir adet daha “:” kullanılarak adresten çıkarılabilir. Ancak “::” bir IPv6 Adresinde en fazla 1 kez kullanılabilir. Bu nedenle IPv6 adresinden 1’den fazla blok çıkarılabilmesi için bu blokların yan yana olması zorunludur:
- ❑ 2001:DB8::2AA:FF:FE28:9C5A

Adres Sınıfları Var mı?

- IPv6'da IPv4'ten farklı olarak adres aralığını belirleyen A, B ve C gibi sınıflar tanımlanmamıştır. IPv6 adresleri için CIDR (Classless Inter-Domain Routing) gösterimi kullanılmaktadır.
- Bu gösterimde IPv6 adresinde ağ adresini belirleyen bit sayısı adres sonunda “/” işareti kullanılarak verilmektedir. Yönlendirici cihazlar, IPv6 paketlerini yönlendirme işleminde ağ adresini belirleyen bu bitleri kullanmaktadır.
- 2001:DB8::2AA:FF:FE28:9C5A /32

IPv6 Adres Tipleri

- ❑ **Tekil Gönderim IPv6 Adresleri:** Tekil gönderim adresleri, tek bir ağ arayüzünü tanımlamak için kullanılmaktadır. Bu tip bir adresi hedefinde bulunduran paketler, tek bir arayüzüne iletilmektedirler.
- ❑
- ❑ • **Çoklu Gönderim (Multicast) Adresleri:** Bu tip adresler, farklı arayüzlerden oluşturulmuş bir grubu tanımlamak için kullanılmaktadır. Hedefi çoklu gönderim adresi olan paketler, gruba dâhil olan tüm arayüzlere iletilmektedir.
- ❑
- ❑ • **Herhangi Birine Gönderim (Anycast) Adresleri:** Herhangi birine gönderim adresleri de çoklu gönderim adresleri gibi, farklı arayüzlerden oluşturulmuş bir grubu tanımlamaktadır. Herhangi birine gönderim adresine yönelmiş bir paket, çoklu gönderimden farklı olarak sadece grubun en yakındaki üyesine iletilir. Bu adres tipleri özellikle yük dağılımı uygulamalarında kullanılır. Aynı servisi veren birden fazla sunucu bulunması durumunda bu sunucuları aynı gruba dâhil ederek istemcilerin kendilerine en yakının sunucudan servis alması sağlanabilir.

IPv6 Adres Tipleri

- IPv6 adresleri “biçim önek” (format prefix) olarak adlandırılan ilk bitlerine göre sınıflandırılmaktadır. Başlangıç olarak IPv6 adres aralığının yaklaşık %15’lik kısmı için kullanım alanı ataması yapılmıştır. Geriye kalan adres aralıkları ilerideki ihtiyaçlar doğrultusunda kullanılacak olup, atama daha sonra yapılacaktır.

Atama	Biçim Öneki (İkili Değer)	IPv6 Adres aralığı	Toplam Adres Aralığındaki Oranı	Toplam Adres Aralığındaki Yüzdesi
Rezerve edilmiş	0000 0000	0::/8	1/256	%0.39
Küresel Tekil Gönderim (Global Unicast) Adresleri	001	2000::/3	1/8	%12.5
Eşsiz Yerel Tekil Gönderim (Unique Local Unicast) Adresleri	1111 1100	FC00::/7	1/128	%0.78
Bağlantı Yerel Tekil Gönderim (Link Local Unicast) Adresleri	1111 1110 10	FE80::/10	1/1024	%0.10
Çoklu Gönderim (Multicast) Adresleri	1111 1111	FF00::/8	1/256	%0.39

IPv6 Adres Tipleri-Rezerve

- ❑ **Rezerve Edilmiş Aralık:** Rezerve edilmiş durumda olan 0::/8 aralığı aşağıda açıklanan özel
- ❑ IPv6 adresleri için kullanılmaktadır.
- ❑ **Belirsiz Adres (Unspecified Address):** 0:0:0:0:0:0:0:0 veya :: şeklinde gösterilen ve IPv4'teki karşılığı 0.0.0.0 olan adrestir. Belirsiz Adres herhangi bir cihaza verilemez. Bu adres genelde soket bağlantılarında kullanılmaktadır.
- ❑ **Yerel İstemci Adresi (Loopback Address):** 0:0:0:0:0:0:0:1 veya ::1 şeklinde gösterilmektedir. Bu adresin IPv4'teki karşılığı 127.0.0.1'dir. Kaynağı veya hedefi bu olan adresler göndericiden ayrılamaz.
- ❑ **IPv4 Eşlemlili IPv6 Adresleri (IPv4-Mapped Addresses):** ::ffff:0:0/96 aralığı içerisinde yer alan IPv6 adresleridir. Bu adres aralığı, IPv4 ve IPv6 paket başlıkları arasında RFC 2765 ile tanımlanan SITT (Stateless IP/ICMP Translation) algoritmasını kullanarak dönüşüm sağlamak için ayrılmıştır. Bu algoritma, sadece IPv6 adresine sahip arayüzlerin, sadece IPv4 adresine sahip arayüzler ile iletişimini sağlamak için kullanılmaktadır. Adres dönüşümünde kullanılan IPv4 adresinin küresel olarak yönlendirilebilen adresler olması gerekmektedir.

