IPv6 EL KİTABI

V2.1 Nisan 2012

[IPv6 El Kitabı, Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi kapsamında hazırlanmış olup, IPv6'ya geçiş aşamasında IPv6 protokolü, geçiş yöntemleri ve yapılandırması konularında ihtiyaç duyulabilecek temel bilgileri barındırmaktadır.]

HAZIRLAYANLAR

Alfabetik Sıra İle

BEYHAN KAAN ÇALIŞKAN – TÜBİTAK ULAKBİM

EMRE YÜCE – TÜBİTAK ULAKBİM

GÖKHAN ERYOL – TÜBİTAK ULAKBİM

İLKNUR GÜRCAN – TÜBİTAK ULAKBİM

MURAT SOYSAL – TÜBİTAK ULAKBİM

NEŞE KAPTAN KOÇ – TÜBİTAK ULAKBİM

ONUR BEKTAŞ – TÜBİTAK ULAKBİM

İÇİNDEKİLER

BÖLÜM 1: IPV6 TEMELLERİ VE YAPILANDIRMASI

IPv6 Nedir?

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. IPv4 adres aralığının büyük bir kısmı şu anda kullanılmakta olup, kalan adreslerin de kısa süre içinde tükenmesi beklenmektedir. IPv4 adres aralığı 256 tane /8 büyüklüğünde birincil tahsis aralığına bölünmüştür. Dünyadaki IP adreslerinin dağıtım koordinasyonu ile görevli merci olan Internet Assigned Numbers Authority (IANA), 3 Şubat 2011 tarihinde elinde kalan son 5 adet birincil tahsis aralığını Avrupa, Kuzey Amerika, Latin Amerika, Afrika ve Asya'daki bölgesel IP adresi dağıtım yetkililerine (Regional Internet Registries) paylaştırmıştır. 2011 yılının Eylül ayına kadar en az bir bölgesel dağıtım yetkilisinin elindeki IPv4 adreslerinin tükenmesi beklenmektedir.

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. Böylece gelecekte herhangi bir adres sıkıntısı yaşanmasını önleyebilecek kadar büyük bir adres aralığı sağlanmaktadır.

IPv4'ün Eksiklikleri

IPv4 ile ilgili yayınlanan RFC 791 dokümanı 1981 yılında yayınlanmış ve günümüze kadar pek fazla değişmemiştir. Kolay uygulanabilmesi ve başka protokollerle birlikte çalışabilmesi, IPv4'ü popüler kılmış ve İnternet'in yaygınlaşmasında büyük rol oynamıştır. IPv4 tasarlanırken günümüzde ortaya çıkan bazı ihtiyaçlar öngörülemediği için, bugün IPv4 kullanımı bazı kısıtlamalar getirmektedir. IPv4'ün özellikle yetersiz kaldığı alanlar şunlardır:

- 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.
- Son yıllarda İnternet ortamında verinin gizliliğinin ve bütünlüğünün korunabilmesi için IP seviyesinde güvenlik gereksinimi artmıştır. 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 adres yapılandırması statik olarak veya Dinamik İstemci Kontrol Protokolü (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

IPv6'da IPv4'ün güçlü yönleri korunarak, günümüz ağlarının değişen gereksinimlerini karşılamak amacıyla pek çok yenilik getirilmiştir. İnternet ağının her geçen gün daha çok kullanıcıyı kapsamasıyla, yönlendirici trafiği ve yönlendirilecek paket sayısı artmıştır. Bu nedenle günümüzde veri işleme hızı önem kazanmıştır. Bir başka deyişle yönlendirmenin veya anahtarlamanın yapıldığı noktalarda veri paketlerinin doğru ve hızlı bir şekilde yönlendirilmesi büyük önem taşımaktadır. İnternet kullanımının yaygınlaşması ve servis çeşitliliğinin artması ile birlikte IPv4'te yaşanan sorunları gidermeyi amaçlayan IPv6'nın yeni özellikleri aşağıda kısaca açıklanmıştır.

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. Şu anda IPv6 adres aralığının çok küçük bir yüzdesi için kullanım alanı tanımlanarak tahsis edilmek üzere ayrılmıştır. Bu sayede gelecekteki kullanım için yeterince adres mevcuttur. Geniş adres aralığının sunduğu bir diğer avantaj ise uçtan uca adresleme yapılabilmesidir. NAT gibi kullanımı durumunda pek çok işletim zorluğunu beraberinde getiren adres dönüştürücü mekanizmalara olan ihtiyaç, IPv6 kullanımı ile ortadan kalkmaktadır.

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. IPv6'nın güvenlik

konusundaki bir diğer üstünlüğü, güvenlik için tanımlanmış ek başlıklar ile yetkilendirme ve şifreleme yapılabilmesidir. 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.

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. IPv6 paketlerinin başlık yapısı ilerideki bölümlerde ayrıntılı olarak işlenmektedir.

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. Bu problemlerin üstesinden gelmek için IPv4'te farklı Servis Kalitesi (QoS) teknikleri kullanılmaktadır. IPv6 başlığında bulunan yeni alanlar trafiğin daha iyi tanımlanması ve buna göre önceliklendirilmesine olanak sağlar. Bu önceliklendirme paket başlığındaki bilgilere göre yapıldığı için, paketin içeriğinin şifrelenmiş olması önceliklendirmeyi etkilememektedir.

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.

Dolaşılabilirlik:

Dolaşılabilirlik, bir istemcinin farklı ağlardan "gerçek ev adresi" ile bağlantı yapabilmesidir. IPv4'te dolaşılabilirlik desteği sorunlu olmakla birlikte mevcuttur. IPv6'da ise sorunsuz çalışmaktadır.

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 kullanılır. Bu mesajlar IPv4'te bulunan "Address Resolution Protocol" (ARP), "ICMPv4 Router Discovery" ve "ICMPv4 Redirect" mesajlarının yerini alır. ICMPv6 ayrıca yönlendirme ve IP paketlerinin dağıtımı esnasında ortaya çıkan hataları ve diğer temel durumların raporlanmasında da kullanılır.

