



# İKİLİ YIĞIN YÖNTEMİYLE IPv6'YA GEÇİŞ



25.08.2020  
ANKARA

NOT:

Bu doküman kurumların IPv6'ya geçişinin ikili yığın (*dualstack*) yöntemiyle yapılacağı varsayılarak hazırlanmıştır.

# İçindekiler

|       |                                                                        |    |
|-------|------------------------------------------------------------------------|----|
| 1.    | IPv6 Başvurusu .....                                                   | 4  |
| 1.1   | IPv6 İle Gelen Yenilikler .....                                        | 5  |
| 1.2   | IPv6 Adres Yapısı.....                                                 | 7  |
| 1.3   | IPv6 Adres Tahsisi ile Sorumlu Kurumlar ve Tahsis Süreci .....         | 9  |
| 1.4   | IPv6'yı işletim sistemlerinde aktif etme .....                         | 14 |
| 1.4.1 | Freebsd .....                                                          | 14 |
| 1.4.2 | Linux .....                                                            | 14 |
| 1.4.3 | Windows.....                                                           | 15 |
| 1.5   | Windows Sistemlerde DHCPv6, DNSv6 Konfigürasyonu .....                 | 15 |
| 1.5.1 | Düğümlere Statik IPv4 ve IPv6 Verilmesi.....                           | 16 |
| 1.5.2 | Durumsuz (Stateless) IP Yapılandırması .....                           | 18 |
| 1.5.3 | Ağ Geçidi Üzerinden Düğümlere DNS Adresi Verilmesi .....               | 20 |
| 1.5.4 | DHCPv6 ile Duruma Bağlı ( <i>Statefull</i> ) IP Yapılandırması .....   | 21 |
| 1.6   | IPv6 Adres Alma Yöntemleri.....                                        | 36 |
| 1.6.1 | Duruma Bağlı Adres Otomatik Konfigürasyonu (DHCPv6) .....              | 37 |
| 1.7   | Adres Çakışması Tespiti (Duplicate Address Detection - DAD).....       | 37 |
| 1.8   | Düğümün DNS Sunucusunu Öğrenmesi .....                                 | 37 |
| 1.8.1 | Durumsuz Adres Otomatik Konfigürasyonu (SLAAC) .....                   | 37 |
| 2.    | Yönlendiricide IPv6 İkili Yığın Konfigürasyonu.....                    | 39 |
| 3.    | IPv6'ya Geçişte Ethernet Switchler Üzerinde Yapılması Gerekenler ..... | 41 |
| 4.    | IPv6'da Sorun Giderme.....                                             | 42 |

## KISALTMALAR

|          |                                                                                                          |
|----------|----------------------------------------------------------------------------------------------------------|
| APNIC    | Asya Pasifik Ağ Bilgi Merkezi<br>(Asia Pacific Network Information Centre)                               |
| ARIN     | Amerika İnternet Sayıları Kayıt Merkezi<br>(American Registry for Internet Numbers)                      |
| BGP      | Sınır Geçiş Protokolü<br>(Border Gateway Protocol)                                                       |
| DHCPv6   | Dinamik İstemci Yapılandırma Protokolü Sürüm 6<br>(Dynamic Host Configuration Protocol)                  |
| DNS      | Alan Adı Sistemi<br>(Domain Name System)                                                                 |
| IANA     | İnternet Tahsisli Sayılar Kurumu<br>(Internet Assigned Numbers Authority)                                |
| IETF     | İnternet Mühendisliği Görev Gücü<br>(Internet Engineering Task Force)                                    |
| IP       | İnternet Protokolü<br>(Internet Protocol)                                                                |
| IPv4     | İnternet Protokolü Sürüm 4<br>(Internet Protocol Version 4)                                              |
| IPv6     | İnternet Protokolü Sürüm 6<br>(Internet Protocol Version 6)                                              |
| ICANN    | İnternet Tahsisli Adlar ve Sayılar Kurumu<br>(Internet Corporation for Assigned Names and Numbers)       |
| ISOC     | İnternet Topluluğu<br>(Internet Society)                                                                 |
| IPSec    | IP Güvenliği Protokolü<br>(Internet Protocol Security)                                                   |
| İSS      | İnternet Servis Sağlayıcı                                                                                |
| LACNIC   | Latin Amerika ve Karayipler Ağ Bilgi Merkezi<br>(Latin America and Caribbean Network Information Centre) |
| LAN      | Yerel Alan Ağı<br>(Local Area Network)                                                                   |
| LIR      | Yerel İnternet Kayıt Merkezi<br>(Local Internet Registry)                                                |
| MAC      | Ortam Erişim Yöntemi<br>(Media Access Control)                                                           |
| NAT      | Ağ Adres Çevrimi<br>(Network Address Translation)                                                        |
| NIR      | Ulusal Kayıt Merkezi<br>(National Internet Registry)                                                     |
| RIPE NCC | RIPE Ağ Koordinasyon Merkezi<br>(RIPE Network Coordination Center)                                       |
| RIR      | Bölgesel İnternet Kayıt Kurumu<br>(Regional Internet Registry)                                           |

## 1. IPv6 Başvurusu

İnternet protokol adreslerinin (İnternet Protocol- IP) yeni sürümü olan IPv6; yetkilendirilmiş internet servis sağlayıcılar (İSS) tarafından, ülkemizin de içinde bulunduğu bölgeye hizmet veren Bölgesel İnternet Kayıt Kurumu olan RIPE Ağ Koordinasyon Merkezi (RIPE Network Coordination Center - RIPE NCC) 'nin yayımladığı "IPv6 Adres Tahsis ve Atama Politikası " başlıklı belgeye göre yapılmaktadır. Bununla birlikte, bu belgenin dışında her bir işletmecinin farklı politikaları olabilmektedir. Örneğin, Türk Telekom IPv6 şebekesinde her devre için yönlendirici (router) portlarında /64 ön ekli IP, çoklu blok olarak ise /56 veya /48 lü IP blokları vermektedir. Kurumlar Türk Telekom'dan aldıkları /48 IP bloğunu kendi iç ağlarında kullanıcı ve sunucularına paylaşmaktadır. Türk Telekom mevcut politikaları gereğince bu adres aralığını yeterli görmekte, müşterileri için adres bloğunda genişletme yapmamaktadır. Tüm işletmecilerde çoklu IP tahsis talepleri süreç olarak IPv4 ile aynı şekilde ilerlemekte olup satış yöneticisi aracılığı ile gerçekleşmektedir.

Bu durum dışında kurumlar kendi tüzel kişilikleri adına RIPE NCC'den doğrudan IP bloğu alabilmektedir. Bu durumda; ilgili kurumun internet hizmeti aldığı ISS ile sınır geçiş protokolü (Border Gateway Protocol- BGP) aracılığıyla haberleşerek kendi IP bloğunu internete duyurması gerekmektedir. Böyle bir durum için yine IPv4 BGP talebi senaryosunun aynısı söz konusu olmaktadır. İSS; kurumların kendisine ait IPv6 bloklarını İSS metro ethernet devresinden anons edebilmesi için ilgili kurum yönlendirici portuna bir IPv6(/64) arayüz IP'si vermektedir. Daha sonra ilgili kurumun RIPE NCC üzerindeki kayıtları tam olduğu sürece İSS'in ilgili kuruma tahsis ettiği IP üzerinden kurumların kendilerine ait bloklarının anonsu kabul edilmektedir.

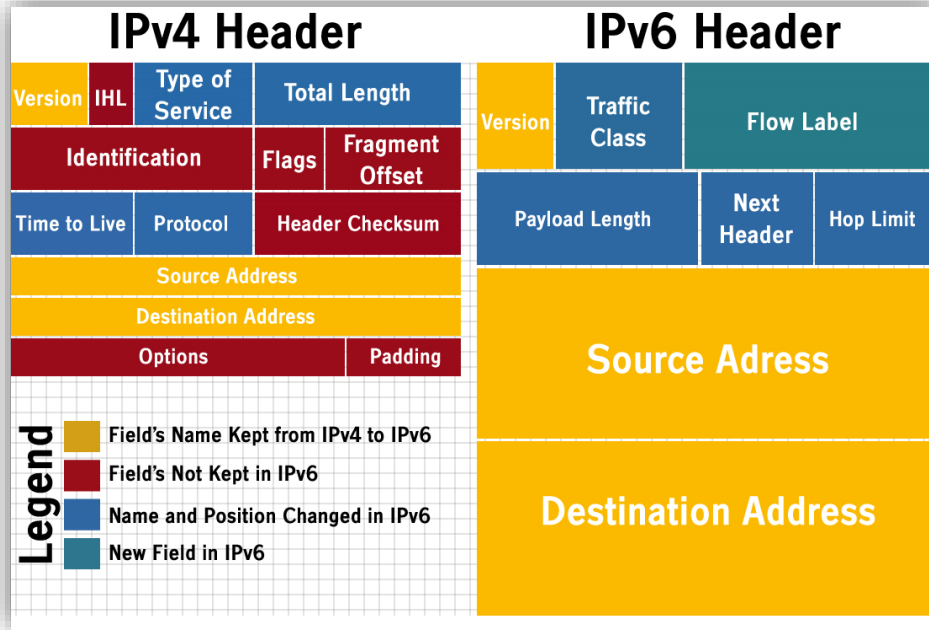
## 1.1 IPv6 İle Gelen Yenilikler

- IPv6 ya ihtiyaç duyulmasının ana nedeni IPV4 IP adreslerinin bitiyor olmasıdır. Bu nedenle IPv6 bitmeyecek bir büyüklükte tasarlanmıştır. Aşağıdaki tabloda aradaki bu fark belirtilmiştir.

| IP Versiyon  | IPv4                          | IPv6                                                            |
|--------------|-------------------------------|-----------------------------------------------------------------|
| Adres Uzayı  | 32 bit                        | 128 bit                                                         |
| Adres Biçimi | 10'luk düzende<br>192.168.1.1 | 16'lık düzende<br>2001:0DB8:0234:AB00:0123:4567:8901:ABCD       |
| Adres Sayısı | 4.292.967.296                 | 340.282.366.920.938.000.000.000.000.000.000.000.000.000.000.000 |

- IPv6 yeni güvenlik özelliklerine sahiptir:
- IP Güvenliği (IPsec) desteği IPv6'da bütünleşik olarak gelmektedir.
  - IPv6 adres uzayı daha geniş olduğu için siber saldırılardan önce yapılan zafiyet tarama işlemlerinin daha zor olması beklenmektedir. Fakat bu istenmeyen kişiler tarafından zafiyet taraması yapılamayacağı anlamına gelmemektedir. Saldırgan dışarı hizmet verilen IP adreslerine zafiyet taraması yapabilmektedir. Hangi IP adreslerinin internetten erişilebilir olduğunun taraması ise IPv4 ile kıyaslandığında daha çok zaman alan bir faaliyettir.
  - IPv6 protokolü yayın (broadcast) yerine çoklu gönderim (multicast) paketler kullandığından birçok bilgi ilgisiz bilgisayarlara gönderilmemektedir. Bununla birlikte ikinci katmandaki bazı ataklar (DHCP, ARP atakları gibi) hala mümkün olmaktadır. Ayrıca eğer anahtarlama cihazlarının çoklu gönderim (multicast) desteği yok veya çoklu gönderim desteği olmakla birlikte Multicast listener Discovery (MLD) snooping fonksiyonu aktif etmemişse, tüm çoklu gönderim(Multicast) paketler anahtarlama cihazı tarafından (broadcast edilecek) yayınlanacaktır.
- IPv6'da paket parçalama (fragmentasyon) işlemleri artık aradaki yönlendiricilerde yapılmamaktadır. Paket parçalama işlemleri yalnız paket üretilirken yapıldığı için yönlendirici cihazlarının üzerindeki yük azalmıştır. Paket fragmentasyonu ile yapılan ataklar hala mümkün olabileceği için güvenlik cihazlarının bir şekilde gönderilen paketleri birleştirerek analiz etmeye devam etmesi gerekmektedir. Bu nedenle güvenlik cihazlarının yükü değişmemiştir.

➤ IPv6 ile beraber daha sade IP başlık yapısı kullanılmaktadır.



➤ IPv6 IPv4 e göre daha gelişmiş servis kalitesi sunmaktadır.

- Ağ adres çevrimine (Network Address Translation – NAT) ihtiyaç olmamasının yanında IP başlık yapısındaki sadelik gibi faktörler paketin üretilmesi ve iletilmesini hızlandırarak servise erişim hızı açısından servis kalitesi artmıştır.
- Bir servisin önceliklendirilmesi (QoS) işlemi için IPv6 iki ayrı alana sahiptir.

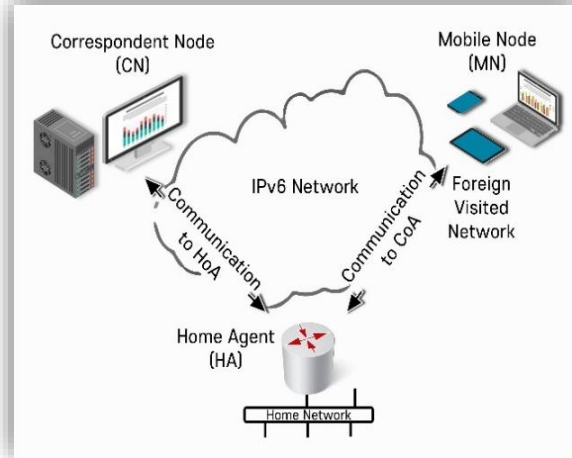
20 bit – akış etiketi (*flow label*)

8 bit – trafik sınıfı göstergesi (*traffic class indicator*)

➤ IPv6 daha esnek otomatik adres yapılandırma seçeneklerine sahiptir.

- DHCP olmaksızın uç noktadaki cihazlara IP ataması sağlanabilmektedir.
- IPv6 farklı ağlarda aynı IP adresini kullanabilmeyi mümkün kılmaktadır. Bu sayede dolaşım halindeyken kesinti problemlerinin ortadan kaldırılması hedeflenmiştir. Bu yapıda mobil düğüm (mobile node) iki adet IPv6 adresine sahiptir.
  - Yerleşik Adres (Home Address - HoA) : Sürekli sahip olunan adres
  - Değişken Adres (Care of Address - CoA): Kullanıcı(mobile node) farklı ağda iken aldığı değişken adres.
- Mobil düğüm nerede olursa olsun Home Agent (HA) yönlendirici ile tünel kurmaktadır.

- Aşağıdaki şekilde bu durum tasvir edilmiştir. HA yönlendirici, önce mobile node ile bir tünel kurar. HOA IP adresi HA router ın üzerindedir. Haberleşilen düğümden (Correspondent node - CN) HoA adresine yapılan istekler HoA ile CoA ipleri arasında kurulan tünel vasıtasıyla iletmektedir.



## 1.2 IPv6 Adres Yapısı

- IPv4'te kullanılan 32 bitlik 10'luk düzendeki 4 oktetten oluşan yazım formatı yerine IPv6'da 128 bitlik ve 16'lık düzende 8 oktet yazım formatına geçilmiştir.

IPv4 → 192.168.1.1

IPv6 → 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A

Farklı düzenlere geçişe ilişkin örnekler aşağıdaki tablodan görülebilmektedir:

| Ondalık | İkilik | Onaltılık |
|---------|--------|-----------|
| 0       | 0000   | 0         |
| 1       | 0001   | 1         |
| 2       | 0010   | 2         |
| 3       | 0011   | 3         |
| 4       | 0100   | 4         |
| 5       | 0101   | 5         |
| 6       | 0110   | 6         |
| 7       | 0111   | 7         |
| 8       | 1000   | 8         |
| 9       | 1001   | 9         |
| 10      | 1010   | A         |
| 11      | 1011   | B         |
| 12      | 1100   | C         |
| 13      | 1101   | D         |
| 14      | 1110   | E         |
| 15      | 1111   | F         |

IPv6 adres yazımında kullanılabilecek bazı kısaltma kuralları bulunmaktadır. Bu kuralları *2A01: 0EA8: 0000: 0000: 01CA:00FF:FE15:6B5A* IPv6 adres örneği üzerinden özetlemek gerekirse;

- Her 16 bitlik blokta solda kalan sıfırlar adresten atılabilmektedir.