IPv6 Adres Tipleri-Küresel Tekil

- **Küresel Tekil Gönderim Adresleri:** 001 biçim öneğine sahip ve arayüzlerin küresel bağlantısı için zorunlu olan adreslerdir. Bu adresler IP adresi dağıtımı ve koordinasyonu ile görevli merci olan Internet Assigned Numbers Authority (IANA) tarafından Avrupa, Kuzey Amerika, Latin Amerika, Afrika ve Asya Bölgesel IP Adresi Dağıtım Yetkililerine, ihtiyaç duyan kurumlara tahsis edilmek üzere dağıtılmıştır. Dolayısıyla bu adresler doğrudan IP adresi dağıtım yetkilisi olan kuruluşlardan veya hizmet alınan İnternet Servis Sağlayıcısı kurumdan alınabilir.
- “Biçim Öneki” ve “Küresel Yönlendirme Öneki” kısımlarından oluşan ilk bölümün bit uzunluğu değişebilmektedir. IP dağıtım yetkilisi tarafından İnternet Servis Sağlayıcı olmayan kurumlara tahsis edilen bu bitlerin sayısı genellikle 48’dir. Bu bölümü takip eden “Alt Ağa Tanıtıcı” bölümü de değişken olmakla Birlikte örnek için 16 bittir. Son bölüm olan “Arabirim Tanıtıcısı” ise genellikle 64 bitlidir.

001	Küresel Yönlendirme Öneki	Alt ağa Tanıtıcı	Arabirim Tanıtıcısı
	n bit	m bit	128-m-n bit

IPv6 Adres Tipleri-Küresel Tekil

- Küresel tekil gönderim adresleri arasından yer alan 2001::/32 adres aralığı IPv4 ve IPv6 arayüzleri arasında iletişim için kullanılan özel bir geçiş mekanizması olan “Teredo Tünelleme” yöntemi için ayrılmış durumdadır.
- 2002::/16 aralığı “6to4 geçiş yöntemi” için ayrılmıştır.

IPv6 Adres Tipleri-Eşsiz Yerel Tekil

- *Eşsiz Yerel Tekil Gönderim Adresleri:* İlk 7 biti 1111110 şeklinde olan ve FC00::/7 aralığında bulunan adreslerdir. Öncelikle, ardından gelen L bitinin değeri 1 olan FD00::/8 alt aralığı kullanılmaktadır. L bitinin 0'a eşit olduğu adresler henüz tanımlanmamıştır. L bitinden sonraki 40 bit, algoritma yardımıyla üretilen “Küresel Tanıtıcı” bölümünü oluşturmaktadır. Bu bölümü, sırasıyla 16 bitlik “Alt Ağ Tanıtıcısı” ve 64 bitlik “Arabirim Tanıtıcısı” takip etmektedir.
- Eşsiz yerel tekil gönderim adresleri yerel ağ trafiği için geliştirilmiş olup, küresel olarak yönlendirilmezler.

1111110	L	Küresel Tanıtıcı	Alt Ağ Tanıtıcısı	Arabirim Tanıtıcısı
7 bit		40 bit	16 bit	64 bit

IPv6 Adres Tipleri-Bağlantı Yerel Tekil

- *Bağlantı Yerel Tekil Gönderim Adresleri:* 1111 1110 10 biçim öneğine sahip ve FE80 ile başlayan adreslerdir. Biçim önekini takip eden 54 bit 0 olup, onları takip eden ve arabirim tanıtıcısı olan son 64 bit ise arabirimin 48 bitlik donanım adresinin tam ortasına 16 bitlik FFFE değeri eklenerek oluşturulur.
- Bağlantı yerel tekil gönderim adresleri, sadece bir arayüz bağlantısı üzerinde otomatik adres yapılandırılması veya komşu keşfi gibi amaçlar ile kullanılan yerel adreslerdir.

1111111010	0	Arabirim Tanıtıcısı
10 bit	54 bit	64 bit

IPv6 Adres Tipleri-Çoklu Gönderim

- *Çoklu Gönderim Adresleri:* ff00::/8 IPv6 öneki çoklu gönderim adresleri için tahsis edilmiştir. Şekil 5'te bu adreslerin yapısı ayrıntılı olarak verilmiştir.

1111111	Bayrak	Kapsam	Grup Tanıtıcısı
8 bit	4 bit	4 bit	112 bit

IPv6 Adres Tipleri-Çoklu Gönderim

- ❑ 11111111 olan ilk 8 bit sonrasında, adresin tipini belirleyen “Bayrak” ve “Kapsam” bitleri
- ❑ gelmektedir.
- ❑ Bayrak bitleri aşağıdaki değerleri alabilir:
 - 4 bitin ilki ileriki kullanım için rezerve edilmiştir ve 0 değerini almalıdır.
 - İkinci bit (R) çoklu gönderim adresinin içinde gömülü olarak randevu noktası (Rendezvous point) adresi içerdiğini belirtir.
 - Üçüncü bitin 1 olması, çoklu gönderim adresinin “tekil gönderim öneki tabanlı çoklu gönderim adresi” olduğunu ve ağ adresinden türetildiğini göstermektedir. Üçüncü bitin 1 olması durumunda 4 bit de 1 olarak set edilir.
 - Dördüncü bitin (T) 0 olması IPv6 çoklu gönderim adresinin kalıcı, 1 olması ise kalıcı olmayan, geçiş için veya dinamik olarak atanmış bir adres olduğunu gösterir.
- ❑ Kapsam bölümündeki bitlerin değeri = 1 ise adres arayüz-yerel bir adrestir.
- ❑ Kapsam bölümündeki bitlerin değeri = 2 ise adres bağlantı-yerel bir adrestir.
- ❑ Kapsam bölümündeki bitlerin değeri = 4 ise adres yönetici-yerel bir adrestir.
- ❑ Kapsam bölümündeki bitlerin değeri = 5 ise adres site-yerel bir adrestir.
- ❑ Kapsam bölümündeki bitlerin değeri = 8 ise adres organizasyon-yerel bir adrestir.