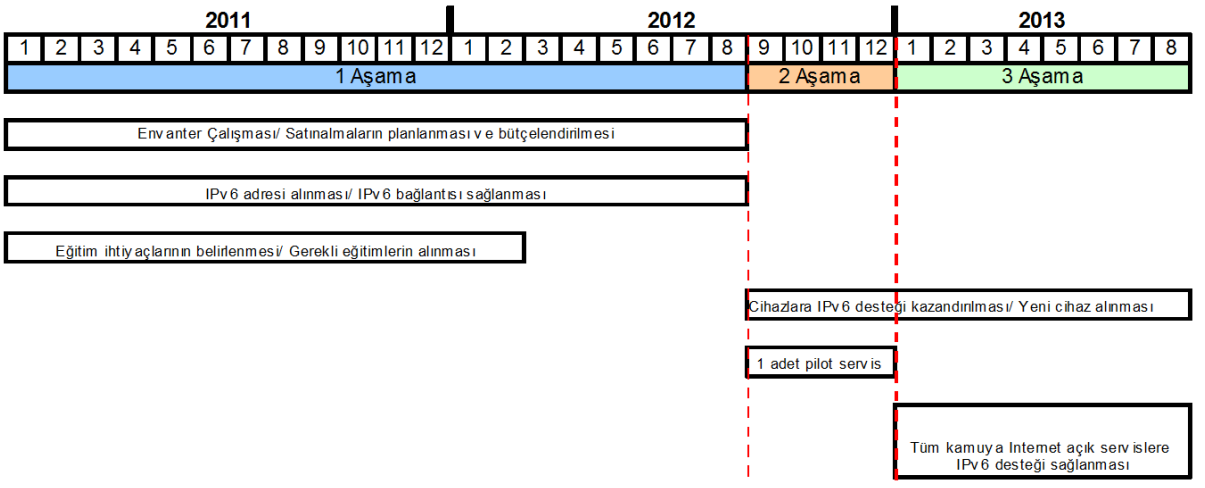
Türkiye'de IPv6 ile ilgili Yürütülen Çalışmalar

Türkiye'de IPv6 kullanımının yaygınlaştırılması ile ilgili çalışmalar Ulusal Akademik Ağ ULAKNET'in yönetiminden ve işletiminden sorumlu TÜBİTAK ULAKBİM tarafından sürdürülmektedir. Bu kapsamdaki çalışmalara 2003 yılı başında Avrupa bölgesel IP adresi dağıtım yetkilisi kurumdan 2001:a98::/32 IPv6 adres aralığının temin edilmesi ile başlamıştır. Mayıs 2003 tarihinde Avrupa Akademik Ağı üzerinden küresel IPv6 bağlantısı sağlanmış olup, ULAKBİM'in sunduğu DNS, FTP, SMTP gibi servisler IPv6 üzerinden erişilebilir duruma getirilmiştir. Bu gelişmelere paralel olarak IPv6 adres aralığı alan üniversite ve araştırma kurumlarının da ikili yığın yöntemi ile ULAK6NET olarak adlandırılan ULAKNET'in IPv6 omurgasına dâhil edilmesi sağlanmıştır.

Türkiye'de IPv6 bilgi birikimine katkı sağlamak amacıyla, 2007 yılında Bilgi Teknolojileri ve İletişim Kurumu (BTK) koordinasyonuyla "IPv6 Forum Türkiye" kurulmuş ve 2010 yılında küresel IPv6 forumuna üyelik gerçekleştirilmiştir. "IPv6 Forum Türkiye" bünyesinde, üniversitelerden, kamu kurumlarından ve servis sağlayıcılardan katılımcılar ile ekonomi, eğitim, yönetim ve teknik içerikli çalışma grupları oluşturulmuştur. 2008 Şubat ayında Türkiye'de IPv6 protokolü ile ilgili ARGE faaliyetlerinde bulunmak, bilgi birikimi oluşturmak ve Türkiye'nin IPv6 geçişini planlamak amacıyla "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" başlatılmıştır. 24 ay süren proje kapsamında farklı IPv6 geçiş yöntemleri analiz edilmiş, farklı tipteki organizasyonlar için en uygun geçiş yöntemini tespit edebilmek için bir karar destek sistemi tasarlanmış, geçiş adımları planlanarak karşılaşılması muhtemel yönetim ve güvenlik problemlerine yönelik çözüm önerileri geliştirilmiştir. Proje kapsamında tüm kamu ve İnternet Servis Sağlayıcı kurumlara IPv6 geçişi konusunda anket çalışması yapılmıştır. Ankette kurumlara teknik personel, IPv6 destekli ve desteksiz cihaz sayıları, IPv6 desteklemeyen cihazların değiştirilme maliyeti ve tahmini yenilenme zamanları konularında sorular yöneltilmiştir. Ayrıca proje kapsamında IPv6 özelliklerinin test edilmesi ve güvenlik açısından incelenmesi için bir IPv6 test yatağı (IPv6-GO) ve IPv6 bağlantısı olmayan İnternet Servis Sağlayıcı kurumların küresel IPv6 ağına bağlanabilmesi için IPv6 Trafik Değişim Noktası (IPv6-DN) kurulmuştur. Türkiye'den 30 İnternet Servis Sağlayıcı, bölgesel IPv6 tahsis kurumu RIPE'tan IPv6 adreslerini almışlardır. Şubat 2011 itibariyle sadece 5 İnternet Servis Sağlayıcının IPv6 adresleri, küresel IPv6 yönlendirme tablolarında yer almakta olup, 3 İnternet Servis Sağlayıcı küresel IPv6 ağına ULAKNET IPv6-DN üzerinden bağlıdır.

Proje kapsamında oluşturulan "Kamu Kurum ve Kuruluşları için IPv6'ya Geçiş Planı", 8 Aralık 2010 tarihli ve 27779 sayılı Resmi Gazete 'de yayınlanan Başbakanlık Genelgesi ile duyurulmuştur.