*2A01:EA8: 0:0:1CA:FF:FE15:6B5A*

- Tamamı sıfırdan oluşan bloklar fazladan bir adet daha “:” kullanılarak sol baştan sadece bir kere olmak üzere adresten çıkarılabilmektedir.

*2A01:EA8::1CA:FF:FE15:6B5A*

IPv6 yazımındaki kısaltmalar ile ilgi olarak aşağıdaki örneklerde yer verilmektedir.

#### ÖRNEK 1:

2001: 0DB8: 003E:EF11:0000:0000:C100:004D

2001:DB8:3E:EF11:0:0:C100:4D

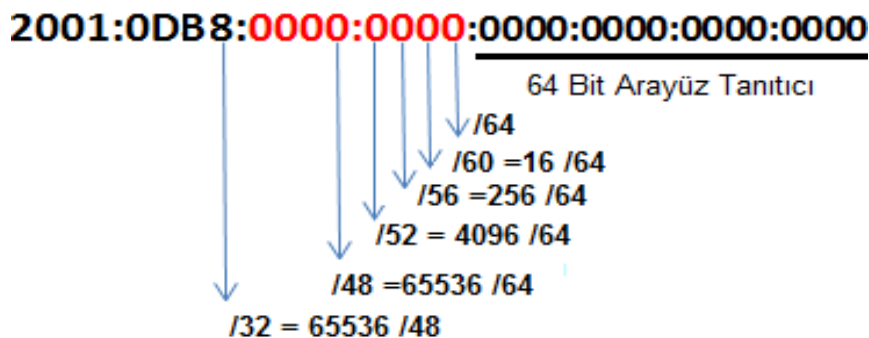
2001:DB8:3E:EF11::C100:4D

#### ÖRNEK 2:

2001:0db8:0000:0000:0000:0000:0000:0001

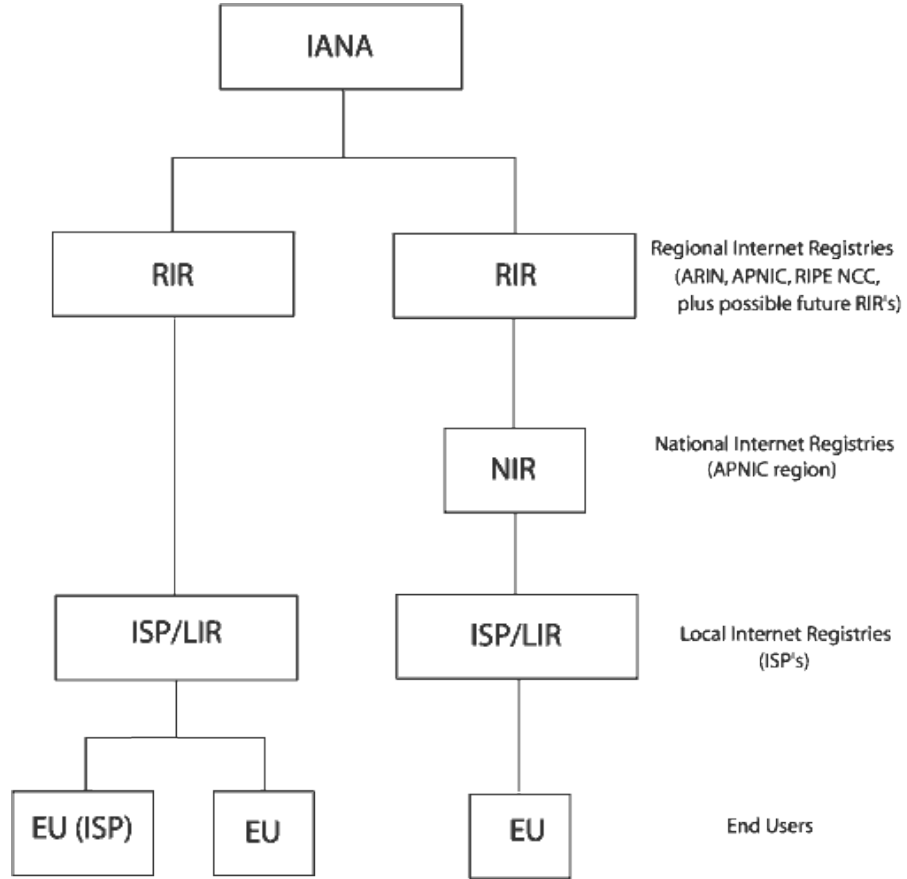
2001:db8:0:0:0:0:0:1

2001:db8::1



### 1.3 IPv6 Adres Tahsisi ile Sorumlu Kurumlar ve Tahsis Süreci

Temel internet kaynaklarının yönetiminden sorumlu bir kuruluş olan İnternet Tahsisli Sayılar Kurumu (Internet Assigned Numbers Authority – IANA), IP adres tahsislerinin denetlenmesi ve DNS'in yönetilmesini sürdürmekte, internet alan adları ve IP adreslerini doğrudan ya da IANA'nın yetki delegasyonu ile dünya çapındaki beş Bölgesel İnternet Kayıt Kurumu aracılığı ile tahsis etmektedir<sup>1</sup>.



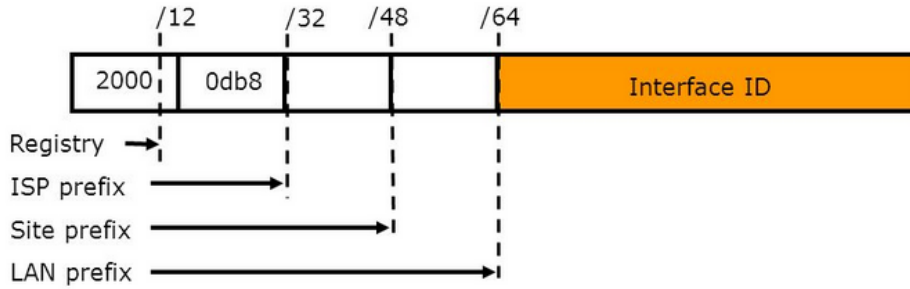
IANA şu anda dağıtımına açılan 2000::/12 bloğunu her biri ayrı kıtalara hizmet veren bölgesel kayıt kurumlarına (ARIN, APNIC, RIPE, AFRINIC) tahsis etmektedir. Ülkemizin de içinde yer aldığı bölge olan Asya ve Avrupa kıtalarına internet kaynakları RIPE NCC tarafından tahsis edilmektedir.

<sup>1</sup> <https://www.ripe.net/publications/docs/ripe-699>



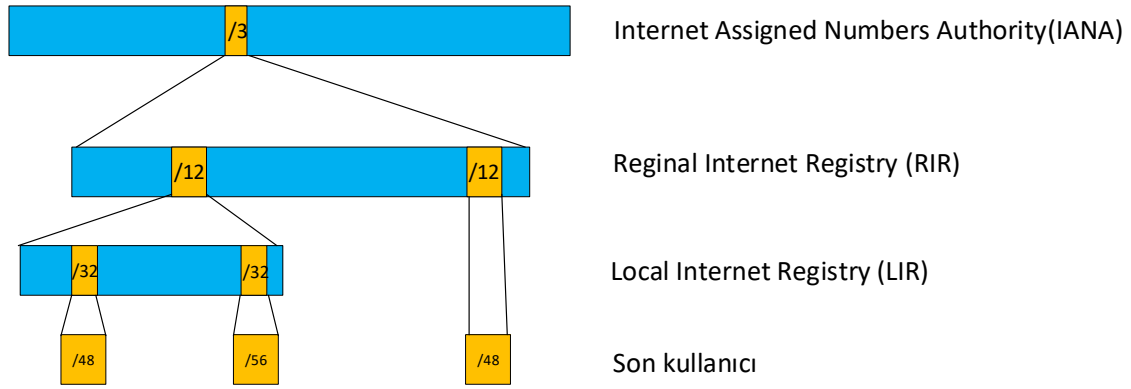
<https://www.ripe.net/about-us/what-we-do/ripe-ncc-service-region>

Bölgesel internet kayıt kurumları kendilerine tahsis edilen IP bloklarını varsa ülkedeki ulusal internet kayıt merkezine yoksa ISS'lere veya yerel internet kayıt merkezlerine (Local Internet Registry- LIR) tahsis etmektedir. Son kullanıcılar ISS'lerden veya yerel internet kayıt merkezlerinden IP bloğu talebinde bulunabilmektedir. IP tahsisine ilişkin ayrıntılar aşağıdaki örnekten görülebilmektedir.



Tahsis süreci:

- IANA 2000::/3 bloğunu kullanıma açmıştır.
- 2000::/3 lük blok içinden tüm bölgesel kayıt kurumları /12'lik ön ekler halinde tahsis edecekleri bloğu alır.
- RIR'lar IANA dan aldığı /12'lik blok içerisinde /32'lik blokları yerel internet kayıt merkezlerine tahsis eder/satar.



LIR'lere verilen bir /32 adres bloğu üzerinden incelenecek olursa:

- Büyük müşterilere genellikle /48, orta ölçekli müşterilere /52 alt ağ verilmektedir.
- /48 adres bloğuna sahip bir müşteri 64K adet /64 bloğuna , /52 içinde 4K adet /64 bloğuna sahip olmaktadır.

Aşağıda RIPE tarafından paylaşılan ve IP bloğu ihtiyaçlarının belirlenmesinde kullanılabilecek bir tablo bulunmaktadır. Söz konusu tablo ile pratik bir şekilde IP bloklarında oluşturulabilecek host sayısı tespit edilebilmektedir.

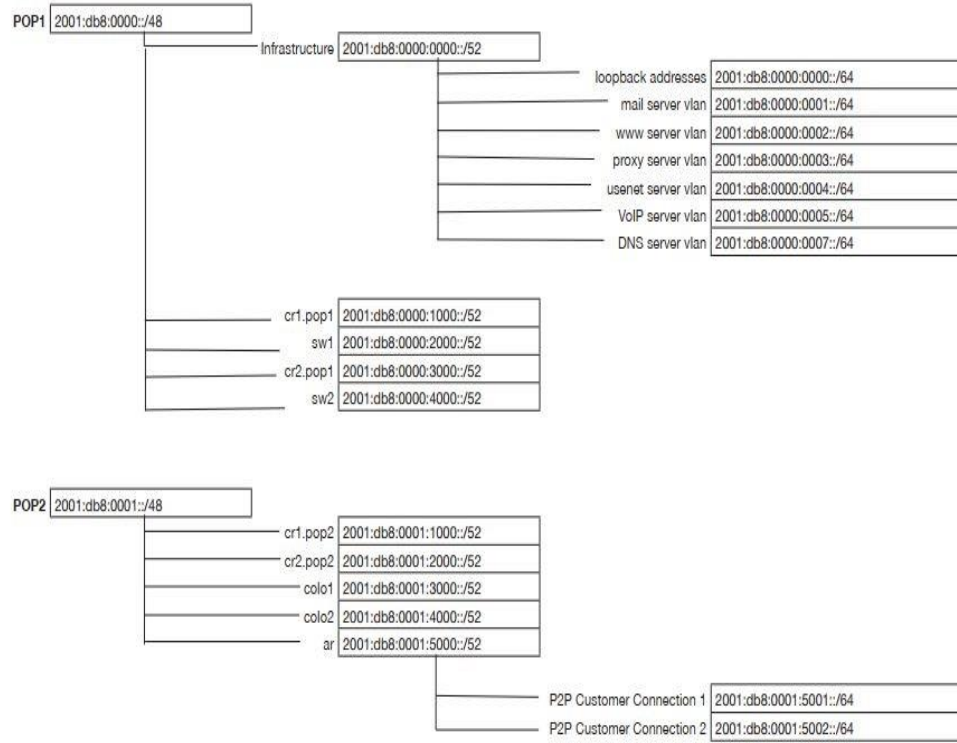
## IPv6 Chart

$K = 1,024 \cdot M = 1,048,576 \cdot G = 1,073,741,824 \cdot T = 1,099,511,627,776$

| Prefix | /48s | /56s | /64s | Bits |
|--------|------|------|------|------|
| /24    | 16M  | 4G   | 1T   | 104  |
| /25    | 8M   | 2G   | 512G | 103  |
| /26    | 4M   | 1G   | 256G | 102  |
| /27    | 2M   | 512M | 128G | 101  |
| /28    | 1M   | 256M | 64G  | 100  |
| /29    | 512K | 128M | 32G  | 99   |
| /30    | 256K | 64M  | 16G  | 98   |
| /31    | 128K | 32M  | 8G   | 97   |
| /32    | 64K  | 16M  | 4G   | 96   |
| /33    | 32K  | 8M   | 2G   | 95   |
| /34    | 16K  | 4M   | 1G   | 94   |
| /35    | 8K   | 2M   | 512M | 93   |
| /36    | 4K   | 1M   | 256M | 92   |
| /37    | 2K   | 512K | 128M | 91   |
| /38    | 1K   | 256K | 64M  | 90   |
| /39    | 512  | 128K | 32M  | 89   |
| /40    | 256  | 64K  | 16M  | 88   |
| /41    | 128  | 32K  | 8M   | 87   |
| /42    | 64   | 16K  | 4M   | 86   |
| /43    | 32   | 8K   | 2M   | 85   |
| /44    | 16   | 4K   | 1M   | 84   |
| /45    | 8    | 2K   | 512K | 83   |
| /46    | 4    | 1K   | 256K | 82   |
| /47    | 2    | 512  | 128K | 81   |
| /48    | 1    | 256  | 64K  | 80   |
| /49    |      | 128  | 32K  | 79   |
| /50    |      | 64   | 16K  | 78   |
| /51    |      | 32   | 8K   | 77   |
| /52    |      | 16   | 4K   | 76   |
| /53    |      | 8    | 2K   | 75   |
| /54    |      | 4    | 1K   | 74   |
| /55    |      | 2    | 512  | 73   |
| /56    |      | 1    | 256  | 72   |
| /57    |      |      | 128  | 71   |
| /58    |      |      | 64   | 70   |
| /59    |      |      | 32   | 69   |
| /60    |      |      | 16   | 68   |
| /61    |      |      | 8    | 67   |
| /62    |      |      | 4    | 66   |
| /63    |      |      | 2    | 65   |
| /64    |      |      | 1    | 64   |

## Örnek:

Your prefix: 2001:db8::/32



Yukarıda paylaşılan örnek şema üzerinden IPv6 planlaması incelenecek olursa:

/32'li bir blok gerek gördükçe çoğaltacak şekilde /48 lık POP noktalarına ayrılmaktadır.

/32 → 64K adet /48 içermektedir.

/48 POP noktası /52'lik alt bloklara ihtiyaç olacak şekilde bölünerek ilerlenmektedir.

/48 → 16 adet /52 bloğu içermektedir.

Küçük çaplı müşterilere /64 IP bloğu dağıtılacağı düşünülürse /52 bloğu içinde 4096 adet müşteri bağlantısı sağlanabilmektedir.

## 1.4 IPv6'yı işletim sistemlerinde aktif etme

Normalde modern işletim sistemlerinin son sürümlerinde IPv6 aktif bir şekilde gelmektedir. Fakat eğer aktif değil ise aşağıdaki gibi IPv6 i aşağıdaki gibi aktif edebilirsiniz.

### 1.4.1 FreeBSD

IPv6 yı aktif etmek için FreeBSD işletim sistemlerinde /etc/rc.conf network konfigürasyon dosyası içindeki ipv6\_enable satırını yes yapmalıyız.

```
# cat /etc/rc.conf  
ipv6_enable=yes
```

IPv6 in aktif olup olmadığını ifconfig <interface\_name> komutu ile kontrol edebiliriz.

```
# ifconfig fxp0
```

netif komutu ile network servisini restart edebilirsiniz.

```
# /etc/rc.d/netif start  
# /etc/rc.d/netif stop  
# /etc/rc.d/netif restart
```

İşletim sisteminin Fe80:: ile başlayan IP adresini interface e atandığını görmelisiniz.