IPv6 Başlık Yapısı

- ❑ IPv6 da, IPv4'ün hantal olan başlık yapısı revize edilmiş, gereksiz olan ya da görevleri üst katmanlara devredilebilen kısımlar çıkarılmıştır.
- ❑ IPv6'nın daha yalın bu başlık yapısı ile ağ cihazlarının işlem gücünden tasarruf edilmesi amaçlanmıştır.
- ❑ Sabit uzunluğa sahip temel bir başlık oluşturulmuş ve günümüz ağlarının gereksinimlerini karşılamak için bu başlık içerisinde yer alan adres bilgisi ile ilgili kısım genişletilmiştir.
- ❑ Temel başlığı ile üst seviye başlıklar arasında yer alan ve "IPv6 uzantı başlıkları" adını taşıyan yeni bir bölüm tanımlanmıştır. Bu yeni bölüm IPv6 ile gelen en önemli özelliklerden biridir. Bu bölümde bütün cihazlar tarafından işlenmesine gerek olmayan, paket ile ilgili ek bilgiler taşınabilmektedir. Böylece temel başlık bölümünde sadece gerekli bilgilerin yer alması sağlanmıştır.

IPv6 Başlık Yapısı

- ❑ Her iki protokolde de bulunan 4 bitlik “Sürüm” bölümü kullanılan protokolün sürümünü belirtmektedir. Bu bölüm IPv4 için 4, IPv6 için 6 değerini almaktadır.
- ❑ IPv4 veri paketleri 20 ile 60 bayt arasında değişen, IPv6 veri paketleri ise 40 baytlık sabit uzunlukta başlık bilgisine sahiptir. Bu nedenle IPv4 başlığında bulunan ve adres bilgisinin uzunluğunu belirten 4 bitlik “Toplam Uzunluk” bölümü IPv6’da kaldırılmıştır. Sabit uzunluktaki başlık, ağ cihazlarında başlık uzunluğunun algılanması için harcanan zamandan ve işlem gücünden tasarruf edilmesini sağlamaktadır.
- ❑ “Servis Tipi” ve “Trafik Sınıfı” alanları her iki başlık için de aynı işleve sahiptir. Öncelik
- ❑ atama ve servis kalitesi (Quality of Service) gibi fonksiyonlar için kullanılmaktadırlar.
- ❑ “Akış Etiketi” kısmı IPv6’yla getirilen yeni bir özelliktir. IPv6 da tercihli olarak
- ❑ kullanılabilen bu bölümle beraber, gerçek zamanlı verilerin bu bölümdeki etiketlere bakılarak hızlı bir şekilde yönlendirilmesi ya da MPLS (Multi Protocol Label Switching) gibi alt katmandaki teknolojilerin verimli kullanılması mümkün olmaktadır.

IPv6 Başlık Yapısı

- IPv6'nın adres başlık yapısındaki en önemli değişikliklerinden biri de yönlendirici gibi ara elemanlarda parçalama (Fragmentation) ve hata kontrolü yapılmamasıdır. Bu görevler bir üst seviyedeki protokol olan TCP'ye bırakılmıştır. Bu değişiklik sayesinde bu işlevleri yerine getirmekte kullanılan "Tanıtım", "Bayraklar", "Parça Telafisi" ve "Başlık Sağlama Toplamı" bölümleri IPv6'da yer almamaktadır.
- 8 bitlik "Yaşam Süresi" ve "Sıçrama Limiti" bölümleri farklı adlandırılmış olsalar da aynı işlevi görmektedirler. Bu bölüm bir veri paketinin bilgisayar ağları üzerinde ne kadar süre kalacağına karar vermek için kullanılmaktadır.
- Bir diğer 8 bitlik adres alanı olan "Sonraki Başlık" ise bir üst katmanda kullanılacak protokolü belirtmektedir. Bu alan aynı zamanda, IPv6'ya ek özellikler getirebilen "Uzantı Başlıklar" (Extension Headers) kısmı ile ilgili bilgiler de taşıyabilmektedir. IPv6'ın sunduğu ek özelliklerden olan ve ihtiyaç anında tercihe bağlı olarak kullanılabilecek "Uzantı Başlıklar" kısmı standart IPv6 başlık yapısının dışına çıkarılarak, ağ cihazlarının paketleri daha hızlı yönlendirmesi sağlanmıştır.

IPv4 Başlığı

Sürüm (Version)	IHL	Servis Tipi (Type of Service)	Toplam uzunluk (Total Length)	
Tanıtım (Identification)			Bayraklar (Flags)	Parça Telifisi (Fragment Offset)
Yaşam Süresi (Time To Live)	Protokol (Protocol)		Başlık Sağlama Toplamı (Header Checksum)	
Kaynak Adres (Source Address)				
Hedef Adres (Destination Address)				
Opsiyonlar (Options)				Tampon (Padding)

IPv6 Başlığı

Sürüm (Version)	Trafik Sınıfı (Traffic Class)	Akış Etiketli (Flow Label)		
Yük Uzunluğu (Payload Length)			Sonraki Başlık (Next Header)	Sıçrama Limiti (Hop Limit)
Kaynak Adres (Source Address)				
Hedef Adres (Destination Address)				

- IPv4 ve IPv6 da aynı olan alanlar
- IPv6 da olmayan alanlar
- IPv6 da adı ve pozisyonu değişen alanlar
- IPv6 da yeni alanlar

IPv6 Extension Headers (Uzantı Başlıkları)

- IPv6 da paketlerle ilgili tercihe bağlı bilgiler, temel başlık ile üst seviye protokol başlıkları arasında yer alan IPv6 uzantı başlıkları bölümünde yer alır
- Bu uzantı başlıkları temel başlık bilgisinden sonra ihtiyaç duyulduğunda kullanılır
- Biri hariç uzantı başlıklarının hepsi sadece IPv6 paketi için hedef olarak belirlenen cihaz tarafından işlenir
- Uzantı başlıkları bölümünde bulunacak başlık sayısı ile ilgili bir kısıtlama yoktur ancak yer alan bütün başlıklar “Sonraki Başlık Değeri” ile tanımlanmalıdır
- Cihazlar bu değerler sayesinde işlenmesi gereken uzantı başlığı olup olmadığını öğrenir, yoksa üst protokol başlığı ile ilgili işlemlere devam eder