Söz konusu plan uyarınca kamu kurum ve kuruluşlarının IPv6'ya geçişinin, aşağıdaki takvim doğrultusunda gerçekleştirilmesi planlanmaktadır:



Şekil 1: Kamu Kurum ve Kuruluşları için IPv6'ya Geçiş Planı Aşamaları

1. Aşama (1 Ocak 2011 - 31 Ağustos 2012):
   1.1. Kamu kurum ve kuruluşları 31 Mart 2011 tarihine kadar aşağıda belirtilen unsurların IPv6 desteğinin olup olmadığı konusunda bir envanter çıkarma çalışması yapacaktır;
      - Üçüncü seviye anahtarlama cihazları,
      - Yönlendirici cihazlar,
      - Güvenlik cihazları,
      - İnternet üzerinden dışarıya verilen hizmetler ve bu hizmetlerin verilmesini sağlayan yazılımlar.

   1.2. İlgili yazılım veya donanımın faydalı kullanım ömürleri göz önünde bulundurularak IPv6 desteği bulunmayan unsurların yenilenmesi için plan yapılacak ve satın alınması öngörülen mal veya hizmetlerin finansmanı bütçe çalışmalarına dâhil edilecektir.
   1.3. Kamu kurum ve kuruluşları en geç 31 Ağustos 2012 tarihi itibariyle IPv6 adresi ve IPv6 bağlantılarını temin etmiş olacaklardır.
   1.4. 31 Ağustos 2012'den sonra IPv6'yı desteklemeyen hiçbir ağ donanım ve yazılımına yatırım yapılmayacaktır.
   1.5. Kamu kurum ve kuruluşları, bilgi işlem personelinin IPv6'ya geçiş ve IPv6 destekli hizmetlerin verilebilmesi konusunda eğitim ihtiyaçlarını belirleyeceklerdir. Gerekli eğitimler 1 Mart 2012 tarihine kadar tamamlanacaktır.
   1.6. Kamu kurum ve kuruluşları, eğitim ihtiyaçlarını ücret mukabilinde Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) bünyesinde oluşturulacak olan IPv6'ya Geçiş Eğitimi Merkezi'nden

karşılayabileceklerdir. Bu eğitimin içeriği ve programı ULAKBİM tarafından belirlenecek ve duyurulacaktır.

1.7. İlgili eğitimin IPv6'ya Geçiş Eğitimi Merkezi'nden alınmadığı hallerde, eğitim alınacak kuruluşun bilgisayar ağları eğitimi hususunda TS EN ISO/IEC 17024 veya ISO/IEC 17024 standardına göre akredite edilmiş, "personel belgelendirme kuruluşu" olması gerekmektedir.

2. Aşama (1 Eylül 2012 - 31 Aralık 2012):

2.1. IPv6 bağlantısı ve adresi temin eden kamu kurum ve kuruluşları 31 Aralık 2012 tarihine kadar İnternet üzerinden verdikleri en az bir adet hizmeti pilot uygulama olarak IPv6 destekli hale getireceklerdir.

3. Aşama (1 Ocak 2013 - 31 Ağustos 2013):

3.1. Kamu kurum ve kuruluşları en geç 31 Ağustos 2013 tarihine kadar İnternet üzerinden verdikleri kamuya açık tüm hizmetleri IPv6'yı destekler hale getireceklerdir.

IPv6 Adres Mimarisi

IPv4'de 32 bit olan adres uzunluğu daha büyük adres aralığı elde etmek için IPv6'da 128-bit olarak genişletilmiştir. 32 bit olan IPv4 adreslerinin gösterimi için ondalık düzen kullanılmaktadır, ancak 128 bit olan IPv6 adreslerinin gösterimi için onaltılık düzen tercih edilmiştir.

Aşağıda bir IPv6 adresi ikilik düzende gösterilmiştir:

```
00100000000000010000110110111000000000000000000000000000000000000000001010
10101000000000111111111111111000101000100111000101101O
```

128 bit olan bu IPv6 adresi öncelikle 16 bit uzunluğunda 8 gruba ayrılmıştır:

```
0010000000000001  0000110110111000  0000000000000000  0000000000000000
0000001010101010  0000000011111111  1111111000101000  1001110001011010
```

Her grup onaltılık sayı düzenine dönüştürülmüş ve IPv6 adresi ":" ile ayrılan 16 bitlik bloklar halinde yazılmıştır:

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

IPv6 adreslerinin aşağıda listelenen kurallar çerçevesinde kısaltılması mümkündür:

- 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
```

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

IPv6 adresleri yönlendirme yöntemlerine göre üç gruba ayrılmaktadır:

- **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 yönlenmiş 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 adresleri "biçim önek" (format prefix) olarak adlandırılan ilk bitlerine göre sınıflandırılmaktadır. Tablo 1'de farklı IPv6 adres tipleri için atanan adres aralıkları ile ilgili ayrıntılı bilgi verilmiştir. 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.

Tablo 1. Ataması Yapılan IPv6 Adres Aralıkları

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

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 Eşlemli 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. Ancak bu dokümanda yer alan adres dönüşümü örneğinde IPv4 adresi olarak 192.168.0.5 kullanılacaktır. Bu IPv4 adresinin 16'lık sistemde gösterimi C0A8:0005 şeklindedir. Dolayısıyla bu adres için IPv4 eşlemli IPv6 adresi ::ffff:C0A8:5 olur.

Küresel Tekil Gönderim Adresleri: 001 biçim önekine 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. Şekil 2'de küresel tekil adresler için bit dağılımı verilmiştir. "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 bu örnek için 16 bittir. Son bölüm olan "Arabirim Tanıtıcısı" ise genellikle 64 bitliktir.

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

Şekil 2: Küresel Tekil Gönderim Adres Yapısı

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. Bunun yanı sıra 2002::/16 aralığı "6to4 geçiş yöntemi" için ayrılmıştır.

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 (Şekil 3). 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

Şekil 3: Eşsiz Yerel Tekil Gönderim Adres Yapısı

Bağlantı Yerel Tekil Gönderim Adresleri: 1111 1110 10 biçim önekine 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

Şekil 4: Bağlantı Yerel Tekil Gönderim Adres Yapısı

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

Şekil 5: Çoklu Gönderim Adres Yapısı

11111111 olan ilk 8 bit sonrasında, adresin tipini belirleyen "Bayrak" ve "Kapsam" bitleri gelmektedir. Bu bitlerin anlamları şu şekildedir:

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.

Bazı ön tanımlı çoklu gönderim adresleri ise aşağıda verilmiştir:

- ff01::1 Tüm düğümler (arayüz-yerel)
- ff01::2 Tüm yönlendiriciler (arayüz-yerel)
- ff02::2 Tüm yönlendiriciler (bağlantı-yerel)
- ff05::2 Tüm yönlendiriciler (site-yerel)

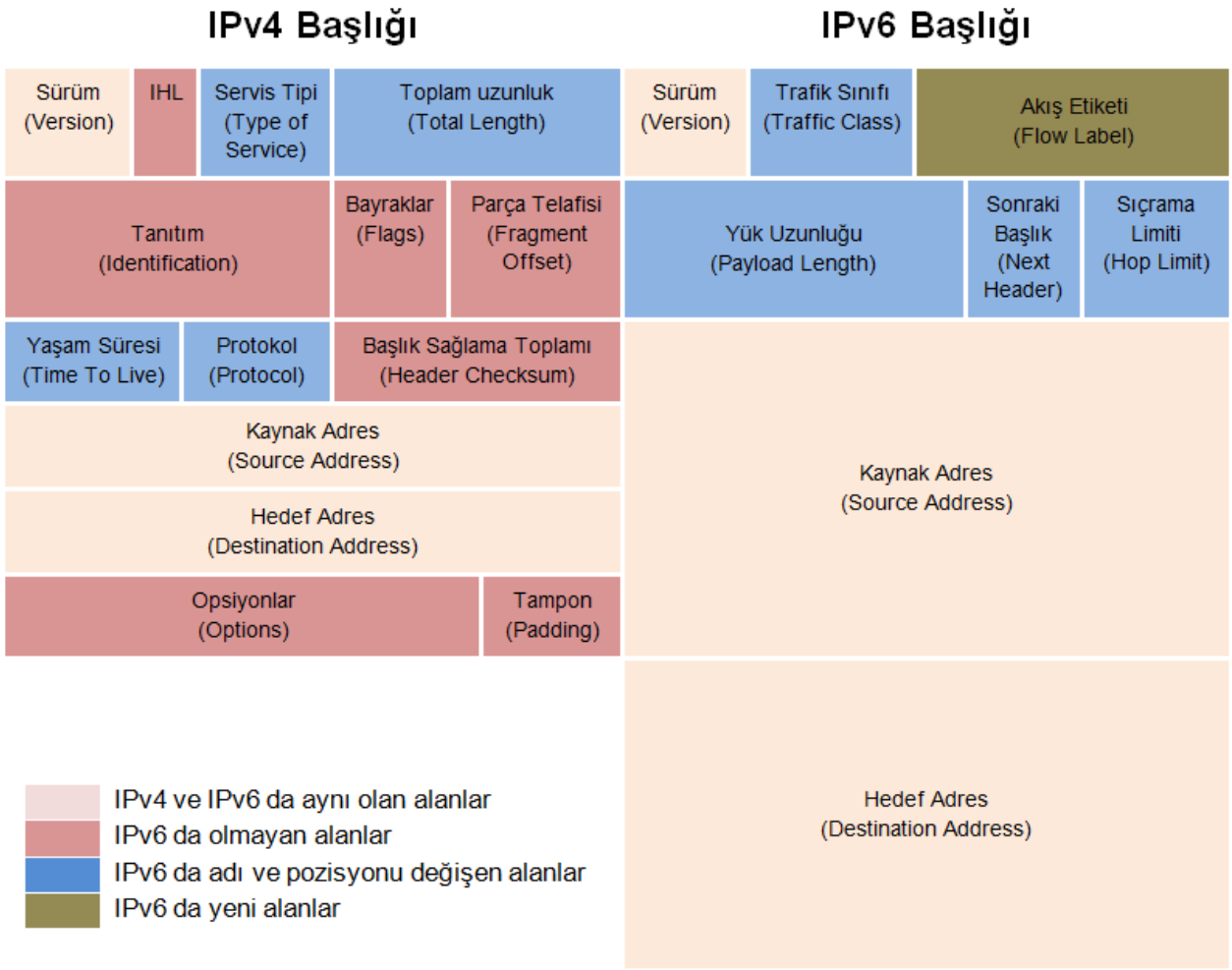
IPv6 Başlık Yapısı

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. Ayrıca 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. Bu yeni bölümün uzunluğu veya içerisinde yer alacak başlık sayısı ile ilgili bir kısıt bulunmamaktadır, böylece yeni başlıklar tanımlanarak IPv6'ya yeni özellikler kazandırılmasına da olanak sağlanmıştır.

Başlık yapıları incelendiğinde, IPv6 ve IPv4 arasındaki farklar daha açık bir şekilde ortaya çıkmaktadır (Şekil 6).

- 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'nın adres başlık yapısındaki en önemli değişiklerinden 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.



Şekil 6: IPv4 ve IPv6 Başlık Yapısı

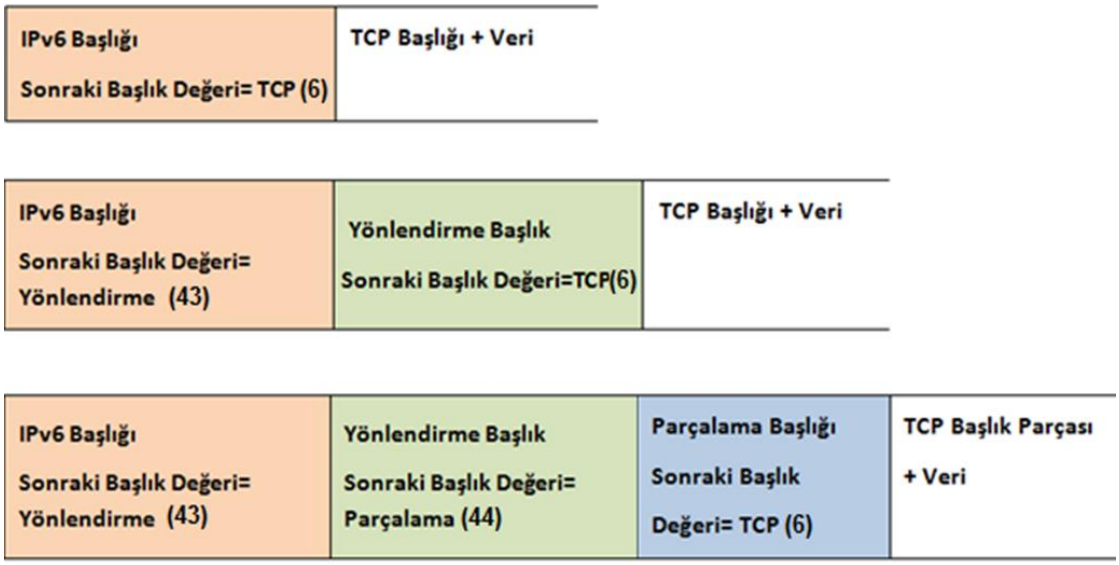
IPv6 Uzantı Başlıkları

IPv6 da paketleri ile ilgili tercihe bağlı bilgiler, temel başlık ile üst seviye protokol başlıkları arasında yer alan IPv6 uzantı başlıkları bölümünde yer almaktadır. Bu uzantı başlıkları temel başlık bilgisinden sonra ihtiyaç duyulduğunda kullanılır. Biri hariç uzantı başlıklarının hepsi sadece IPv6 paketi için hedef olarak belirlenen cihaz tarafından işlenmektedir. 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, yok ise üst protokol başlığı ile ilgili işlemlere devam eder (Şekil 7).

Uzantı başlıkları boyut açısından değişkenlik göstermektedirler. Eğer bir paket için birden fazla uzantı başlığı kullanılıyor ise bu başlıkların aşağıdaki sırada bulunması önerilmektedir.

- Sıçrama Seçenekleri Başlığı (Hop-by-Hop Options Header)[1]
- Hedef Seçenekleri Başlığı (Destination Options Header)[2]
- Yönlendirme Başlığı (Routing Header)
- Parçalama Başlığı (Fragment Header)
- Doğrulama Başlığı (Authentication header)[3]
- Kapsüllenmiş Güvenlik Yük Başlığı (Encapsulating Security Payload Header) [4]
- Hedef Seçenekleri Başlığı (Destination Options Header) [5]
- Dolaşılabilirlik Başlığı (Mobility Header)
- Üst Protokol Başlığı (Upper-layer Header)



Şekil 7: Uzantı Başlıkları

[1] Pakette yer alması durumunda "Sıçrama Seçenekleri" başlığının ilk sırada bulunması zorunludur.
[2] IPv6 hedef adresi bölümünde bulunan ilk hedef ile yönlendirme başlığındaki müteakip cihazlar tarafından işlenecek bilgi içermesi durumunda
[3] Bu başlıklar ile ilgili ek şartlar RFC-2406 belgesinde verilmiştir
[4] Bu başlıklar ile ilgili ek şartlar RFC-2406 belgesinde verilmiştir