Ayrıca IPv6 loopback IP adresi olan ::1 IP adresine ping atarak kontrol yapabilirsiniz.

```
# ping6 ::1
```

### 1.4.2 Linux

IPv6 yı aktif etmek için FreeBSD işletim sistemlerinde /etc/rc.conf network konfigürasyon dosyası içindeki ipv6\_enable satırını yes yapmalıyız.

```
# cat /etc/sysconfig/network  
NETWORKING_IPV6=yes
```

service veya systemd komutu ile network servisini restart edebilirsiniz.

```
# /sbin/service network restart
```

veya

```
# systemctl restart networking
```

İşletim sisteminin Fe80:: ile başlayan IP adresini interface e atandığını görmelisiniz.

Ayrıca IPv6 loopback IP adresi olan ::1 IP adresine ping atarak kontrol yapabilirsiniz.

```
# ping6 ::1
```

### 1.4.3 Windows

Windows işletim sistemlerinde IPv6 özellikleri kurulum sırasında yüklenir ve aktif edilir. Eğer IPv6 aktif değil ise

```
# netsh interface ipv6 install
```

Komutu ile aktif edilebilir.

```
# ipconfig
```

Komutu ile İşletim sisteminin Fe80:: ile başlayan IP adresinin arayüze atandığını görmelisiniz.

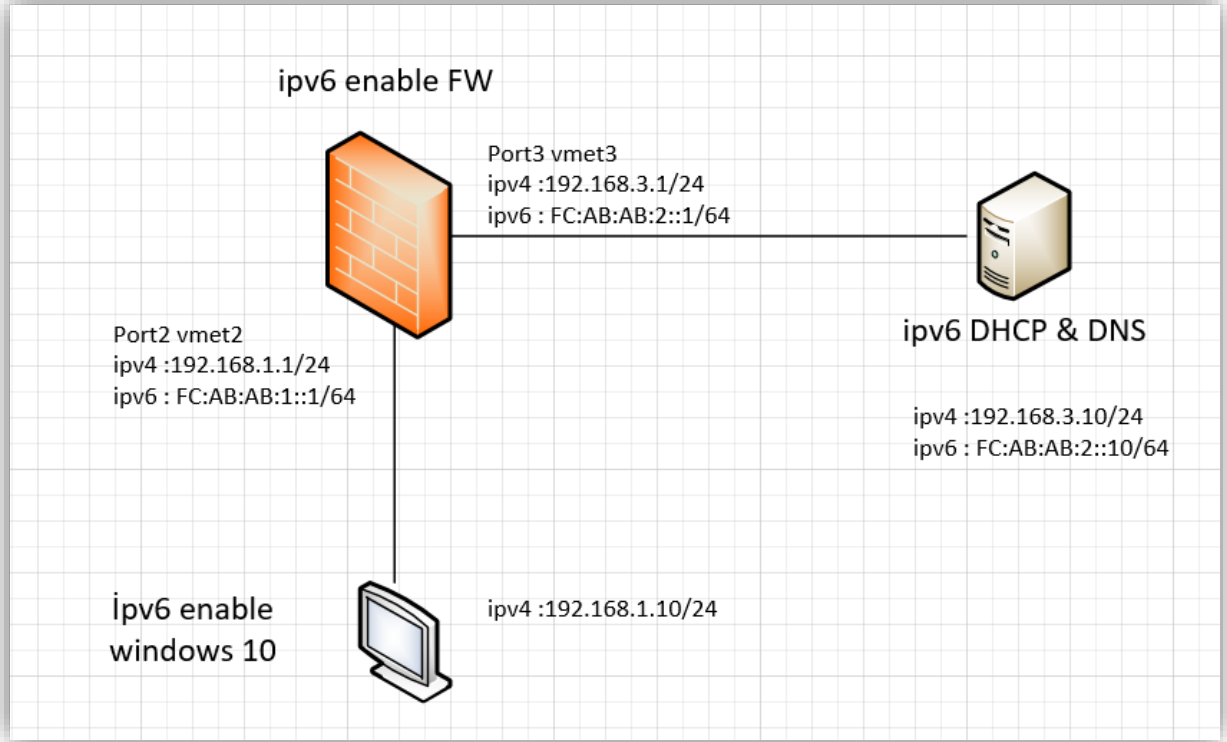
```
# ping ::1
```

Komutu ile *loopback interface*'e ping atarak test edebiliriz.

IPv6 adresleri verildikten sonra tüm düğümlere çoklu gönderim adresi olan ff02::1 adresine ping atabilirsiniz. Bu adrese ping atınca bu ping paketi sizin node unuzun bulunduğu network de bulunan tüm node'lara gönderilir ve bu nodeların hepsinden gelen cevap paketleri sizin node'a gelir. Böylece aynı network de bulunan tüm node'ları öğrenmiş olursunuz. Aynı network içindeki haberleşme link local IP adresi ile yapıldığı için tüm cevap paketleri fe80:: IPv6 adresine sahiptir.

## 1.5 Windows Sistemlerde DHCPv6, DNSv6 Konfigürasyonu

DHCPv6 ve DNSv6 konfigürasyonlarına ilişkin hususlar, topolojisi aşağıda verilen bir uygulama üzerinden anlatılmaktadır.

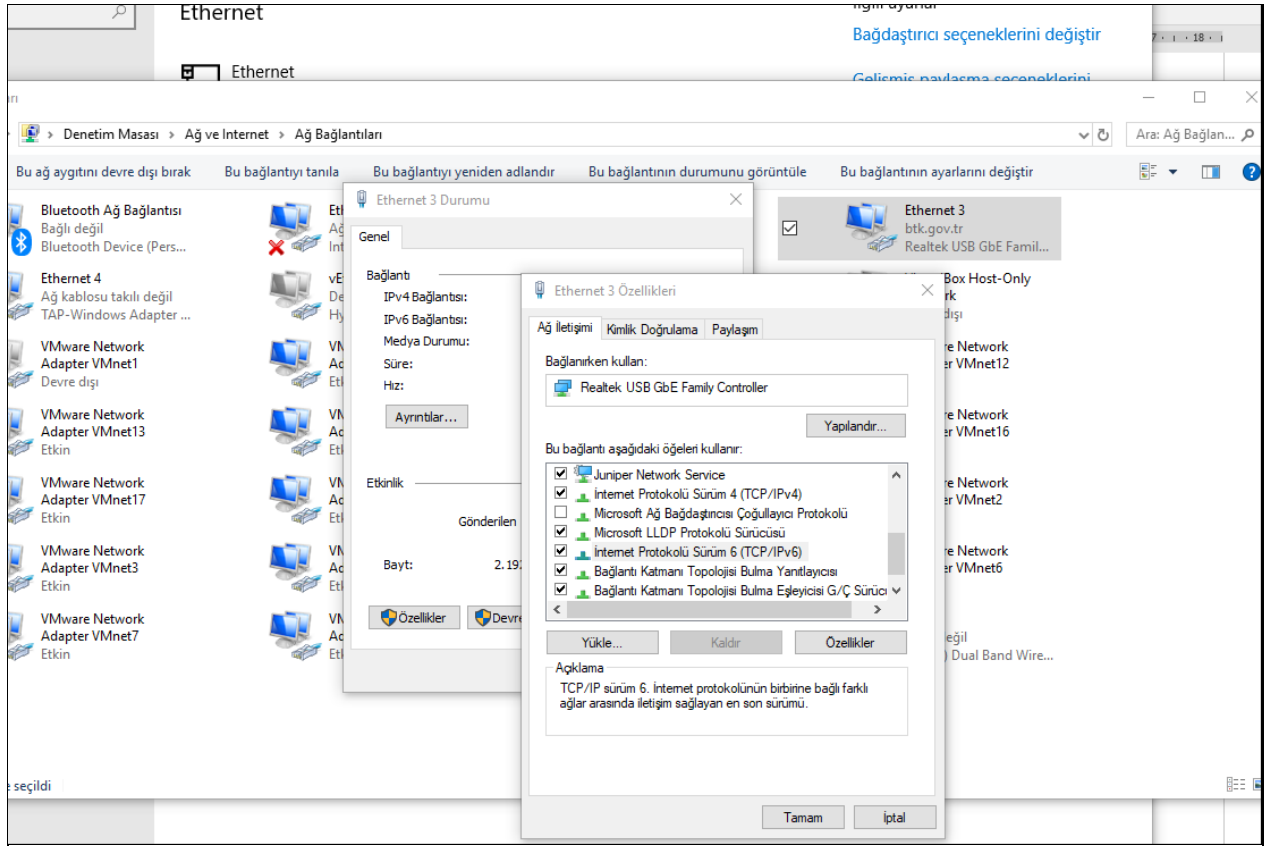


Uygulamada sırasıyla aşağıdaki işlemler gerçekleştirilecektir:

- 1) Düğümlere statik IPv4 adresleri atanarak erişimlerin sağlanması.
- 2) Win10 makinesinin durum tutmayan (*stateless*) *metod ile* IP alması için yapılandırma yapılması
- 3) Win10 makinesinin durum tutan (*statefull*) *metod ile* IP alması için yapılandırma yapılması

### 1.5.1 Düğümlere Statik IPv4 ve IPv6 Verilmesi

Statik IP adreslerini Denetim Masası\Ağ ve İnternet\Ağ Bağlantıları başlığı altında yer alan “ethernet özellikleri” başlığı altından yapılabilmektedir.



Topolojideki Windows 10 ve Windows 2012 sunucuda statik IP ataması yapıldıktan ve ağ geçidinde ilgili izinler verildikten sonra erişimlerin sağlanıp sağlanamadığı ping6 komutu ile test edilebilir.

```
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix  . : 
IPv6 Address. . . . . : fc:ab:ab:2::10
Link-local IPv6 Address . . . . . : fe80::70c8:2058:bd46:21e9%12
IPv4 Address. . . . . : 192.168.3.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fc:ab:ab:2::1
                            192.168.3.1

Tunnel adapter isatap.{DB97D689-655A-4DC8-A463-35C65A5BBAA5}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 

C:\Users\Administrator>ping -6 FC:AB:AB:1::10

Pinging fc:ab:ab:1::10 with 32 bytes of data:
Reply from fc:ab:ab:1::10: time<1ms
Reply from fc:ab:ab:1::10: time<1ms
Reply from fc:ab:ab:1::10: time<1ms
Reply from fc:ab:ab:1::10: time<1ms

Ping statistics for fc:ab:ab:1::10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

### 1.5.2 Durumsuz (Stateless) IP Yapılandırması

Ağ geçidi üzerinde yapılan aşağıdaki yapılandırma sayesinde istemci link-local IP adresini kullanarak ağ geçidini bulacak ve ağ geçidi üzerinden kullanacağı ön ek bilgisini görebilecektir. Söz konusu yapılandırma cihazdan cihaza değişebilmekle birlikte iki portta belirtilen *ipv6-prefix-list* komutu çalıştırıldığında ilgili porttan yayınlanacak IPv6 öneki görülebilmektedir.

```
edit "port2"
  set vdom "root"
  set ip 192.168.1.1 255.255.255.0
  set allowaccess ping https ssh http
  set type physical
  set snmp-index 2
  config ipv6
    set ip6-address fc:ab:ab:1::1/64
    set ip6-allowaccess ping https ssh
    set ip6-send-adv enable
    config ip6-prefix-list
      edit fc:ab:ab:1::/64
      next
    end
  end
next
edit "port3"
  set vdom "root"
  set ip 192.168.3.1 255.255.255.0
  set allowaccess ping
  set type physical
  set snmp-index 3
  config ipv6
    set ip6-address fc:ab:ab:2::1/64
    set ip6-allowaccess ping https ssh
    set ip6-send-adv enable
    config ip6-prefix-list
      edit fc:ab:ab:2::/64
      next
    end
  end
end
```

Port2 arkasındaki Windows 10 işletim sisteminde *ipconfig* komutu ile alınan IP adresin kontrol edildiğinde fc:ab:ab:1::/64 bloğundan IP aldığı görülmektedir.

```
Ethernet adapter Ethernet0 2:

Connection-specific DNS Suffix . . : 
IPv6 Address. . . . . : fc:ab:ab:1:ec67:a6ab:52b6:7662
Temporary IPv6 Address. . . . . : fc:ab:ab:1:fd26:b3ed:8ab6:2d54
Link-local IPv6 Address . . . . . : fe80::ec67:a6ab:52b6:7662%7
IPv4 Address. . . . . : 192.168.1.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::20c:29ff:fea0:2328%7
                          192.168.1.1
```

Benzer şekilde Port3 arkasındaki Windows 2012 sunucudan kontrol edildiğinde fc:ab:ab:2::/64 bloğundan IP bilgisi aldığı görülmektedir. *Ping* komutu ile farklı bloklar arasındaki erişim test edilebilmektedir.

```

C:\Users\Administrator>ping -6 fc:ab:ab:1:ec67:a6ab:52b6:7662 -t

Pinging fc:ab:ab:1:ec67:a6ab:52b6:7662 with 32 bytes of data:
Reply from fc:ab:ab:1:ec67:a6ab:52b6:7662: time<1ms
Reply from fc:ab:ab:1:ec67:a6ab:52b6:7662: time<1ms
Reply from fc:ab:ab:1:ec67:a6ab:52b6:7662: time<1ms
Reply from fc:ab:ab:1:ec67:a6ab:52b6:7662: time<1ms
Reply from fc:ab:ab:1:ec67:a6ab:52b6:7662: time<1ms
Reply from fc:ab:ab:1:ec67:a6ab:52b6:7662: time<1ms
Reply from fc:ab:ab:1:ec67:a6ab:52b6:7662: time<1ms
Reply from fc:ab:ab:1:ec67:a6ab:52b6:7662: time<1ms
Reply from fc:ab:ab:1:ec67:a6ab:52b6:7662: time<1ms
Reply from fc:ab:ab:1:ec67:a6ab:52b6:7662: time<1ms
Reply from fc:ab:ab:1:ec67:a6ab:52b6:7662: time<1ms

Ping statistics for fc:ab:ab:1:ec67:a6ab:52b6:7662:
    Packets: Sent = 11, Received = 11, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C

```

Varsayılan rota (*default route*) kaydına *router print -6* komutu ile bakıldığında kaydın ağ geçidinin global unicast IP'si olmadığı, onun yerine ağ geçidinin link local IP adresi olduğu görülebilmektedir.

```

IPv6 Address. . . . . : fc:ab:ab:2:70c8:2058:bd46:21e9
Link-local IPv6 Address . . . . . : fe80::70c8:2058:bd46:21e9%12
IPv4 Address. . . . . : 192.168.3.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::20c:29ff:fea0:2332%12
                             192.168.3.1

Tunnel adapter isatap.{DB97D689-655A-4DC8-A463-35C65A5BBAA5}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\Administrator>route print -6
=====
Interface List
 12...00 0c 29 4c 59 01 .....Intel(R) 82574L Gigabit Network Connection
 1.....Software Loopback Interface 1
 13...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
=====

IPv6 Route Table
=====
Active Routes:
    If Metric Network Destination      Gateway
    12     266 ::/0                      fe80::20c:29ff:fea0:2332
    1       306 ::1/128                    On-link
    12     266 fc:ab:ab:2::/64                On-link
    12     266 fc:ab:ab:2:70c8:2058:bd46:21e9/128
                                         On-link
    12     266 fe80::/64                      On-link
    12     266 fe80::70c8:2058:bd46:21e9/128
                                         On-link
    1       306 ff00::/8                      On-link

```

Ayrıca ağ geçidinin MAC adresinden link lokal adresi hesaplanabilmektedir:

Port3'teki ağ geçidinin MAC adresi : 00:0C:29:A0:23:32 dir. MAC adresi EUI-64 işlemine tabi tutulursa;

00:0C:29:FF:FE:A0:23:32

0000 0000:0C:29:FF:FE:A0:23:32

Fe80::02:0C:29:FF:FE:A0:23:32

Port 3'ün link-local unicast adresi : fe80::20C:29FF:FEA0:2332 olduğu görülebilmektedir.

### 1.5.3 Ağ Geçidi Üzerinden Düğümlere DNS Adresi Verilmesi

Ağ geçidi düğümlere DNS'i DHCP den alması gerektiği bilgisini *other flag* değerini 1 olarak ayarlandığında yapmaktadır. Bu işlem *set ip6-other-flag enable* komutu ile yapılmaktadır.