IPv6 Extension Headers (Uzantı Başlıkları)

- ❑ Uzantı başlıkları boyut açısından değişkenlik gösterirler
- ❑ Eğer bir paket için birden fazla uzantı başlığı kullanılıyorsa bu başlıklar şu sırada olmalıdır:
 - Sıçrama Seçenekleri Başlığı (Hop-by-Hop Options Header)
 - Hedef Seçenekleri Başlığı (Destination Options Header)
 - Yönlendirme Başlığı (Routing Header)
 - Parçalama Başlığı (Fragment Header)
 - Doğrulama Başlığı (Authentication header)
 - Kapsüllenmiş Güvenlik Yük Başlığı (Encapsulating Security Payload Header)
 - Hedef Seçenekleri Başlığı (Destination Options Header)
 - Dolaşılabilirlik Başlığı (Mobility Header)
 - Üst Protokol Başlığı (Upper-layer Header)

IPv6 Extension Headers (Uzantı Başlıkları)

IPv6 Başlığı

Sonraki Başlık Değeri= TCP (6)

TCP Başlığı + Veri

IPv6 Başlığı

Sonraki Başlık Değeri=
Yönlendirme (43)

Yönlendirme Başlık

Sonraki Başlık Değeri=TCP(6)

TCP Başlığı + Veri

IPv6 Başlığı

Sonraki Başlık Değeri=
Yönlendirme (43)

Yönlendirme Başlık

Sonraki Başlık Değeri=
Parçalama (44)

Parçalama Başlığı

Sonraki Başlık
Değeri= TCP (6)

TCP Başlık Parçası

+ Veri

Sonraki Başlık Değeri	Uzantı Başlığı	Tanımı	RFC
0	Sekme Seçenekleri	Paketin yolu boyunca üzerinden geçtiği tüm cihazlar (kaynak ve hedef de dâhil) tarafından işlenmesi gereken bilgileri barındırır.	2460
43	Yönlendirme Başlığı	Paketin izleyeceği yol ile ilgili bilgi içerir. Bir kaynak oluşturduğu paketin ziyaret etmesini istediği bir veya daha fazla sayıdaki hedef düğüm ile ilgili bilgileri bu başlık ile tanımlayabilir.	2460
44	Parçalama Başlığı	Bu başlık kaynak tarafından hedefe mevcut paketin asıl verinin parçalarını içerdiği durumlarda kullanılır. IPv4 paket başlığında yer alan ancak IPv6 başlığından kaldırılan Kimlik Bilgisi ve Parça numarası bölümlerini barındırır.	2460
51	Doğrulama Başlığı	Güvenlik için kullanılır. Verinin doğrululuğu, bütünlüğünü sağlamak ve tekrar gönderimini engellemek amacıyla kullanılır.	2402
50	Kapsüllenmiş Güvenlik Yük Başlığı	Bu başlık bazen tek başına, bazen de doğrulama başlığı ile beraber IPv6'da güvenlik sağlamak için kullanılmaktadır. Taşınan verinin şifrelenmiş olduğunu gösterir.	2406
60	Hedef Seçenekleri	Bu başlıkla tanımlanan seçenekler sadece hedef cihaz tarafından işlenmektedir.	2460
135	Dolaşılabilirlik Başlığı	Bu başlık dolaşılabilirlik uygulamasında bağlanma tablolarının oluşturulması için yayınlanan mesajlarda kullanılır.	3775
59	Sonraki başlık yok	Bu başlık kendisinden sonra herhangi bir ek başlık olmadığını gösterir.	2460

IPv6 Extension Headers (Uzantı Başlıkları)

Üst Katman Protokolleri için tanımlanan sonraki başlık değerleri

Sonraki Başlık Değeri	Üst Protokol
6	TCP
11	UDP
58	ICMP

ICMPv6

- ❑ İnternet Kontrol Mesajlaşma Protokolü (Internet Control Message Protocol-ICMP) mesajları ağ iletişiminde yaşanan sorunların, iletişime dâhil olan ağ bileşenlerine iletilmesi amacıyla kullanılır
- ❑ Bir paket hedefine ulaştırılamadığında, bir yönlendiricinin kendisine gelen bir paketi yönlendirecek kadar boş kapasitesi olmadığında ya da bir paket için belirlenen rotadan daha kısa bir rotanın varlığı keşfedildiğinde ICMP mesajları ile bu durum bildirilir
- ❑ IPv4 tabanlı iletişimde ICMP mesajları sınır yönlendiricilerinde engellenir. Bunun temel nedeni ICMP'nin saldırganlar tarafından keşif aşamalarında kullanılmasıdır
- ❑ ICMPv6 aynı protokolün IPv6 için uyarlanmış halidir
- ❑ ICMPv6 tüm IPv6 düğümlerinin iletişimleri için temel bir protokol olarak tasarlanmıştır ve RFC 2463'e göre bu düğümler ICMPv6'yı eksiksiz desteklerler

ICMPv6

	0-7 Bit	8-16 Bit	16-31 Bit
Başlık (Header) 0-31 Bit	Tip (Type)	Kod (Code)	Sağlama Toplamı (Checksum)
Protokol yükü (Protokol Payload)	Mesaj (Message)		

- ❑ IPv6 paketinde üst protokolü tanımlayan sonraki başlık değeri 58 ise, bu paket bir ICMPv6 mesajı taşır
- ❑ ICMPv6 bilgileri iki bölümde taşınır:
 - İlk 32 bit başlık bölümünü oluşturur: Başlığın ilk 8 biti mesajın tipi ile ilgili bilgiyi taşır. Eğer en anlamlı bit 0 ise (0-127 arası değerler için) bu bir hata mesajıdır. Eğer en anlamlı bit 1 ise (128-255 arası değerler için) bu bir bilgi mesajıdır. 8 bitlik kod alanı içeriği mesaj tipine bağlıdır. 16 bitlik sağlama toplamı alanı ICMP paketi için minimum seviyede bütünlük doğrulaması yapar
 - Sonraki bitler ise protokol yükü için kullanılır