[5] Sadece hedef cihaz tarafından işlenecek bilgiler içermesi durumunda

Tanımlı olan IPv6 uzantı başlıkları, tanımlı oldukları RFC belgeleri ve bu başlıkları tanımlayan sonraki başlık değerler Tablo 2'de verilmiştir. Tablo 3'te ise üst protokoller için kullanılan sonraki başlık değerleri bulunmaktadır.

Tablo 2. IPv6 Ek başlıkları

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

Tablo 3. Üst 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 kullanılmaktadır. 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. Ancak, IPv4 tabanlı iletişimde ICMP mesajlarının sınır yönlendiricilerinde engellenmesi sık rastlanan bir uygulamadır. Bunun temel nedeni ICMP'nin saldırganlar tarafından keşif aşamalarında kullanılmasıdır.

ICMPv6 de bu protokolün IPv6 için uyarlanmış halidir. ICMPv6 tüm IPv6 düğümlerinin iletişimleri için temel bir protokol olarak tasarlanmıştır ve RFC 2463 ile bu düğümlerin ICMPv6'yı eksiksiz desteklemesi zorunluluğu ortaya konmuştur. IPv6 paketinde üst protokolü tanımlayan sonraki başlık değeri 58 ise, bu paket bir ICMPv6 mesajı taşımaktadır. ICMPv6 bilgileri iki bölümde taşınmaktadır. İlk 32 bit başlık bölümünü oluşturmaktadır. Bu bölümün ilk 8 biti mesajın tipi ile ilgili bilgiyi taşır. Eğer yüksek sıralı bit 0 ise (0-127 arası değerler için) bu bir hata mesajıdır. Eğer yüksek sıralı 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 kullanılmaktadır. ICMPv6 paket yapısı Şekil 8'de verilmiştir.

	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)		

Şekil 8: ICMPv6 Paket Yapısı

Aşağıda yer alan Tablo 4 ve Tablo 5 de ICMPv6 hata ve bilgi mesajları tip ve kod değerleri ile birlikte ayrıntılı olarak yer almaktadır.

Tablo 4. RFC 4443 belgesinde tanımlanan ICMPv6 hata mesajları

Tip	Kod	Açıklama
1		Hedef Erişilemez (Destination Unreachable)
1	0	Hedefe yönlendirme bilgisi yok (no route to destination)
1	1	Hedef ile iletişim yönetimsel olarak engellenmiştir (communication with destination administratively prohibited)
1	2	Kaynak adresin kapsamı dışında (beyond scope of source address)
1	3	Adres erişilemez (address unreachable)
1	4	Port erişilemez (port unreachable)
1	5	Kaynak adres başarısız giriş-çıkış politikası (source address failed ingress/egress policy)
1	6	Hedef rotası reddedildi (reject route to destination)
1	7	Yönlendirme başlığında hata (Error in Source Routing Header)
2	0	Paket çok büyük (Packet Too Big)
3		Zaman aşımı (Time Exceeded)
3	0	Sekme limiti aşımı (hop limit exceeded in transit)
3	1	Parça birleştirme zaman aşımı (fragment reassembly time exceeded)
4		Parametre problemi (Parameter Problem)
4	0	Başlık alanında hata (erroneous header field encountered)
4	1	Tanımlanamayan sonraki başlık tipi (unrecognized Next Header type encountered)
4	2	Tanımlanamayan IPv6 opsiyonu (unrecognized IPv6 option encountered)

Tablo 5. ICMPv6 Bilgi Mesajları

Tip	Kod	Açıklama	RFC
128	0	Yankı İsteği (Echo Request)	4443
129	0	Yankı Cevabı (Echo Reply)	4443
130	0	Çoklu Gönderim Dinleyici Sorgusu (Multicast Listener Query)	2710
131	0	Çoklu Gönderim Dinleyici Raporu (Multicast Listener Report)	2710
132	0	Çoklu Gönderim Dinleyici Tamam Mesajı (Multicast Listener Done)	2710
133	0	Yönlendirici Talep Mesajı (Router Solicitation)	4861
134	0	Yönlendirici İlan Mesajı (Router Advertisement)	4861
135	0	Komşu Talep Mesajı (Neighbor Solicitation)	4861
136	0	Komşu İlan Mesajı (Neighbor Advertisement)	4861
137	0	Yeniden Yönlendirme Mesajı (Redirect Message)	4861
138		Yönlendiricileri Yeniden Numaralandırma (Router Renumbering)	Crawford
139		ICMP Düğüm Bilgisi Sorgusu (Query ICMP Node Information)	4620
140		ICMP Düğüm Bilgisi Cevabı (Response ICMP Node Information)	4620
141	0	Ters Komşu Keşfi Teklif Mesajı (Inverse Neighbor Discovery Solicitation Message)	3122
142	0	Ters Komşu Keşfi İlan Mesajı (Inverse Neighbor Discovery Advertisement Message)	3122
143	0	Sürüm 2 Çoklu Gönderim Dinleyici Raporu (Version 2 Multicast Listener Report)	3810
144	0	Ev Ajanı Adres Keşif -Talep Mesajı (Home Agent Address Discovery Request Message)	3375
145	0	Ev Ajanı Adres Keşif -Cevap Mesajı (Home Agent Address Discovery -Reply Message)	3375
146	0	Mobil Önek Talep Mesajı (Mobile Prefix Solicitation)	3375
147	0	Mobil Önek İlan Mesajı (Mobile Prefix Advertisement)	3375

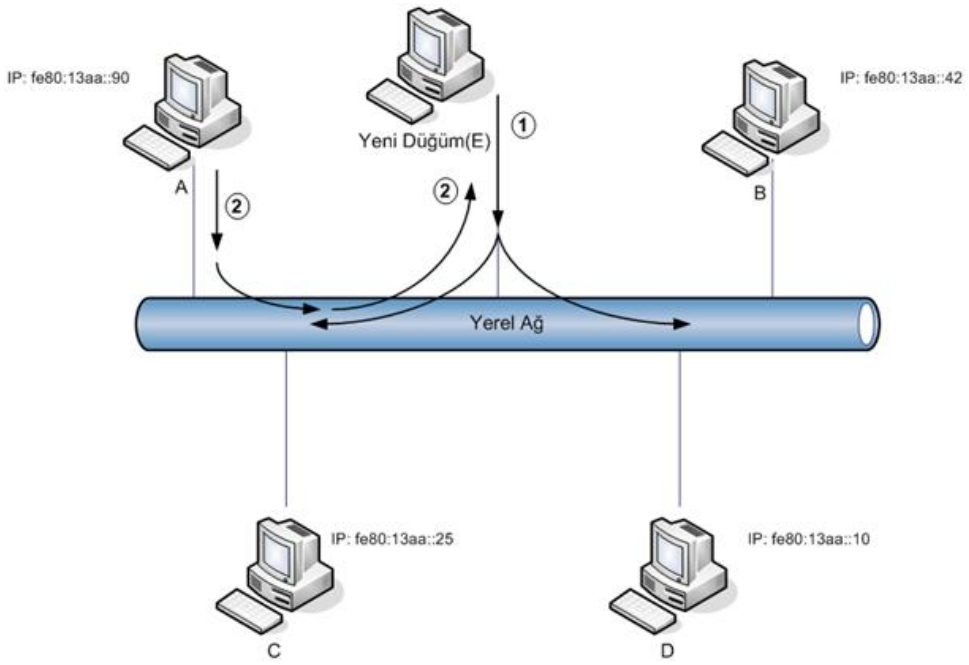
Komşu Keşfi (Neighbor Discovery)

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 yapılmaktadır. IPv6'da düğümler aynı ağda bulundukları komşularıyla Komşu Keşfi Protokolü ile sürekli iletişim halinde bulunurlar. Düğümler, ağdaki diğer düğümlerin bağlantı yerel adreslerinin öğrenilmesi, komşuların erişilebilirlik durumların tespit edilmesi, ağ üzerindeki yönlendiricileri sorgulamak ve yönlendiricilerden ağ yapılandırma bilgilerini elde etmek amaçlarıyla Komşu Keşfi Mesajlarını kullanırlar. Tanımlanmış 5 farklı komşu keşfi mesajı bulunmaktadır. Bu mesajlar ve görevleri aşağıda kısaca açıklanmıştır.