```
testfw (port2) # show
config system interface
  edit "port2"
    set vdom "root"
    set ip 192.168.1.1 255.255.255.0
    set allowaccess ping https ssh http
    set type physical
    set snmp-index 2
    config ipv6
      set ip6-address fc:ab:ab:1::1/64
      set ip6-allowaccess ping https ssh
      set ip6-send-adv enable
      set ip6-other-flag enable
      config ip6-prefix-list
        edit fc:ab:ab:1::/64
        next
      end
    end
  next
end
```

Bu uygulamada DHCP sunucu olarak ağ geçidi olarak kullanılan "testfw" kullanılacaktır.

```
testfw # config system dhcp6 server
testfw (server) # show
config system dhcp6 server
  edit 1
    set domain "abc.com"
    set interface "port2"
    set dns-server1 fc:ab:ab:2::10
  next
end
```

İstemci tarafından kontrol edildiğinde DNS adresi olarak fc:ab:ab:2::10 adresi görülebilmektedir.

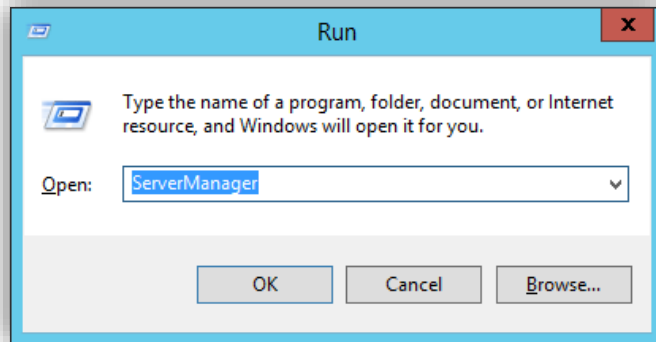
```
Ethernet adapter Ethernet0 2:

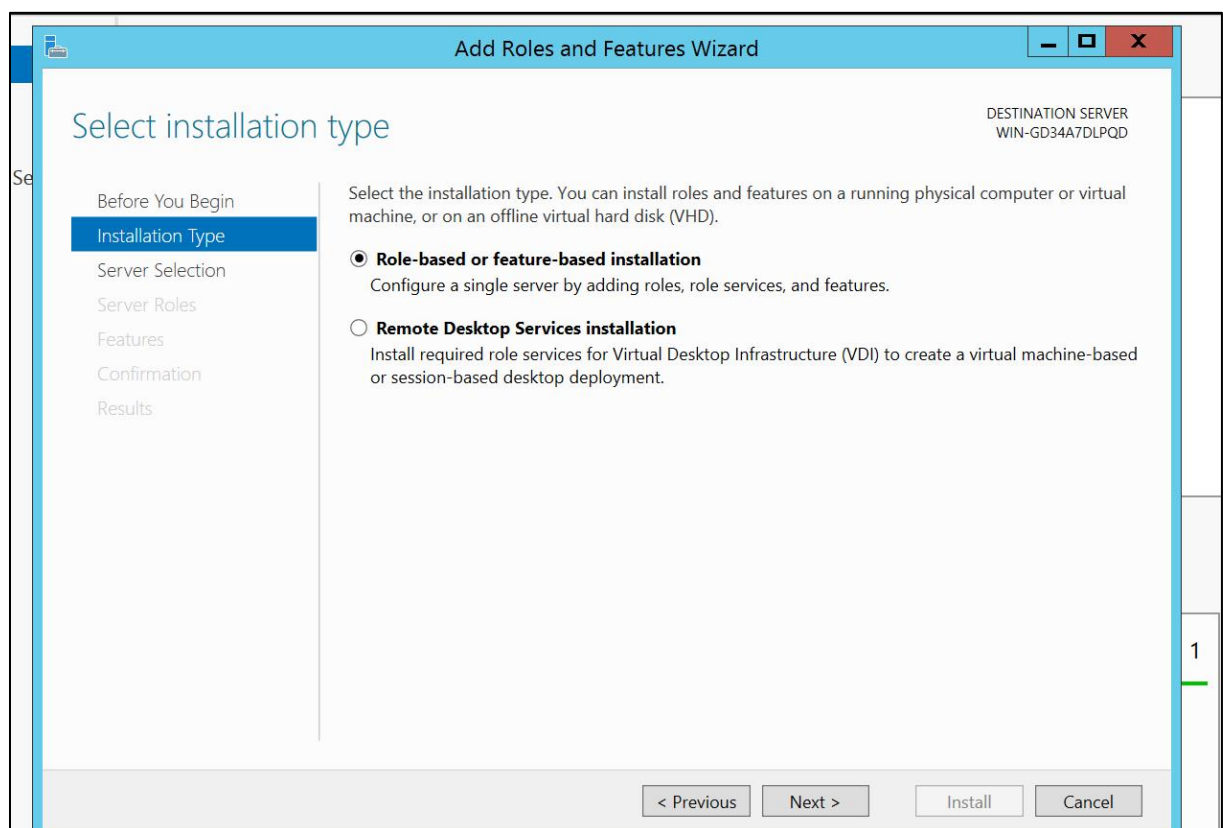
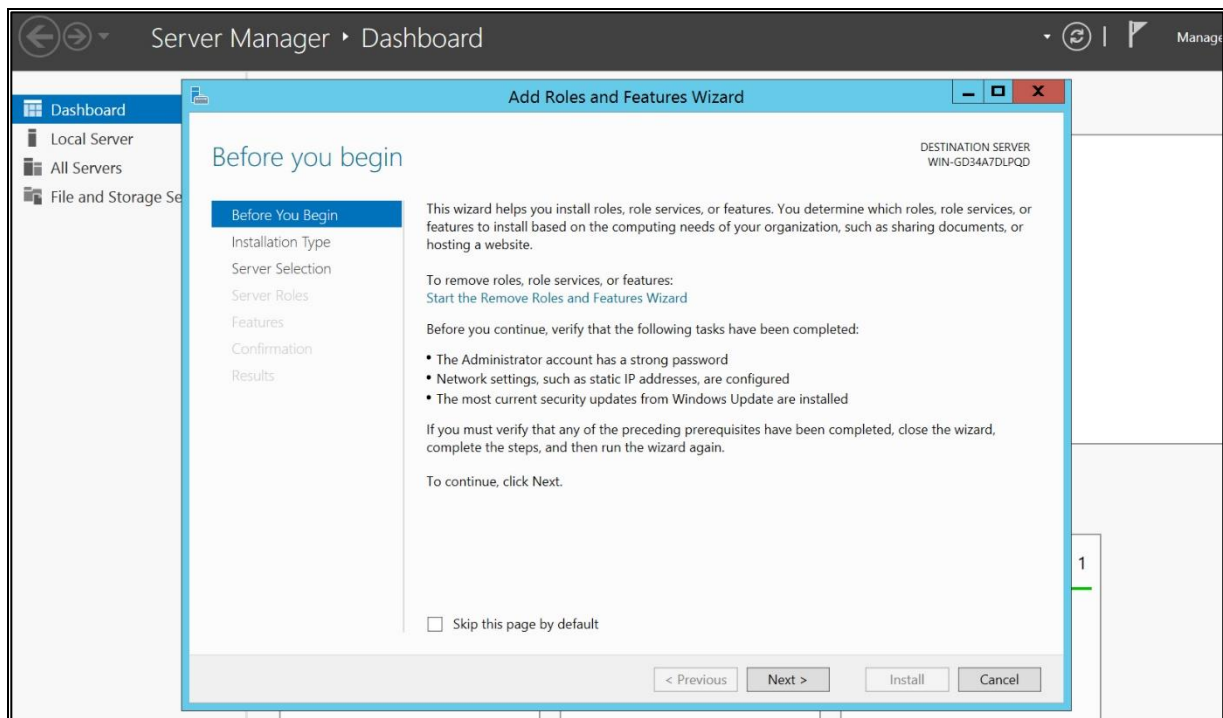
Connection-specific DNS Suffix . . : abc.com
Description . . . . . : Intel(R) PRO/1000 MT Network Connection #2
Physical Address. . . . . : 00-0C-29-E6-7C-1F
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : fc:ab:ab:1:ec67:a6ab:52b6:7662(Preferred)
Temporary IPv6 Address. . . . . : fc:ab:ab:1:54a3:9822:2ca0:fbbd(Preferred)
Link-local IPv6 Address . . . . . : fe80::ec67:a6ab:52b6:7662%7(Preferred)
IPv4 Address. . . . . : 192.168.1.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::20c:29ff:fea0:2328%7
                             192.168.1.1
DHCPv6 IAID . . . . . : 83889193
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-7F-E8-53-00-0C-29-11-3E-52
DNS Servers . . . . . : fc:ab:ab:2::10
NetBIOS over Tcpi. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                             abc.com
```

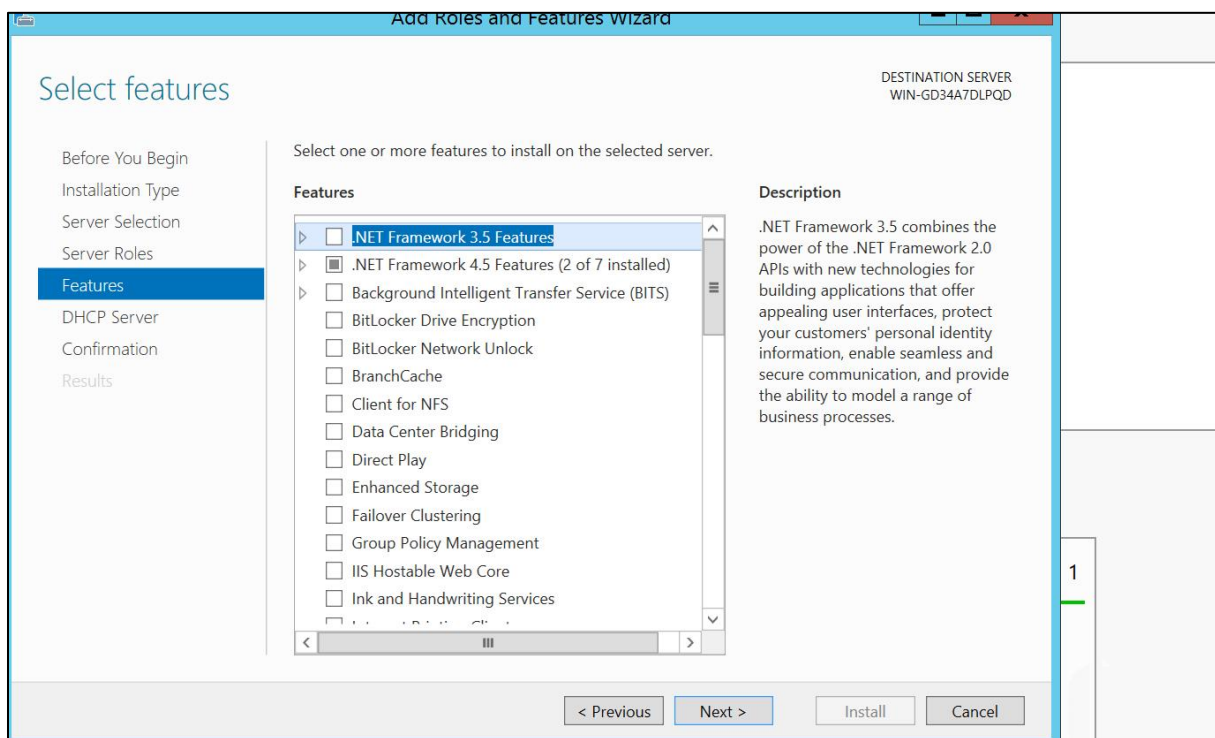
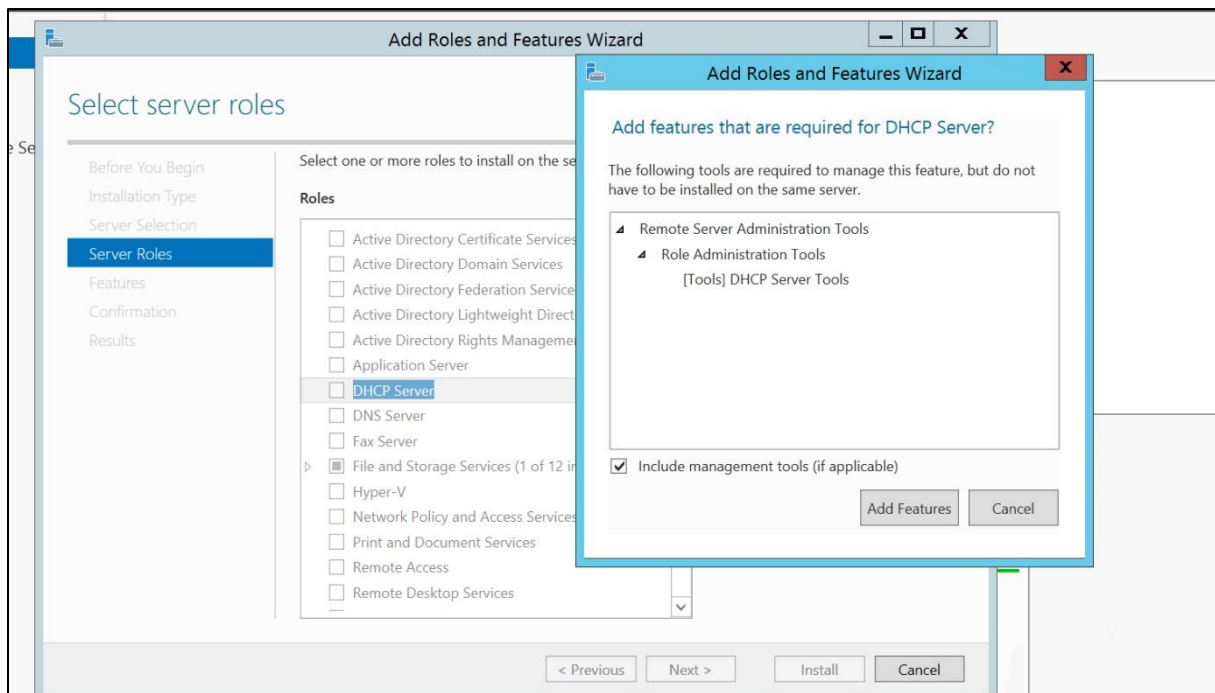
#### 1.5.4 DHCPv6 ile Duruma Bağlı (*Statefull*) IP Yapılandırması

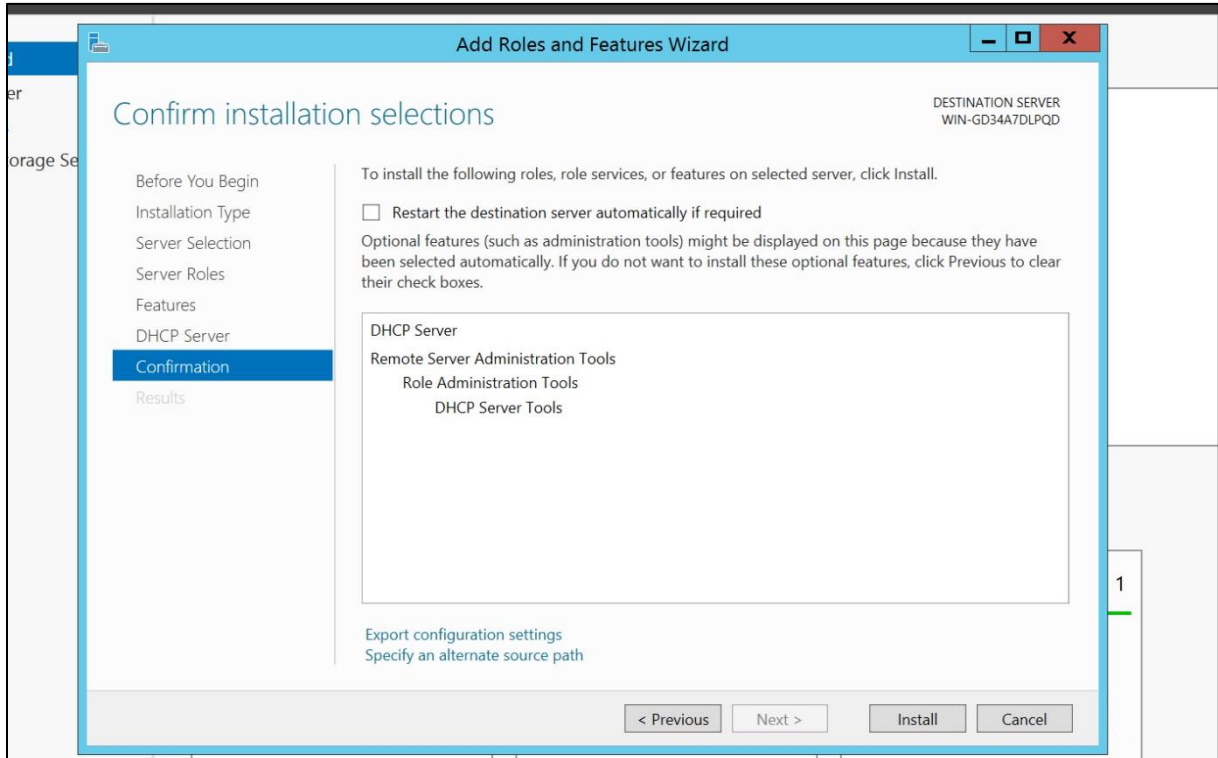
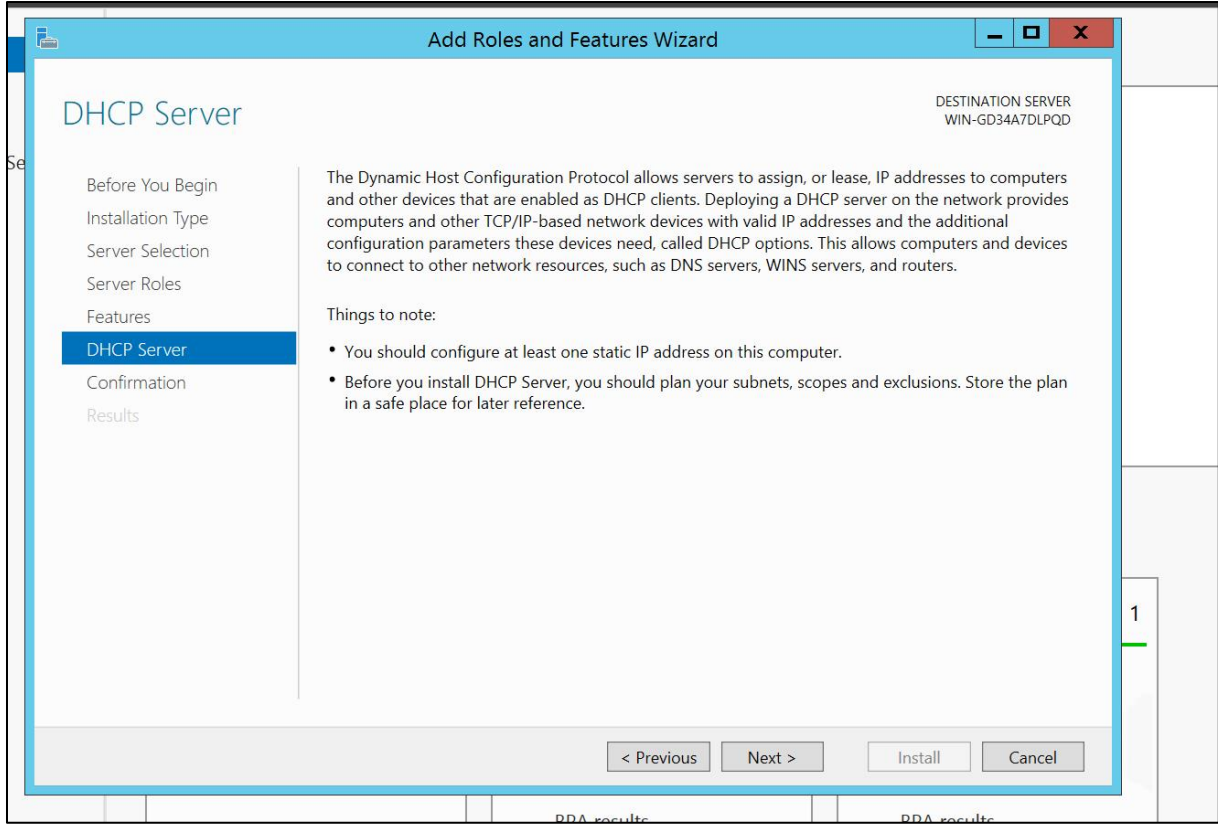
Windows DHCPv6 kurulumunda izlenecek temel adımlar aşağıdaki gibidir.

Çalıştır alanına *ServerManager* yazılır.



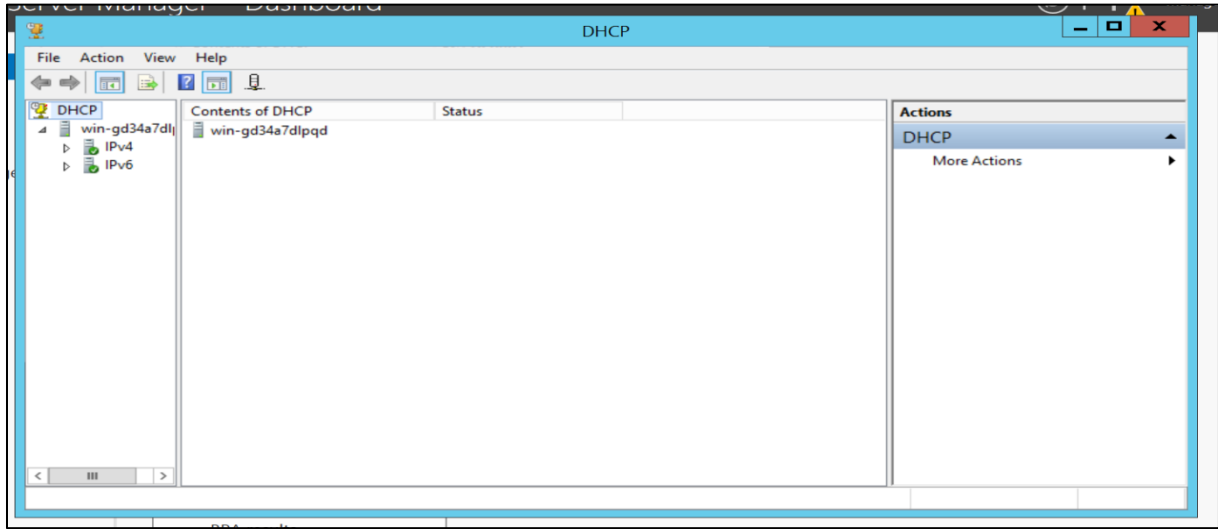




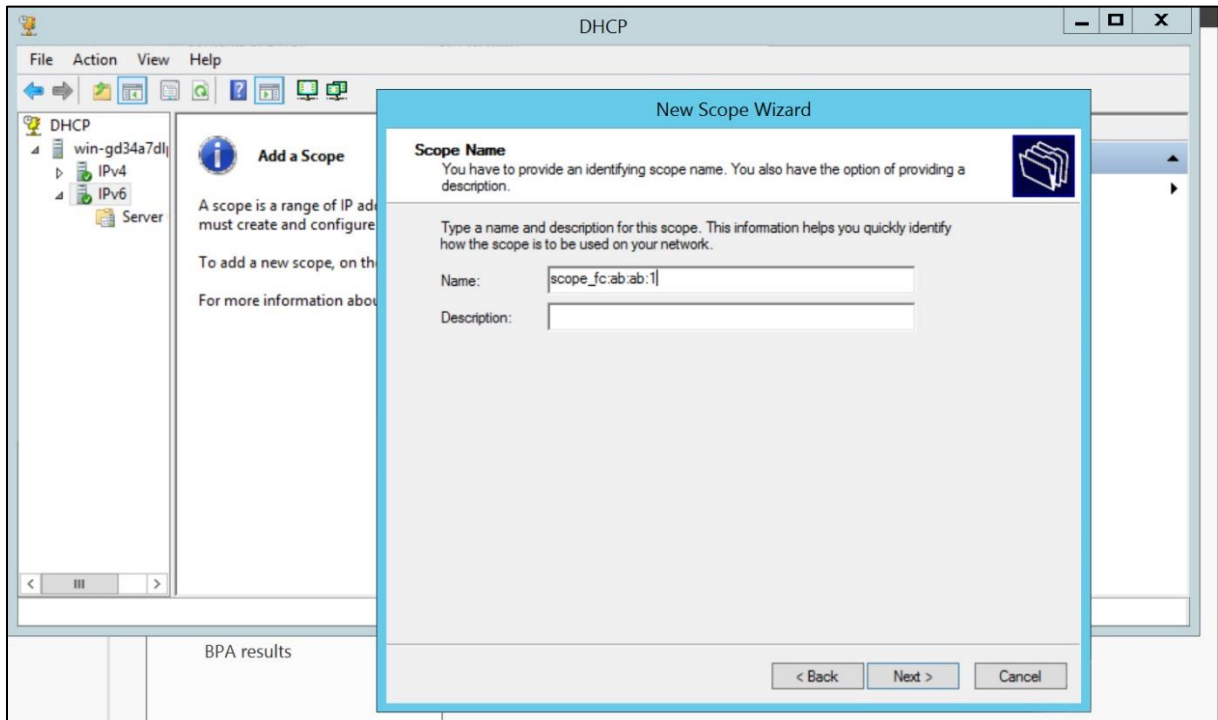


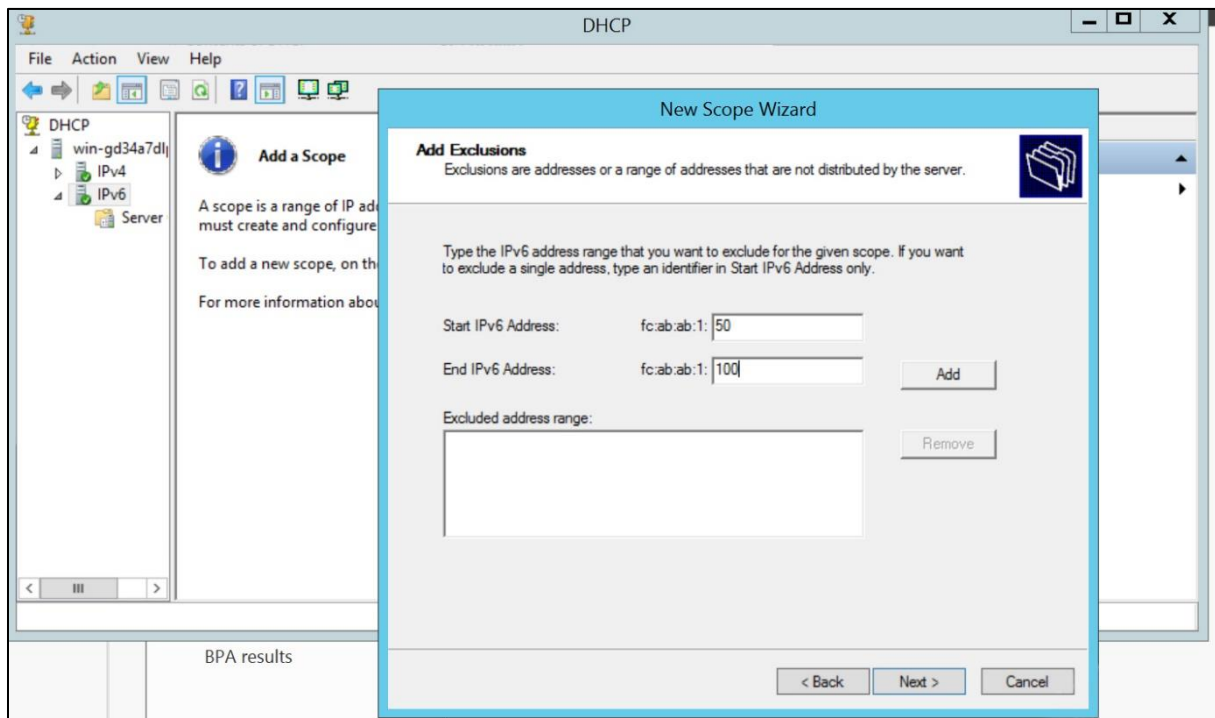
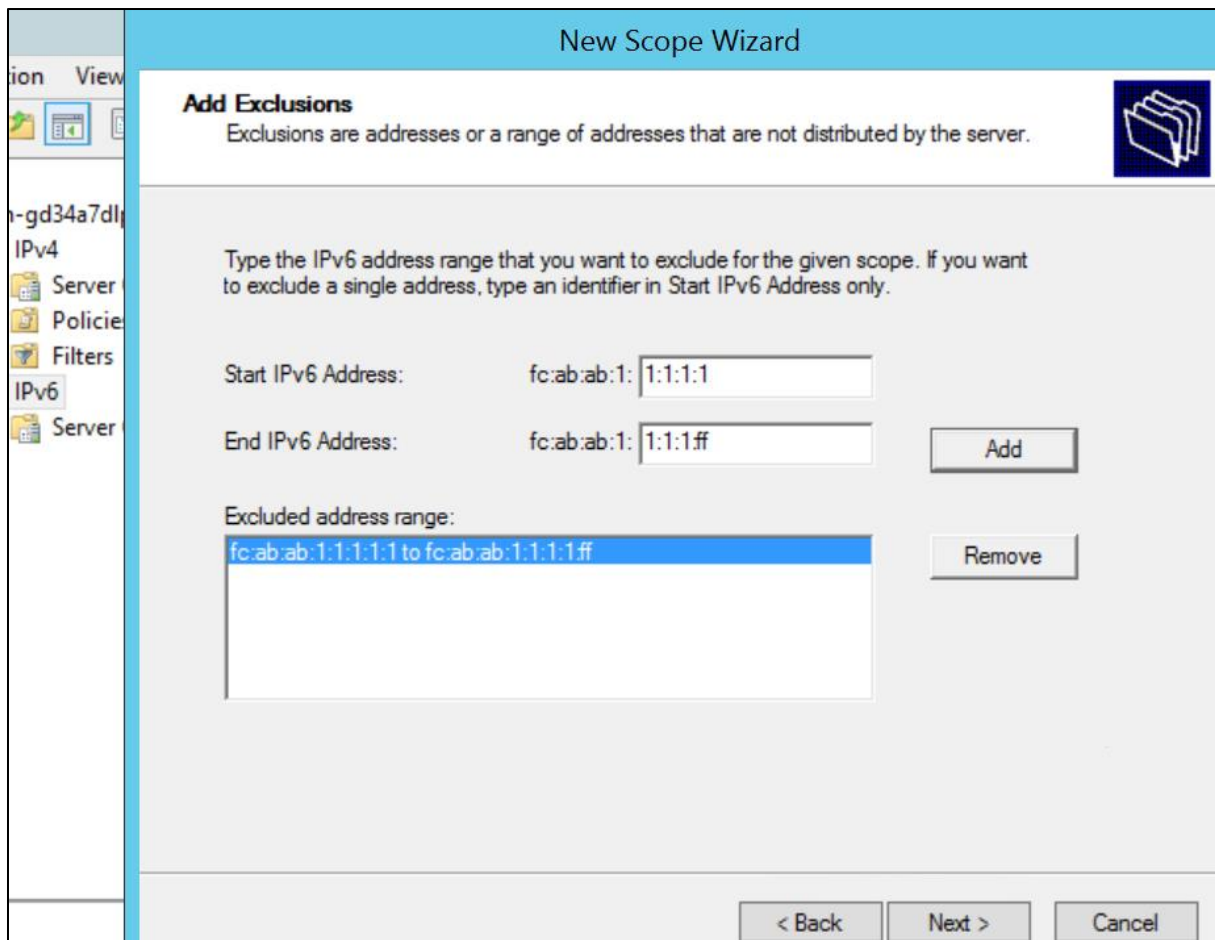
Kurulum tamamlandıktan sonra DHCP sunucu konsolunda çalıştır alanına *dhcpgmt.msc* yazılarak veya sistem yönetici menüsünden araçlar başlığı altındaki DHCP seçilerek erişilebilmektedir.

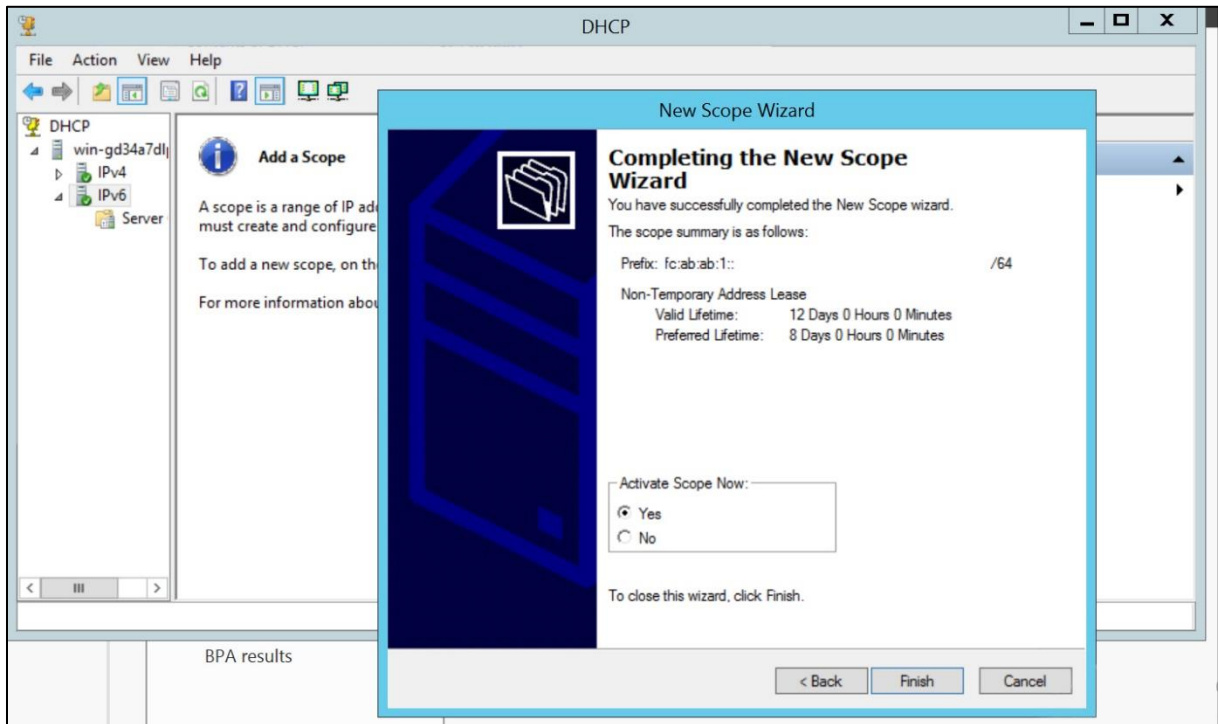
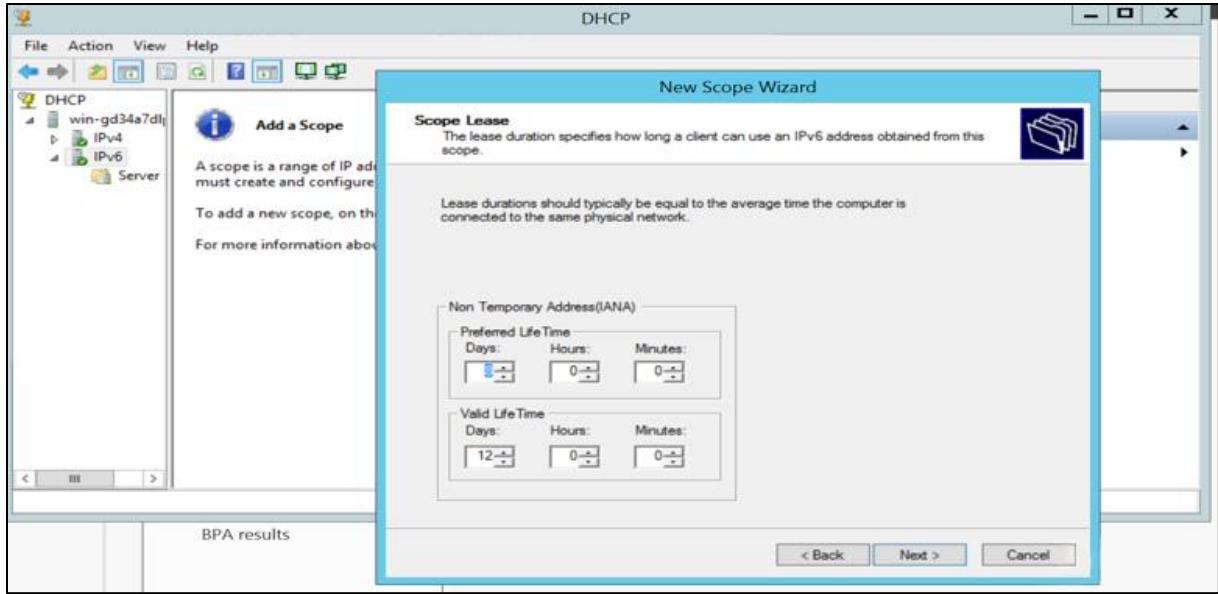
DHCP yönetim konsolu aşağıdaki gibidir:



Bir sonraki adımda fc:ab:ab:1::/64 bloğu için DHCP’de kapsam tanımı yapılabilmesi için:







Genelde DHCP sunucuları düğümlerden farklı bir ağ bloğunda yer almaktadır. Bu durumda düğümün bağlı bulunduğu ağ geçidi üzerinde *DHCP relay* konfigürasyonu yapılmalı ve bu konfigürasyonda DHCP sunucusunun IPv6 adresi belirtilmelidir.

Aşağıda Fortigate marka bir firewall'da *DHCP relay* konfigürasyonunun nasıl yapıldığı görülebilmektedir.