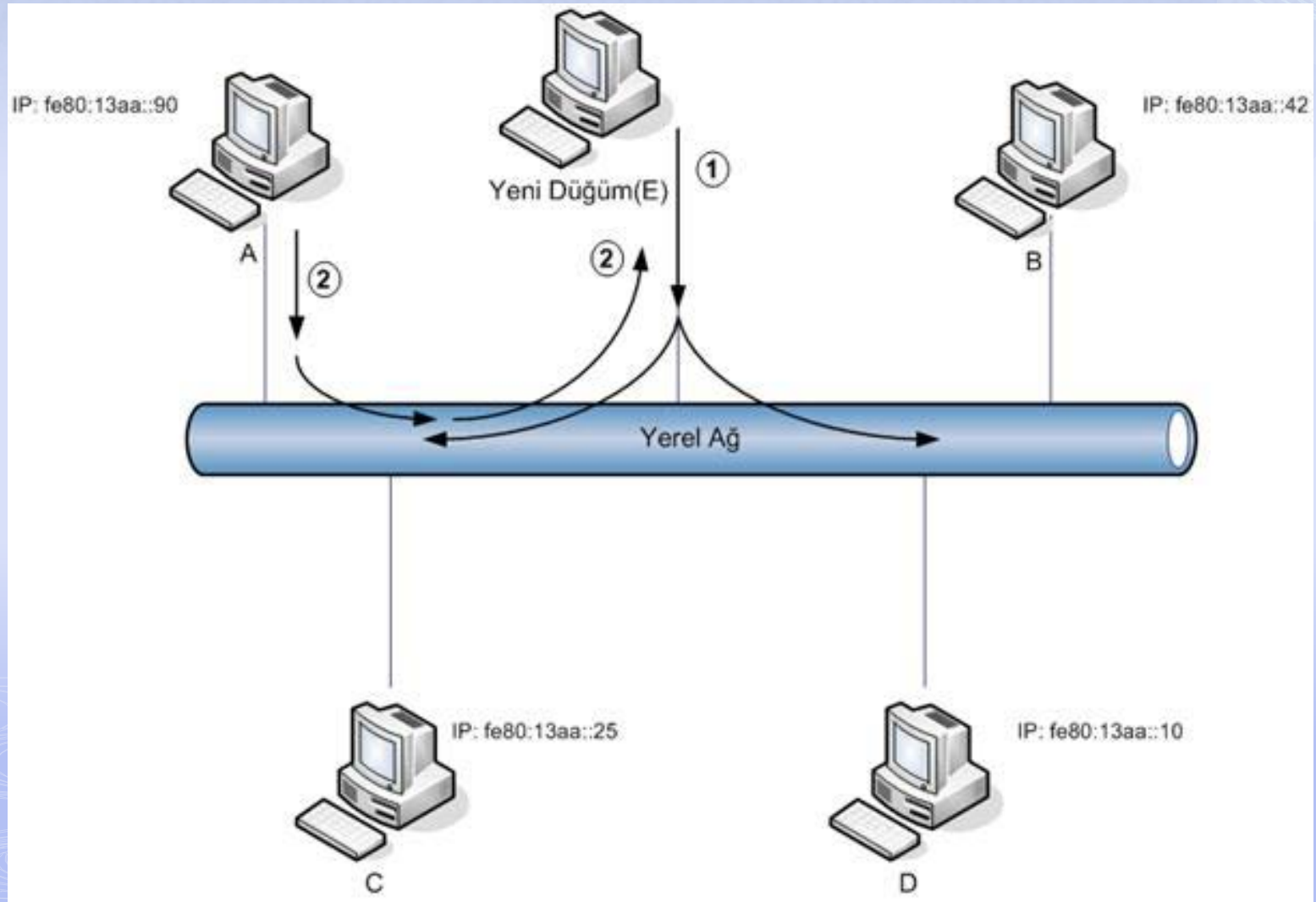
Komşu Keşfi (Neighbour Discovery)

- ❑ Komşu keşfi protokolü, IPv6'nın önemli parçalarından birisidir
- ❑ IPv4'de kullanılan yönlendirici keşfi (router discovery-RDISC), adres çözümleme protokolü (address resolution protocol-ARP) ve ICMP yeniden yönlendirme bileşenlerinin görevleri IPv6'da komşu keşfi tarafından yapılır
- ❑ IPv6'da düğümler aynı ağda bulundukları komşularıyla Komşu Keşfi Protokolü ile sürekli iletişim halinde bulunurlar
- ❑ Düğümler şu amaçlar için Komşu Keşfi Mesajlarını kullanırlar:
 - ağdaki diğer düğümlerin bağlantı yerel (link-local) adreslerini öğrenmek
 - komşuların erişilebilirlik durumların tespit etmek
 - ağ üzerindeki yönlendiricileri sorgulamak
 - yönlendiricilerden ağ yapılandırma bilgilerini elde etmek

Komşu Keşfi (Neighbour Discovery)