- ***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. Bu mesaj ağ öneki, MTU büyüklüğü, düğüm tarafından adres oluşturulurken hangi otomatik yapılandırma yönteminin kullanılabileceği, varsayılan ağ geçidi ve geçerlilik süresi gibi bilgiler içermektedir.
- ***Komşu Talep Mesajı (Neighbor Solicitation - RS):*** 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.

Şekil 9'da Komşu Keşfi protokolünün kullanımı konusunda bir örnek verilmiştir. Aynı yerel ağa bağlı A, B, C, D düğümleri ve bunların IP adresleri görülebilmektedir. 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 çoklu gönderim adresine komşu talep mesajı gönderir (1). Talep mesajını alan düğümler eğer bu adresi kullanıyorlarsa bir ilan mesajıyla cevap verirler. Şekil 9'da A

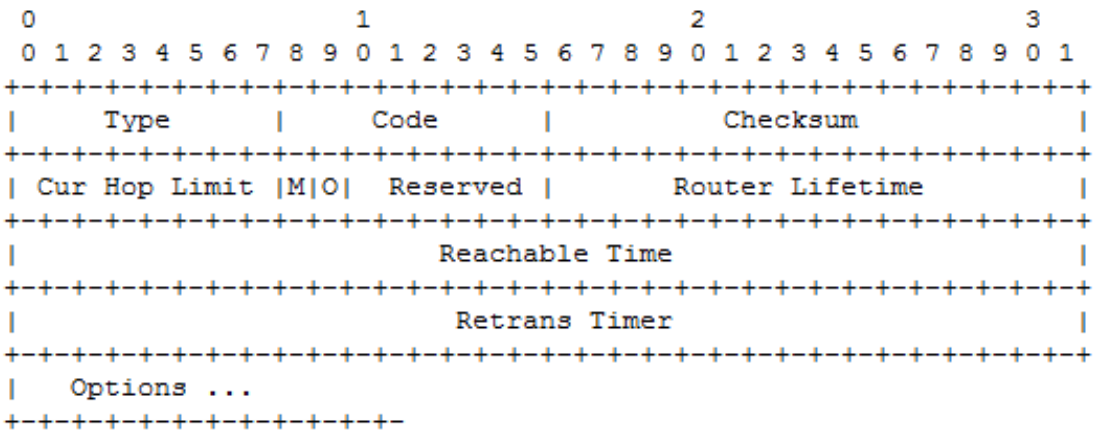
düğümü fe80:13aa::90 adresini kullandığı için tüm düğümlere bir ilan mesajı gönderir (2). İlan mesajını alan E, adres kullanıldığı için bu adresi kendi arayüzüne atayamaz. Bu durumda ya düğüme sistem yöneticisi tarafından bir adres verilir veya alternatif bir arayüz tanımlayıcısıyla yeni bir adres oluşturulup süreç tekrar başlatılır. Eğer talebe belirli bir süre cevap gelmez ise, E düğümü oluşturduğu adresi kullanmaya başlar.



Şekil 9: Komşu Keşfi Örneği

Temel 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, Dinamik İstemci Kontrol Protokolü sürüm 6 (DHCPv6) kullanılarak yapılabilir. Otomatik adres tanımlamanın yanı sıra, istemcilere statik olarak IPv6 adreslerinin tanımlanması da mümkündür.



Şekil 10: Yönlendirici İlan Mesajı

Otomatik adres yapılandırma için önemli görev üstlenen Yönlendirici İlan Mesajının yapısı Şekil 10'da verilmiştir. Mesaj içerisinde 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 bitleri sıfır ve bir olmak üzere iki farklı değer alabilirler. Bu değerlere göre istemcilere aktarılan bilgi aşağıda verilmiştir. Her iki bit için varsayılan değerler sıfırdır.

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)[6]

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)[7]

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.

[6] *Bu durum için durum denetimsiz DHCPv6 ifadesi de kullanılabilir.*

[7] *Bu durum kullanılmamaktadır. M bitinin değeri 1 ise O bitinin değerinin de 1 olması beklenmektedir.*

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 bir olup, ağ önek bilgisinin adres yapılandırması için kullanılabileceğini gösterir. Bayrak değeri sıfır ise, istemciler ilgili “Yönlendirici İlan Mesajı"ndaki ağ önek bilgisini bu işlem için kullanmaz. Özellikle durum denetimli adres yapılandırma yöntemi kullanılan ağlarda, yönlendirci ilan mesajlarındaki bu bayrağın değeri sıfır olarak tanımlanmalıdır. Aksi takdirde istemciler hem durum denetimli hem de durum denetimsiz otomatik adres yapılandırma yöntemlerinin kullanarak iki farklı küresel IPv6 adresi alırlar.

Durum Denetimsiz Otomatik Adres Yapılandırması

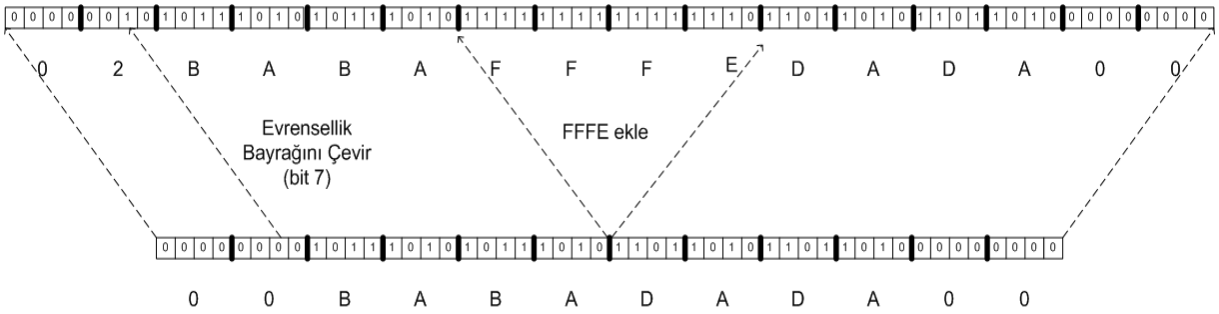
Durum denetimsiz otomatik adres yapılandırması ”RFC 2462: IPv6 Stateless Address Auto configuration” ile tanımlanmıştır. Bu yöntemde ağa bağlanan düğümlerin kullandıkları IPv6 adresleri bir sunucu veya otorite tarafından belirlenmez ve kayıt altına alınmaz. Durum Denetimsiz Otomatik Adres yapılandırmasında istemci ile yönlendirici arasındaki iletişim aşağıdaki gibi gerçekleşir:

- İstemci kendi bağlantı yerel adresini kullanarak yönlendirici talep mesajını ağdaki bütün yönlendiricileri temsil eden çoklu 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 Küresel IPv6 adresini oluşturur (Şekil 11).

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

- **Şekil 11: Küresel Tekil Adres Yapısı**

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. Şekil 12’da MAC adresinden ağ arabirim tanıtıısının oluşturulması anlatılmaktadır.



Şekil 12: MAC Adresinden Arabirim Tanıtıcısı Oluşturulması

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 Adres Yapılandırması:

Durum denetimli otomatik adres yapılandırmasında, 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, Dinamik İstemci Kontrol Protokolü sürüm 6 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, çoklu gönderim 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 çoklu gönderim adresleri kullanılarak uygulanır. Kullanılan çoklu gönderim adresleri:

- Tüm DHCP sunucuların ve nakledici ajanların 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.

dhcp6s DHCP Sunucusu

IPv6 ağlarında DHCP sunucu olarak dhcp6s yazılımı yaygın olarak kullanılmaktadır. Ayrıca, Linux ve BSD sunucular üzerinde DHCP Sunucu olarak kullanılmakta olan ISC DHCP uygulaması, IPv4'ün yanı sıra 4.1.0 sürümünden itibaren IPv6 DHCP sunucu özelliğini desteklemektedir.

dhcp6s yapılandırma dosyası, /etc/dhcp6s.conf dosyasıdır. 2001:db8:1:2::/64 öneki için örnek yapılandırma dosyası, aşağıdaki gibidir:

```
interface eth0 {
      server-preference 255;
      renew-time 60;
      rebind-time 90;
      prefer-life-time 130;
      valid-life-time 200;
      allow rapid-commit;
      option dns_servers 2001:db8:1:2::1 ipv6.ulakbim.gov.tr;
      link AAA {
            range 2001:db8:1:2::1000 to 2001:db8:1:2::ffff/64;
            prefix 2001:db8:1:2::/64;
      };
};
```

ISC dhcp sunucusu örnek yapılandırması

```
default-lease-time 600;
max-lease-time 7200;
log-facility local7;
 subnet6 2001:a98:1f:f3::/64 {
       range6 2001:a98:1f:f3::100 2001:a98:1f:f3::120;
       option dhcp6.name-servers 2001:a98:10::251;
       option dhcp6.domain-search "ulakbim.gov.tr";
 # İstemciye  sabit IPv6 adresi verilmesi icin örnek yapılandırma
#
#      host ipv6sabit{
#    host-identifier option dhcp6.client-id 00:01:00:01:14:dc:f7:33:08:00:27:fd:0f:14;
#       fixed-address6 2001:a98:1f:f3::701;
#  }
}
```

Cisco Yönlendirici Otomatik Adres Yapılandırma Örnekleri:

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

M biti varsayılan değer 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
```