```
testfw (port2) # show
config system interface
  edit "port2"
    set vdom "root"
    set ip 192.168.1.1 255.255.255.0
    set allowaccess ping https ssh http
    set type physical
    set snmp-index 2
    config ipv6
      set ip6-address fc:ab:ab:1::1/64
      set ip6-allowaccess ping https ssh
      set ip6-send-adv enable
      set ip6-manage-flag enable
      set ip6-other-flag enable
      set dhcp6-relay-service enable
      set dhcp6-relay-ip fc:ab:ab:2::10
    end
  next
end
```

İstemci tarafında durumsuz olarak alınan IP adresinin aşağıdaki gibi bırakılıp, tekrar IP talep edildiğinde DHCP sunucuda belirtilen aralıktan IP alındığı görülebilmektedir.

|                                                                 |                                                                 |
|-----------------------------------------------------------------|-----------------------------------------------------------------|
| C:\Users\IEUser>ipconfig /release6                              | C:\Users\IEUser>ipconfig /renew6                                |
| Windows IP Configuration                                        | Windows IP Configuration                                        |
| Ethernet adapter Ethernet0 2:                                   | Ethernet adapter Ethernet0 2:                                   |
| Connection-specific DNS Suffix . :                              | Connection-specific DNS Suffix . :                              |
| Link-local IPv6 Address . . . . . : fe80::ec67:a6ab:52b6:7662%7 | IPv6 Address. . . . . : fc:ab:ab:1:748e:ca1d:6429:a6a6          |
| IPv4 Address. . . . . : 192.168.1.10                            | Link-local IPv6 Address . . . . . : fe80::ec67:a6ab:52b6:7662%7 |
| Subnet Mask . . . . . : 255.255.255.0                           | IPv4 Address. . . . . : 192.168.1.10                            |
| Default Gateway . . . . . : fe80::20c:29ff:fea0:2328%7          | Subnet Mask . . . . . : 255.255.255.0                           |
| 192.168.1.1                                                     | Default Gateway . . . . . : fe80::20c:29ff:fea0:2328%7          |
|                                                                 | 192.168.1.1                                                     |

Windows IPv6 DHCP sunucu üzerinden Windows IPv6 DNS sunucusunu kullanırmak ve DNS sunucusunun kurulumunu yapabilmek amacıyla aşağıdaki işlemler yapılmalıdır:

## Before you begin

DESTINATION SERVER  
WIN-GD34A7DLPQD

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:  
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

< Previous Next > Install Cancel

## Select installation type

DESTINATION SERVER  
WIN-GD34A7DLPQD

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**  
Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**  
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous Next > Install Cancel

## Select destination server

DESTINATION SERVER  
WIN-GD34A7DLPQD

Before You Begin  
Installation Type  
**Server Selection**  
Server Roles  
Features  
Confirmation  
Results

Select a server or a virtual hard disk on which to install roles and features.

- ☒ Select a server from the server pool  
☐ Select a virtual hard disk

### Server Pool

| Filter: <input type="text"/> |              |                                             |
|------------------------------|--------------|---------------------------------------------|
| Name                         | IP Address   | Operating System                            |
| WIN-GD34A7DLPQD              | 192.168.3.10 | Microsoft Windows Server 2012 R2 Datacenter |

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

Next >

Install

Cancel

## Select server roles

DESTINATION SERVER  
WIN-GD34A7DLPQD

Before You Begin  
Installation Type  
Server Selection  
**Server Roles**  
Features  
Confirmation  
Results

Select one or more roles to install on the

### Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☒ DHCP Server (Installed)
- ☐ DNS Server
- ☐ Fax Server
- ☐ File and Storage Services (1 of 12)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

### Add Roles and Features Wizard

#### Add features that are required for DNS Server?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
  - [Tools] DNS Server Tools

☒ Include management tools (if applicable)

Add Features

Cancel

< Previous

Next >

Install

Cancel

Local Server

## Confirm installation selections

DESTINATION SERVER  
WIN-GD34A7DLPQD

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
DNS Server  
**Confirmation**  
Results

To install the following roles, role services, or features on selected server, click Install.

- ☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

|                                    |
|------------------------------------|
| DNS Server                         |
| Remote Server Administration Tools |
| Role Administration Tools          |
| DNS Server Tools                   |

Export configuration settings  
Specify an alternate source path

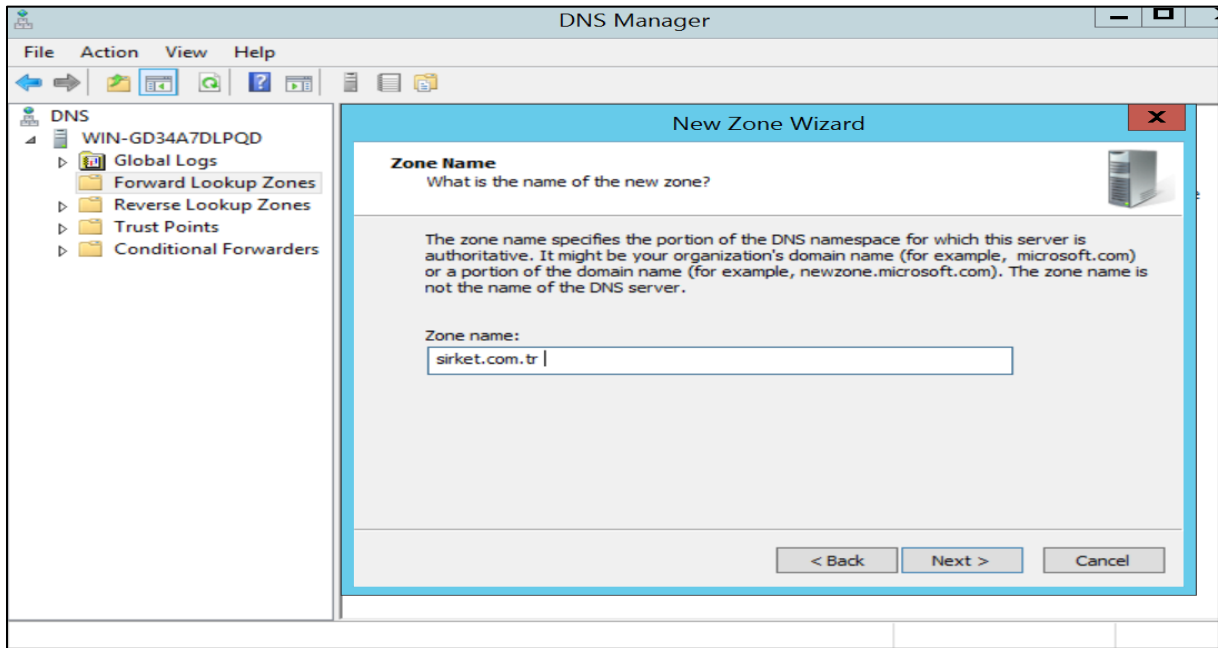
< Previous

Next >

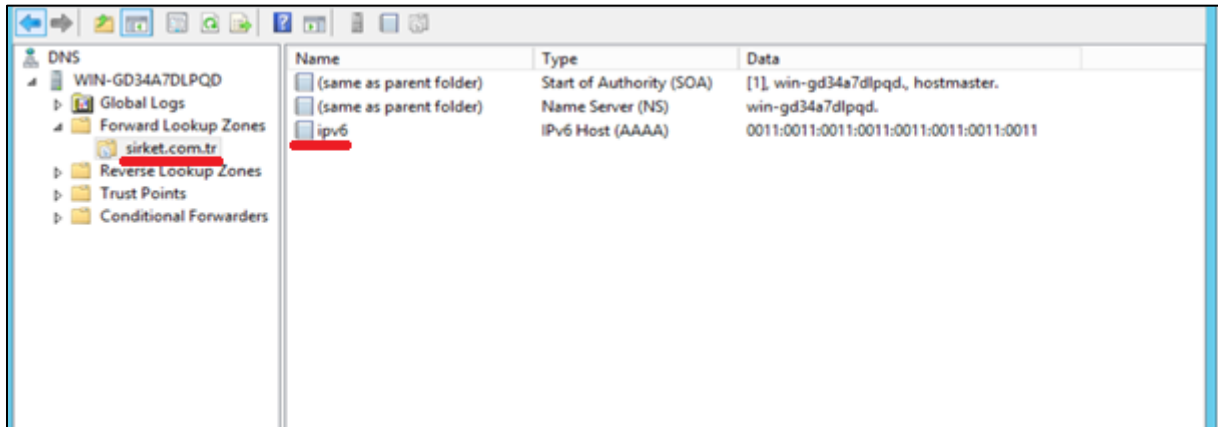
Install

Cancel

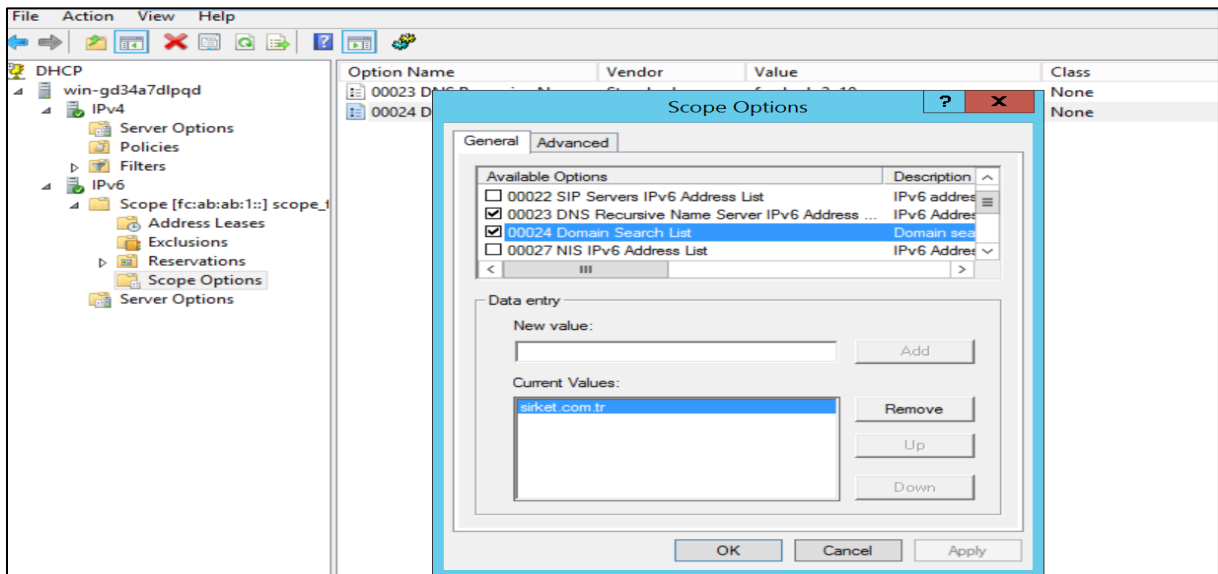
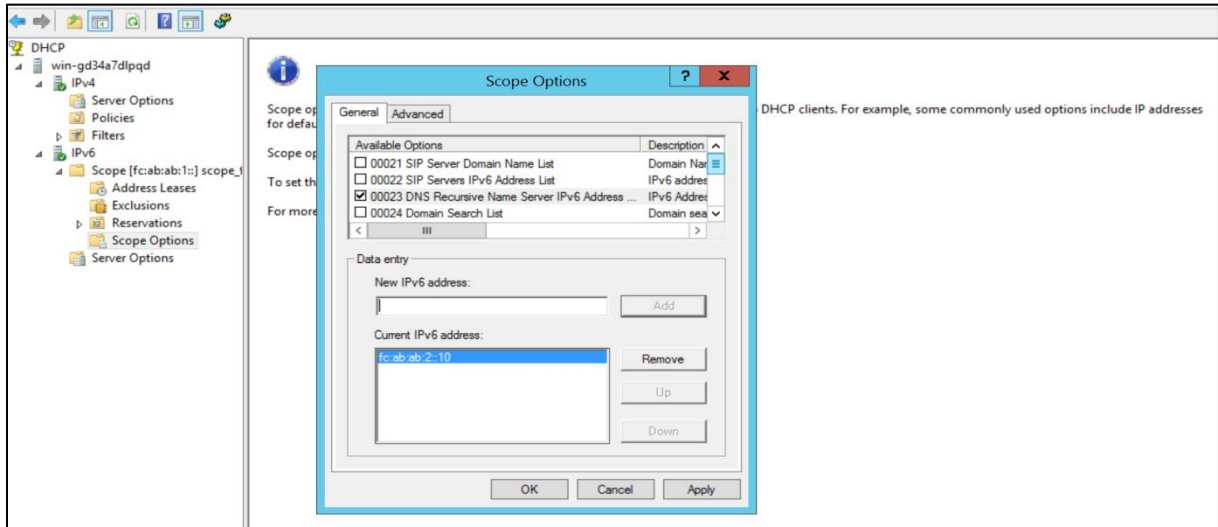
Kurulum sonrasında sirket.com.tr şeklinde bir *zone* tanımı şu şekilde yapılabilir:



Test sırasında kullanmak amacıyla bir host kaydı aşağıdaki şekilde girilebilir:



DHCP tarafında DNS tanımlaması aşağıdaki şekilde gerçekleştirilmektedir.



İstemci tarafında DNS'in IP alıp almadığı şu şekilde kontrol edilebilmektedir:

```
C:\Users\IEUser>ipconfig /renew6
```

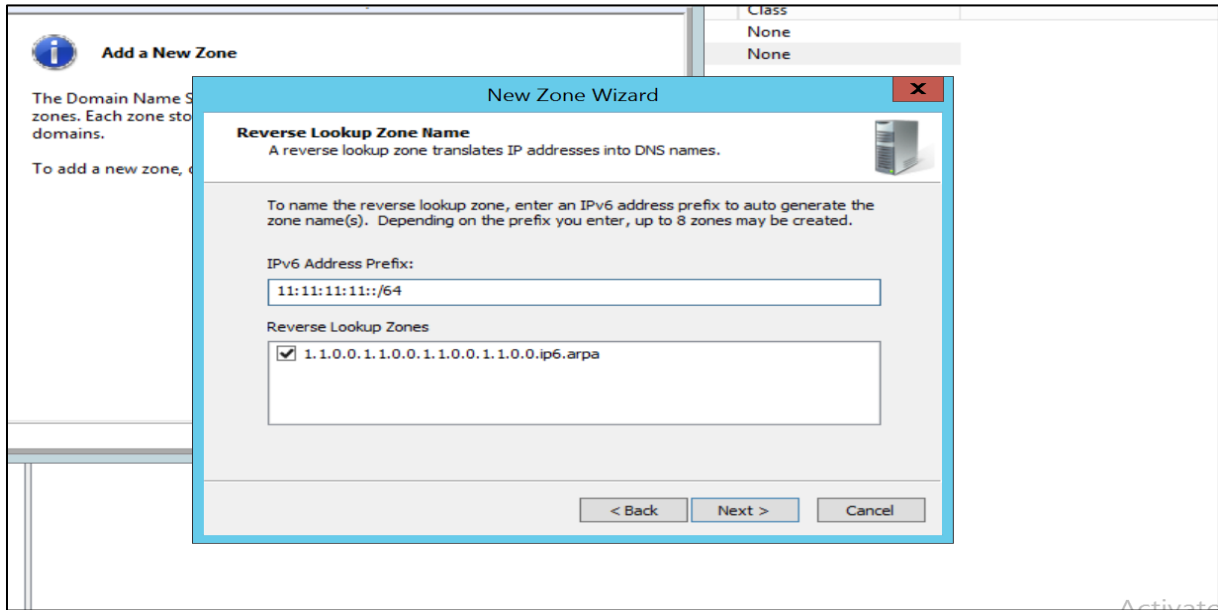
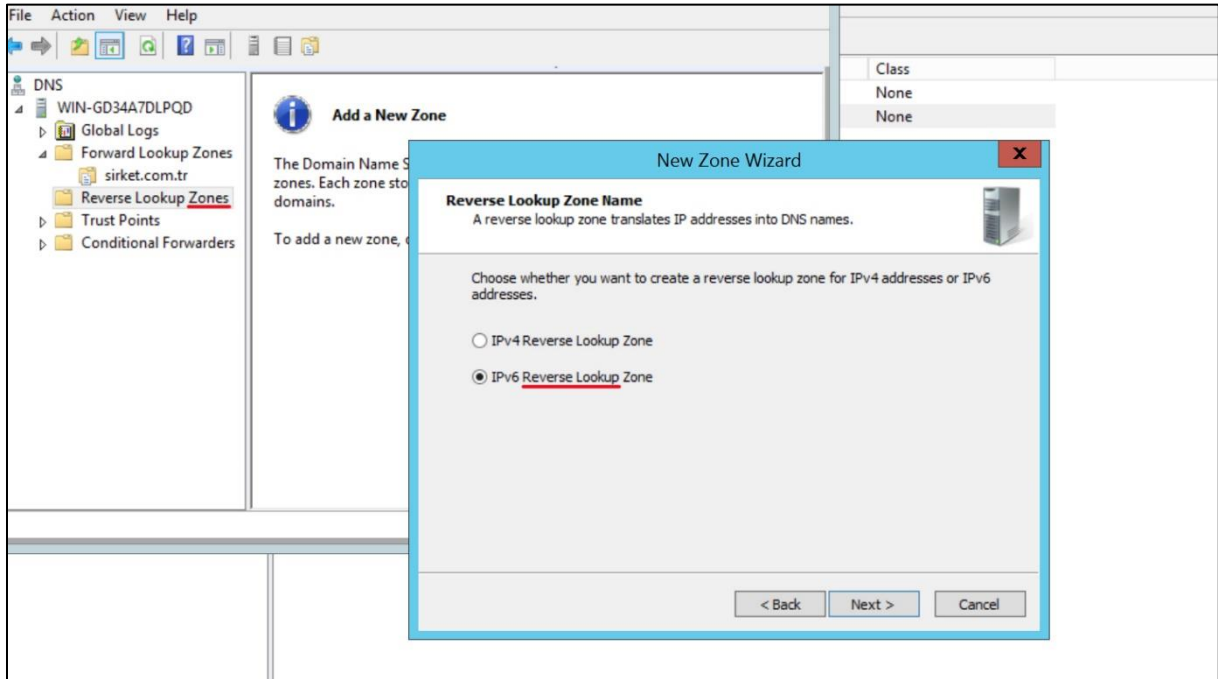
Windows IP Konfigürasyonu

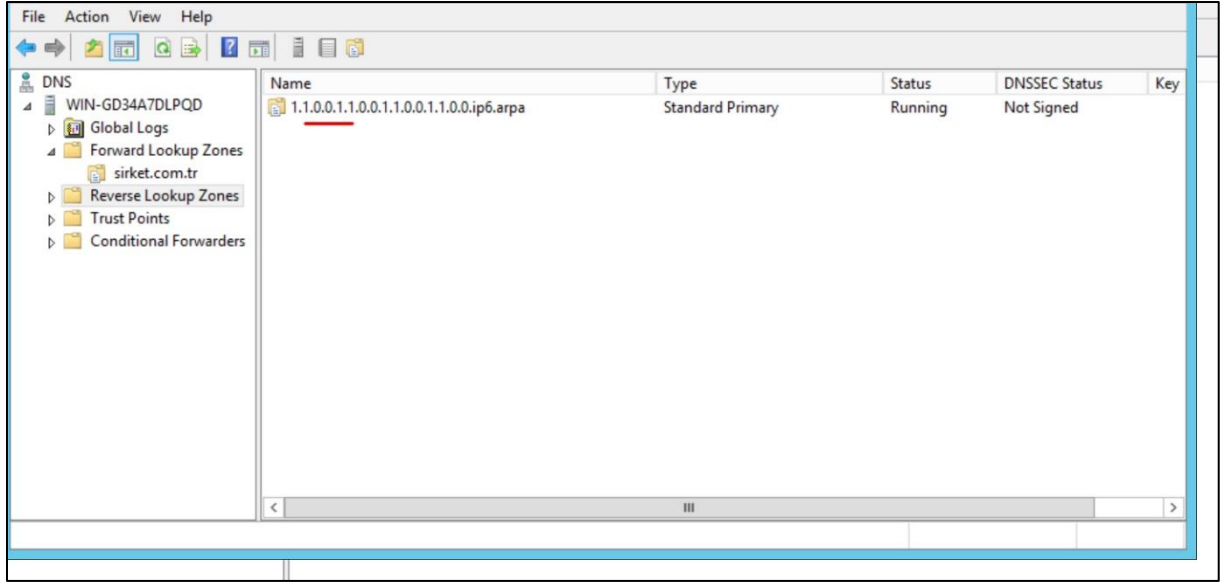
*Ethernet adapter Ethernet0 2:*