- Tanımlanmış 5 farklı komşu keşfi mesajı vardır:
 - **Yönlendirici Talep Mesajı (Router Solicitation - RS):** Düğümler tarafından, ağa bağlı yönlendiricileri öğrenmek amacıyla kullanılır. Ağa bağlı yönlendiricilerin “Yönlendirici İlan” mesajlarının periyodik güncelleme zamanını beklemeden yollamasını sağlar
 - **Yönlendirici İlan Mesajı (Router Advertisement - RA):** Ağa bağlı yönlendiriciler varlıklarını duyurmak ve ağa bağlanmak için gerekli parametreleri bildirmek için periyodik olarak ya da “Yönlendirici Talep Mesajına” cevaben “Yönlendirici İlan Mesajı” yayınlarlar. Ağ öneki, MTU büyüklüğü, düğüm tarafından adres oluşturulurken hangi otomatik yapılandırma yönteminin kullanılabileceği, varsayılan ağ geçidi ve geçerlilik süresi gibi bilgiler içerir
 - **Komşu Talep Mesajı (Neighbor Solicitation - NS):** Bu mesaj ağa bağlı tüm düğümler tarafından diğer düğümlerin bağlantı katmanı adreslerinin (link-layer) bulunması ve daha önceden iletişim kurulmuş ve bağlantı katmanı adresleri komşu tamponuna (neighbor cache) eklenmiş komşuların erişilebilirliğinin kontrol edilmesi amacıyla kullanılır
 - **Komşu İlanı (Neighbor Advertisement - NA):** Komşu Talep mesajına cevap olarak ya da düğümde oluşan bağlantı katmanı adresi değişikliğinin ilan edilmesi amacıyla yayınlanır
 - **Yeniden Yönlendirme (Redirect):** Yönlendiriciler tarafından düğümlere yollanır. Mesaj içeriğinde belirli bir hedef IPv6 adresi için daha iyi bir yönlendirme yolunun varlığı belirtilir

Komşu Keşfi (Neighbour Discovery)



Komşu Keşfi (Neighbour Discovery)

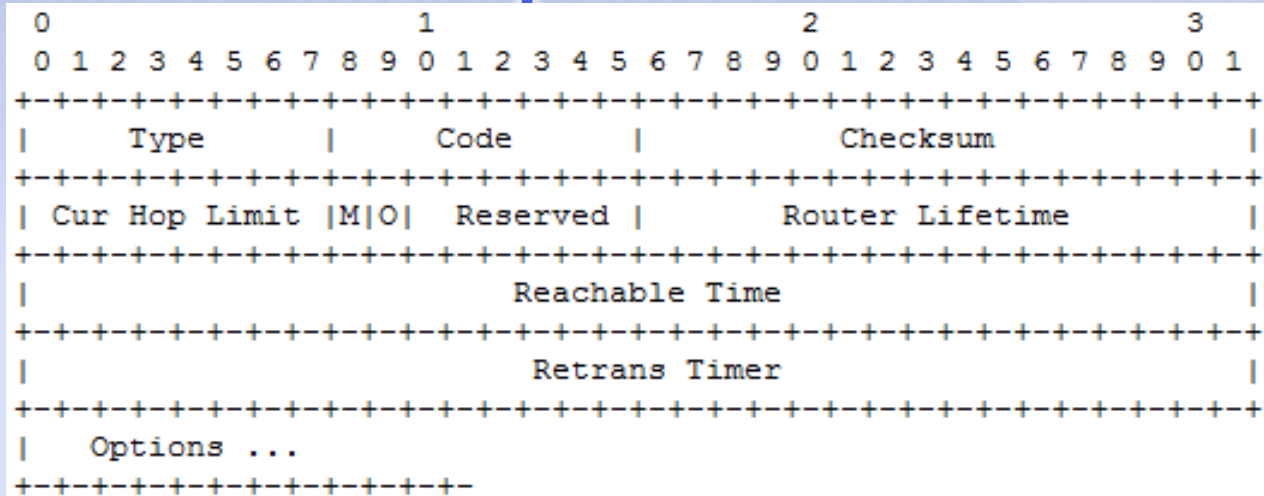
- ❑ Örnek şekle göre aynı yerel ağa bağlı A, B, C, D düğümleri ve bunların IP adresleri görülüyor. Ağa yeni bağlanan düğüm E, arayüz tanımlayıcısı ve ağ öneki yardımıyla oluşturduğu “fe80:13aa::90” adresini kullanmak ister. Öncelikle bu adresin ağda kullanılıp kullanılmadığını kontrol etmek için bütün düğümlerin multicast gönderim adresine komşu talep mesajı gönderir. Talep mesajını alan düğümler eğer bu adresi kullanıyorlarsa bir ilan mesajıyla cevap verirler.
- ❑ A düğümü fe80:13aa::90 adresini kullandığı için tüm düğümlere bir ilan mesajı gönderir. İlan mesajını alan E, adres kullanıldığı için bu adresi kendi arayüzüne atayamaz. Bu durumda ya düğüme sistem yöneticisi tarafından bir adres verilir veya alternatif bir arayüz tanımlayıcısıyla yeni bir adres oluşturulup süreç tekrar başlatılır. Eğer talebe belirli bir süre cevap gelmezse, E düğümü oluşturduğu adresi kullanmaya başlar.

IPv6 Yapılandırması

- IPv6 adreslerinin otomatik tanımlanması, Durum Denetimli (Stateful) veya Durum Denetimsiz (Stateless) olmak üzere iki şekilde yapılabilir
- Durum Denetimsiz Otomatik Adres Yapılandırması, ağ üzerinde bulunan yönlendiricinin ağa sürekli olarak gönderdiği bilgiler aracılığı ile yapılır
- Durum Denetimli Otomatik Adres Yapılandırması ise, DHCPv6 kullanılarak yapılabilir
- Otomatik adres tanımlamanın yanı sıra, istemcilere statik olarak IPv6 adreslerinin tanımlanması da mümkündür.

IPv6 Yapılandırması

Router
ilan
mesajı



- ❑ Otomatik adres yapılandırmasında önemli görev Yönlendirici İlan Mesajındadır
- ❑ Mesaj içinde bulunan M ve O bitleri (Managed Address Configuration Flag, Other Configuration Flag) istemcilere adres yapılandırması ve DNS sunucu bilgisi gibi ek parametreleri elde etmek için durum denetimsiz ve durum denetimli adres yapılandırma yöntemlerinden hangisini kullanabilecekleri konusunda bilgi içerir
- ❑ M ve O bitlerinin değerlerine göre istemcilere farklı bilgiler aktarılır. Her iki bit için varsayılan değerler sıfırdır.

IPv6 Yapılandırması

- Her iki bitin değeri sıfır ise ($M = 0$ ve $O = 0$)
 - İstemci adres yapılandırması için durum denetimsiz otomatik adres yapılandırma kullanır, ek parametreleri diğer yöntemler (statik yapılandırma) ile elde eder.
- M bitinin değeri sıfır, O bitinin değeri bir ise ($M = 0$ ve $O = 1$)
 - İstemci adres yapılandırması için durum denetimsiz otomatik adres yapılandırma kullanır, ek parametreleri durum denetimli otomatik adres yapılandırma yöntemi ile elde eder.
- M bitinin değeri 1, O bitinin değeri sıfır ise ($M = 1$ ve $O = 0$)
 - İstemci adres yapılandırması için durum denetimli otomatik adres yapılandırma yöntemi kullanılır, ek parametreleri diğer yöntemler (statik yapılandırma) ile elde eder.
- $M = 1$ ve $O = 1$ ise (DHCPv6 statefull)
 - İstemci adres yapılandırması ve ek parametreleri durum denetimli otomatik adres yapılandırma yöntemini kullanarak elde eder.

IPv6 Yapılandırması

- ❑ İstemciler, durum denetimsiz otomatik adres yapılandırma yönteminde “Yönlendirici İlan Mesajları” ile duyurulan ağ önek bilgisini kendi adreslerini oluşturmak için kullanmadan önce mesaj içerisindeki özerklik bayrağının (Autonomous Flag) değerini kontrol ederler
- ❑ Bu bayrak için varsayılan değer 1 olup, ağ önek bilgisinin adres yapılandırması için kullanılabileceğini gösterir
- ❑ Bayrak değeri 0 ise, istemciler ilgili “Yönlendirici İlan Mesajı”ndaki ağ önek bilgisini bu işlem için kullanmaz
- ❑ Özellikle durum denetimli adres yapılandırma yöntemi kullanılan ağlarda, yönlendirici ilan mesajlarındaki bu bayrağın değeri sıfır olarak tanımlanmalıdır
- ❑ Aksi takdirde istemciler hem durum denetimli hem de durum denetimsiz otomatik adres yapılandırma yöntemlerini kullanarak iki farklı global IPv6 adresi alırlar.

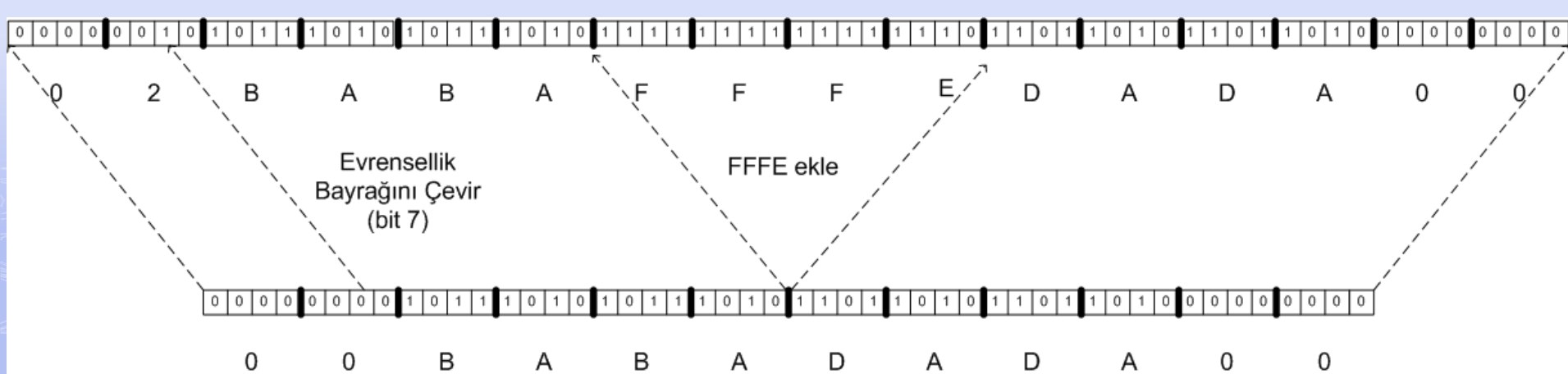
Durum Denetimsiz Otomatik IPv6 Yapılandırması

- Bu yöntemde ağa bağlanan düğümlerin kullandıkları IPv6 adresleri bir sunucu veya otorite tarafından belirlenmez ve kayıt altına alınmaz
- İstemci ile router arasındaki iletişim şöyle gerçekleşir:
 - İstemci kendi bağlantı yerel adresini kullanarak yönlendirici talep mesajını ağdaki bütün yönlendiricileri temsil eden multicast gönderim adresine iletir
 - Talep mesajını alan yönlendirici, ağ katmanındaki yapılandırma parametrelerini içeren yönlendirici ilan mesajı ile cevap verir
 - Bu bilgiyi alan istemci, kendi arabirim tanıtıcısını yönlendiriciler tarafından anons edilen önek ile birleştirerek global IPv6 adresini oluşturur

Durum Denetimsiz Otomatik IPv6 Yapılandırması

Küresel Yönlendirme Öneki	Alt Alan Ağı Tanıtıcısı	Arabirim Tanıtıcısı
48 bit	16 bit	64 bit

- İstemci, arabirim tanıtıcısını oluştururken 48 bitlik MAC adreslerini kullanır
- Arabirim tanıtıcısı, düğümlerin ağ arayüzlerinin 48 bitlik MAC adreslerinin tam ortasına 0xFF ve 0xFE değerleri eklenerek oluşturulur. Ayrıca MAC adresinin 7. biti kontrol amacıyla çevrilir
- Ağ üzerinde Yönlendirici İlan Mesajı anonsu olmaması durumunda, düğümler bağlantı yerel adreslerini oluşturarak aynı ağa bağlı diğer düğümlerle iletişim kurabilirler. Durum denetimsiz otomatik adres yapılandırmasının bu özelliği IPv6 ağlarında tak-çalıştır yönteminin işlerliğini sağlamaktadır.