```
Connection-specific DNS Suffix . : sirket.com.tr
IPv6 Address. . . . . : fc:ab:ab:1:cedb:fc06:252b:174
Link-local IPv6 Address . . . . . : fe80::ec67:a6ab:52b6:7662%7
IPv4 Address. . . . . : 192.168.1.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::20c:29ff:fea0:2328%7
                           : 192.168.1.1
```

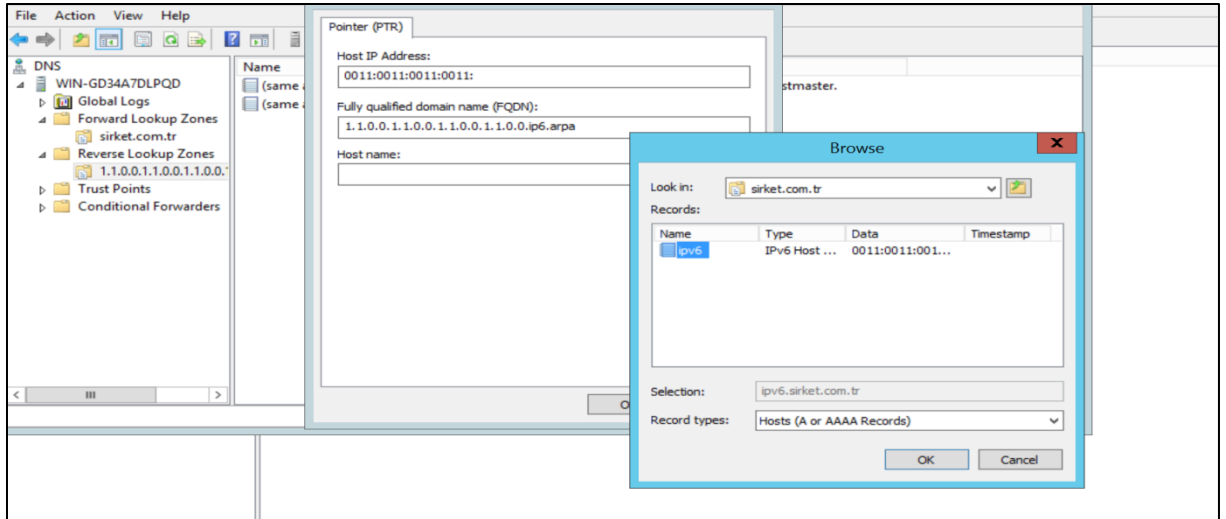


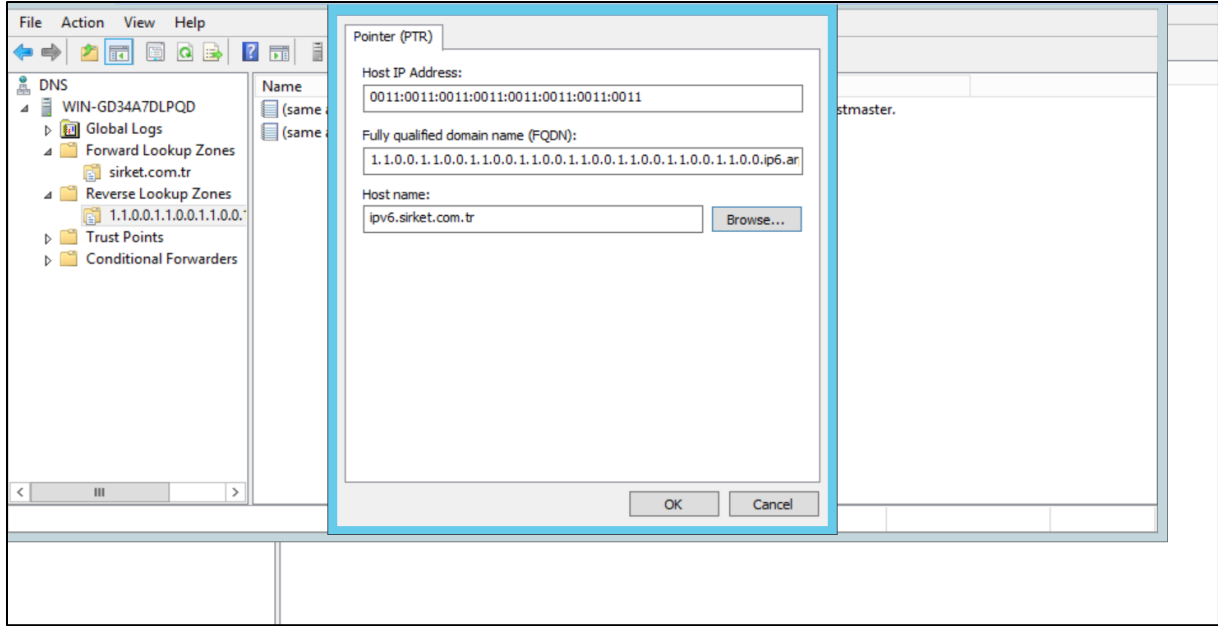
DNS Sunucuda reverse DNS kaydı girilebilmesi için öncelikli olarak reverse zone tanımı yapılmalıdır;





Reverse zone kaydının tamamlanması için:





İstemci tarafında reverse kaydı test edilmek istendiğinde ilgili IP için alan adı elde edilebilmektedir.

> 11:11:11:11:11:11:11:11

Server: UnKnown

Address: fc:ab:ab:2::10

Name: ipv6.sirket.com.tr

Address: 11:11:11:11:11:11:11:11

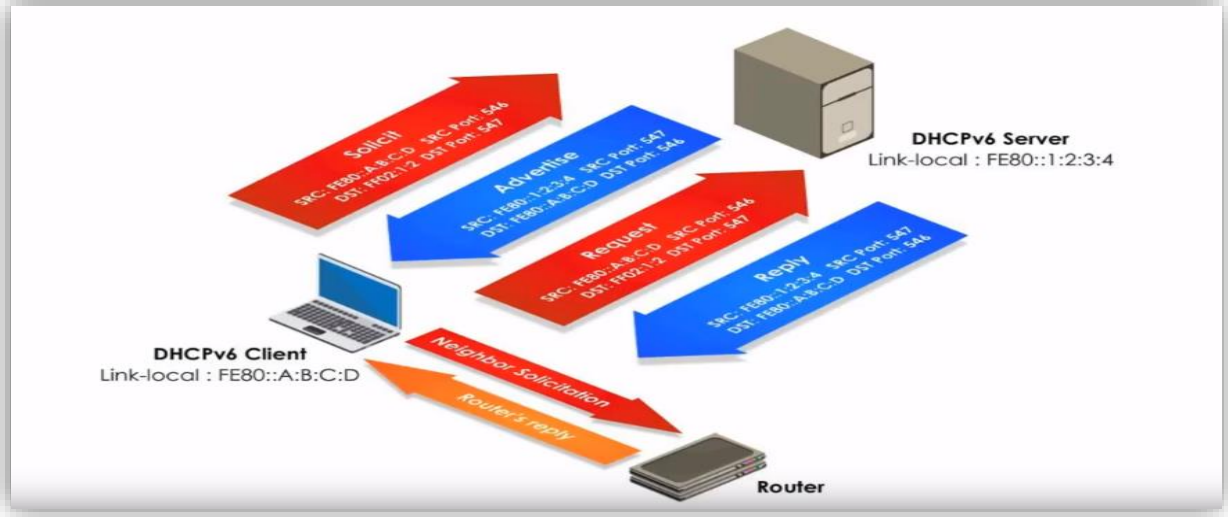
## 1.6 IPv6 Adres Alma Yöntemleri

IPv6'da, cihazlar IPv6 adresini 3 farklı yöntemle alabilmektedir:

- Durumsuz Adres Otomatik Konfigürasyonu (Stateless address autoconfiguration - SLAAC)  
Otomatik olarak gerçekleşen yapılandırmada cihaz IPv6 ön ek bilgisini yönlendiriciden almakta, geri kalan host bilgisini kendisi üretmektedir.
- Duruma Bağlı Adres Otomatik Konfigürasyonu (Statefull Adress Autoconfiguration)  
DHCPv6 ile gerçekleştirilmektedir.
- Manuel

### 1.6.1 Duruma Bağlı Adres Otomatik Konfigürasyonu (DHCPv6)

- Yönlendirici Mbit olarak düğüme “1” döner ise düğüm DHCPv6’dan IP alması gerektiğini anlamaktadır.



### 1.7 Adres Çakışması Tespiti (Duplicate Address Detection - DAD)

Cihazın kendi link-local adresini üretmeden önce ortamda aynı IP adresi olup olmadığını kontrol etmesine DAD adı verilmektedir.

- Düğüm kendi MAC adresindeki son 24 biti alarak oluşan link local adresi ile kendisine ait olması gereken *solicited-node* çoklu gönderim adresine istek göndererek ortamda aynı IP adresi olup olmadığının tespitini sağlamaktadır.

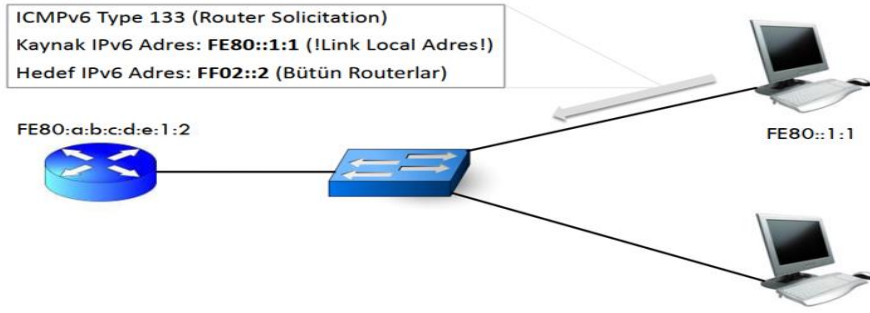
### 1.8 Düğümün DNS Sunucusunu Öğrenmesi

Other bit “0” ise yönlendirici, istemciye DNS vb. diğer bilgileri manuel girmesi gerektiğini belirtir.

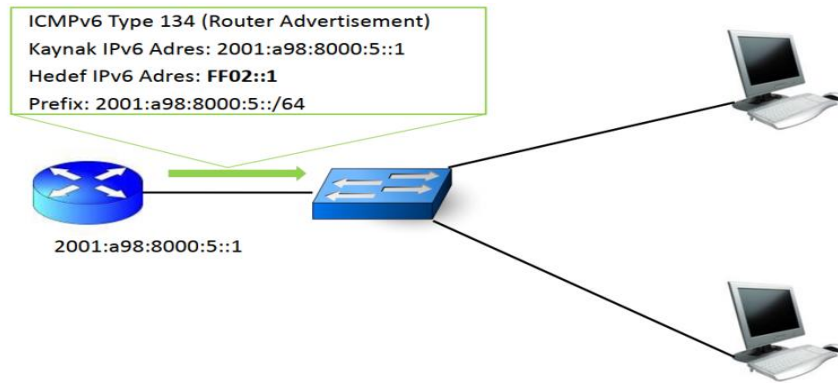
Other bit “1” ise yönlendirici, istemciye DNS ve diğer parametreleri DHCP den öğrenmesi gerektiğini belirtir.

#### 1.8.1 Durumsuz Adres Otomatik Konfigürasyonu (SLAAC)

- SLAAC’de istemci kendi yerel bağlantı adresini kullanarak FF02::2 çoklu gönderim adresine talep (*solicitation*) paketi göndermektedir. FF02::2 adresine gönderilen çoklu gönderim paketi ilgili ağda yer alan tüm yönlendiricilere gitmektedir.



- Yönlendirici kendisine gelen isteğe karşılık olarak *router solicitation* (RS) paketi gönderir. RS paketinin içinde ilgili ağa ait ön ek adresi ve/veya istemciye IP bilgisini *stateless* olarak oluşturması gerektiğini ya da DHCP'den IP alması gerektiğini belirten bilgi bulunmaktadır.



- Ayrıca bu aşamada istemci, yönlendiricinin adresini öğrenmektedir.

Yönlendirici istemciyi bilgilendirmek için RS mesajı içerisinde “managed” ve “other” bitlerini kullanmaktadır.

M bit “0” ise yönlendirici ön eki verir ve istemciden IP’sini kendisinin hesaplamasını bildirir.

M bit “1” ise yönlendirici istemciye IP bilgisini DHCP’den alması gerektiğini belirtir.

Yönlendirici M bit olarak istemciye “0” dönerse, istemci IP’sini kendisi otomatik olarak aşağıda yer alan örnekteki gibi hesaplamaktadır.

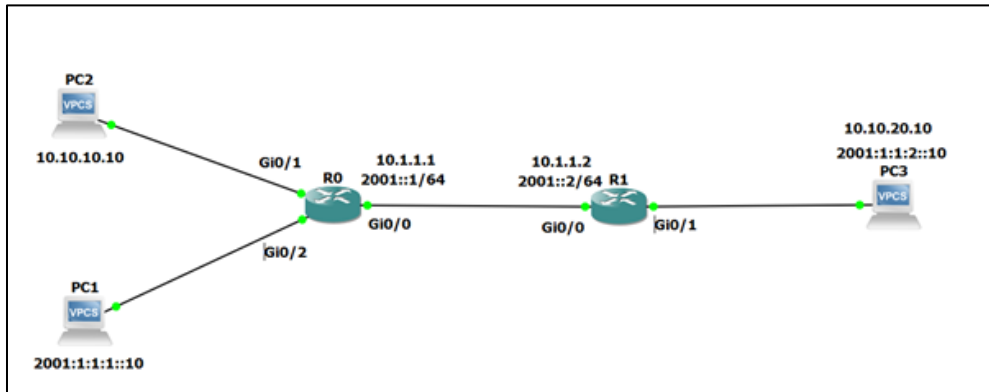
Örneğin PC’nin MAC adresi 02:90:27:17:FC:0F olsun. PC /64 ön ek bilgisini aldıktan sonra geri kalan 64 bit için EUI -64 işlemi başlamaktadır:

02:90:27:FF:FE:17:FC:0F

İstemci IP adresi:

2001:A98:8000:5:0290:27FF:FE17:FC0F/64

## 2. Yönlendiricide IPv6 İkili Yığın Konfigürasyonu



Verilen örnekte tüm olası senaryoların görülebilmesi için PC1 node u IPv6 PC2 node u IPv4 PC3 nodu ise ikili yığın (dualstack / hem IPv4 hem IPv6 ) olarak ayarlanmıştır.

Aşağıdaki konfigürasyon örneğinde görüldüğü gibi ikili yığın konfigürasyonu için yönlendiriciler üzerinde yapılması gereken konfigürasyon arayüze hem IPv4 hem de IPv6 adresini atamaktır.

### ROUTER 0 CONFİG

```
!
interface GigabitEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 ipv6 address 2001::1/64
 no cdp enable
!
interface GigabitEthernet0/1
 ip address 10.10.10.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 media-type rj45
 ipv6 address 2001:1:1:1::1/64
 no cdp enable
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
ipv6 route ::/0 2001::2
!
!
!
control-plane
!
banner exec ^C
```

## ROUTER 1 CONFİG

```
!
interface GigabitEthernet0/0
 ip address 10.1.1.2 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 ipv6 address 2001::2/64
 no cdp enable
!
interface GigabitEthernet0/1
 ip address 10.10.20.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 ipv6 address 2001:1:1:2::1/64
 no cdp enable
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
ipv6 route ::/0 2001::1
!
!
!
control-plane
!
```

SLAAC ile düğümlerin otomatik olarak adres alması için *router advertisement* (RA) fonksiyonu yönlendirici üzerinde aktif edilmelidir. Birçok yönlendirici ve firewall üzerinde bu işlem ayrıca bir komut ile yapılır. Fakat Cisco da Router(config)#ipv6 unicast-routing komutu ile IPv6 yönlendirme aktif edildiğinde RA fonksiyonu tüm portlarda otomatik olarak aktif olur.

### 3. IPv6'ya Geçişte Ethernet Switchler Üzerinde Yapılması Gerekenler

IPv6 protokolü *broadcast* yerine *multicast* kullanmak üzere dizayn edilmiştir. Ethernet switchlerin multicast paketleri tanıyabilmesi için *MLD snooping* fonksiyonlarının aktif edilmiş olması gerekir. Eğer MLD snooping fonksiyonu aktif edilmemiş ise Ethernet switch üzerinden akan tüm multicast trafik broadcast edilecektir. Bu durum kurum ağı üzerinde pasif dinleme ile bilgi toplamak isteyen saldırganlara daha çok bilginin gönderilmesi anlamına gelmektedir.

MLD, IPv6 çoklu gönderim(*multicast*) yönlendiricileri tarafından, doğrudan bağlı bağlantılarında çoklu gönderim dinleyicilerinin varlığını keşfetmek ve hangi çoklu gönderim paketlerinin hangi komşu düğümler ile ilgilendiğini keşfetmek için kullanılan bir protokoldür.

MLD, IGMP'den türetilmiştir; MLD sürüm 1 (MLDv1), IGMPv2'ye ve MLD sürüm 2 (MLDv2), IGMPv3'e eşdeğerdir. MLD, Internet Denetim İletisi Protokolü sürüm 6'nın (ICMPv6) bir alt protokolüdür ve MLD iletileri, IPv6 paketlerinde, başlık değeri 58 ile tanımlanan ICMPv6 iletilerinin alt kümesidir.

Ethernet switch'ler hem MLDv1 hem de MLDv2 protokol paketlerini izleyebilir ve hedef IPv6 multicast MAC adreslerine dayalı olarak IPv6 multicast verilerini anahtarlar. Ethernet switch'ler aynı anda MLD gözetleme ve IGMP gözetleme yapmak üzere yapılandırılabilir.

Cisco switchler için MLD protokolü aşağıdaki gibi aktif edilmektedir.

```
Switch(config)# ipv6 mld snooping
```

Global olarak MLD aktif edildikten sonra mevcut vlanlar için ayrıca MLD aktif edilmelidir. İstenen vlanlar da aşağıdaki gibi MLD aktif edilebilir.

```
Switch(config)# ipv6 mld snooping vlan 100
```

veya

```
Switch(config)# ipv6 mld snooping vlan all
```

Komutu ile tüm mevcut vlanlar için MLD yi aktif edilebilir.

#### 4. IPv6'da Sorun Giderme

Birçok açıdan IPv6 da sorun giderme işlemi IPv4'tekine benzer şekilde gerçekleştirilmektedir.

- Ping komutu aşağıdaki gibi karşı tarafa paketlerinizin gidip gelmesinde bir problem olup olmadığının testi için kullanılır.

```
C:\Users>ping 2A03:23EE:110:3E7::1
```

- Yine aynı şekilde tracert komutu aşağıdaki şekilde karşı tarafa giden iletişim hattı üzerinde hangi router, firewall gibi L3 cihazların olduğunun tespiti için kullanılır.

```
C:\Users>tracert 2A03:23EE:110:3E7::1
```

- IPv6 de arp protokolü yoktur. Bu yüzden #arp -a komutu kullanılamaz. Bunun yerine show IPv6 neighbor benzeri bir komut ile sizin ile aynı network üzerinde bulunan IP adresleri ve bunlara ait MAC adresleri görülebilir.

Bu komut Windows makineler için *#netsh interface ipv6 show neighbor* şeklindedir.

```
C:\Windows\system32> netsh interface ipv6 show neighbor
```

Interface 14: Wireless Network Connection

| Internet Address          | Physical Address  | Type               |
|---------------------------|-------------------|--------------------|
| fe80::9c5a:e957:a865:bde9 | 00-0c-29-36-fd-f7 | Stale              |
| fe80::fa66:feff:fe31:7250 | f8-66-f2-31-72-50 | Reachable (Router) |
| ff02::1                   | 33-33-00-00-00-01 | Permanent          |
| ff02::2                   | 33-33-00-00-00-02 | Permanent          |
| ff02::c                   | 33-33-00-00-00-0c | Permanent          |
| ff02::16                  | 33-33-00-00-00-16 | Permanent          |
| ff02::1:2                 | 33-33-00-01-00-02 | Permanent          |
| ff02::1:3                 | 33-33-00-01-00-03 | Permanent          |
| ff02::1:ff20:4696         | 33-33-ff-20-46-96 | Permanent          |

- Düğüm üzerinde IPv6'nın aktif olup olmadığı IPv6 loopback adresine *ping* atılarak test edilebilir.

```
ping ::1
```

- Neighbor tablosu belirli aralıklar ile temizlenir bu nedenle neighbor tablosuna bakıldığında o andaki tüm IPv6 komşuları görülemeyebilir. Bu nedenle ff02::1 adresine ping atılarak vlan içerisindeki tüm komşulara ping paketi gönderilebilir. Ardından gelen cevap paketleri vasıtası ile neighbor tablosu yenilenebilir. Fakat eğer IPv6 düğümleri üzerinde firewall var ise ve bu firewall ping paketlerini engelliyor ise aslında var olan bir düğümden cevap alınamaz. Bu konuya dikkat edilmelidir.
- Aynı ağda bulunan tüm aktif IPv6 düğümleri öğrenmek için all node multicast adresine ping atılabilir.

*Ping ff02::1*