Durum Denetimli Otomatik IPv6 Yapılandırması

- ❑ Düğümler IPv6 adreslerini ve ağa bağlanmak için gerekli diğer parametreleri ağa bağlı bir sunucudan edinirler
- ❑ Sunucu dağıttığı IPv6 adresleri ile ilgili bir veri tabanı tutarak durum denetimi gerçekleştirir
- ❑ Durum denetimli adres yapılandırılması, DHCPv6 aracılığı ile yapılabilir
- ❑ IPv6 ağlarında DHCP kullanılmasını gerektirecek durumlar:
 - Ağ tasarımında, yönetme, izleme gibi sebeplerle kullanılan adreslerin kontrol edilmesine ihtiyaç duyulması,
 - Bazı ek yapılandırma bilgilerinin istemcilere ulaştırılması ihtiyacı (DNS, SIP, vb.).
- ❑ DHCP, multicast adresleri kullanarak, istemcinin DHCP sunucusuna talebini iletmesine ve sunucunun istemciye gerekli ağ yapılandırma bilgilerini göndermesine olanak sağlar
- ❑ DHCP istemcisi ile aynı ağda bulunmayan DHCP sunucularına mesajların ulaştırılması da, DHCP nakledici (DHCP relay) yapılandırması ile yine multicast adresleri kullanılarak uygulanır
- ❑ Kullanılan multicast adresleri:
 - Tüm DHCP sunucuların ve relay agentların bulunduğu FF02::1:2 bağlantı yerel adresi
 - Tüm DHCP sunucuların bulunduğu FF05::1:3 site yerel adresi.
- ❑ Durum denetimli otomatik adres yapılandırması yöntemi ile varsayılan ağ geçidi bilgisi istemcilere iletilmez. İstemciler yönlendirici ilan mesajı aldıkları cihazın IPv6 adresini varsayılan ağ geçidi olarak kaydederler.

Cisco Router Otomatik Yapılandırma Örnekleri

Adres yapılandırması (M ve O) ve Özerklik (Autonomous) Bayrakları

- ❑ M biti varsayılan değeri 0'dır. Değeri 1 yapmak için:
 - *Router(config-if)#ipv6 nd managed-config-flag*
- ❑ O biti varsayılan değer 0'dır. Değeri 1 yapmak için:
 - *Router(config-if)#ipv6 nd other-config-flag*
- ❑ A biti varsayılan değer 1'dir. Değeri 0 yapmak için:
 - *Router(config-if)#ipv6 nd prefix 2001:db8:1:2::/64 no-autoconfig*

Cisco Router Otomatik Yapılandırma Örnekleri

Yönlendirici İlanı için Temel Yapılandırma

```
interface GigabitEthernet0/1  
ipv6 address 2001:db8:1:2::1/64  
ipv6 enable  
ipv6 nd prefix 2001:db8:1:2::/64
```

Cisco Router Otomatik Yapılandırma Örnekleri

DHCPv6 Stateless Temel Yapılandırma

```
ipv6 dhcp pool IPv6DNS
dns-server 2001:DB8:A:B::1
dns-server 2001:DB8:3000:3000::42
domain-name duzce.edu.tr
!
interface Ethernet0/0
  ipv6 enable
  ipv6 address 2001:DB8:1:2::1/64
  ipv6 nd other-config-flag
  ipv6 dhcp server IPv6DNS
```


Cisco Router Otomatik Yapılandırma Örnekleri

DHCPv6 Statefull Temel Yapılandırma

```
ipv6 local pool VLAN10 2001:db8:1::/48 64
!  
ipv6 dhcp pool DHCPv6HAVUZ  
prefix-delegation 2001:db8:1::23F6:33BA/64 00030001000E84244E70  
prefix-delegation pool VLAN10  
dns-server 2001:db8:1::19  
domain-name duzce.edu.tr  
!  
interface FastEthernet0/0  
ipv6 address 2001:db8:1::1/64  
ipv6 address FE80::1 link-local  
ipv6 nd managed-config-flag  
ipv6 nd other-config-flag  
ipv6 dhcp server DHCPv6HAVUZU rapid-commit preference 1 allow-hint
```

Statik Adres Yapılandırma

❑ Cisco

```
interface GigabitEthernet0/1  
ipv6 address 2001:db8:2:1::1/64  
ipv6 enable
```

❑ FreeBSD

```
/sbin/ifconfig fxp0 inet6 2001:db8:2:1::2/64  
/sbin/route add -inet6 default 2001:db8:2:1::1
```

❑ Linux

```
/sbin/ifconfig eth0 add 2001:db8:2:1::2/64  
/sbin/route add --inet6 default gw 2001:db8:2:1::1
```

Statik Adres Yapılandırma

□ Windows XP

- Windows XP işletim sisteminde grafik arayüzü kullanılarak IPv6 adresi ataması yapılamaz
- Komut satırından girilebilecek “netsh interface ipv6 install” komutu ile IPv6 desteği yüklenir, ardından komut satırı kullanılarak IPv6 adres ve varsayılan ağ geçidi atama işlemi yapılır

netsh interface ipv6 install

netsh interface ipv6 set address “Local Area Connection” 2001:db8:2:1::1

□ Windows 7

- IPv6 desteği kurulumda otomatik olarak gelir. IPv6 ayarları grafik arayüz veya komut satırı ile yapılabilir

netsh interface ipv6 set address “Local Area Connection” 2001:db8:2:1::1