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
```

DHCPv6 Stateless Temel Yapılandırma

```
ipv6 dhcp pool IPv6DNS
dns-server 2001:DB8:A:B::1
dns-server 2001:DB8:3000:3000::42
domain-name ulakbim.gov.tr
!
interface Ethernet0/0
 İpv6 enable
 ipv6 address 2001:DB8:1:2::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp server IPv6DNS
```

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 abc.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
```

BSD ve Linux Yönlendiricileri Otomatik Adres Yapılandırma Örnekleri

Yönlendirici İlanı için Temel Yapılandırma

Linux ve BSD yönlendiricileri üzerinde, yönlendirici ilanı için kullanılan radvd ve rtadvd yapılandırmaları 2001:db8:1:2::/64 öneki için aşağıdaki gibidir:

rtadvd örnek yapılandırma

```
default:\
        :chlim#64:raflags#0:rltime#1800:rtime#0:retrans#0:\
        :pinfoflags="la":vltime#2592000:pltime#604800:mtu#0:
ef0:\
         :addr="2001:db8:1f:3:prefixlen#64:tc=default:
```

radvd örnek yapılandırma

```
interface eth0 {
    AdvSendAdvert on;
    MinRtrAdvInterval 180;
    MaxRtrAdvInterval 600;
    prefix 2001:db8:1:2::/64 {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```

DHCPv6 Stateless Temel Yapılandırma

rtadvd örnek yapılandırma

```
default:\
 :chlim#64:raflags="o":rltime#0:rtime#0:retrans#0:\
        :pinfoflags="la":vltime#2592000:pltime#604800:mtu#0:
ef0:\
         :addr="2001:db8:1f:3:prefixlen#64:tc=default:
```

DHCPv6 Statefull Temel Yapılandırma

radvd örnek yapılandırma

```
interface eth0
{
    AdvSendAdvert on;
    AdvManagedFlag on;
    AdvOtherConfigFlag on;
```

```
   MinRtrAdvInterval 180;
   MaxRtrAdvInterval 600;
   prefix 2001:db8:1:2::/64
   {
      AdvOnLink on;
      AdvAutonomous off;
      AdvRouterAddr on;
   };
};
```

Statik Adres Yapılandırma Örnekleri

Farklı işletim sistemleri için IPv6 adresinin statik olarak nasıl tanımlanacağı aşağıda verilmiştir.

Cisco IOS

```
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
```

Windows XP

Windows XP işletim sisteminde grafik arayüzü kullanılarak IPv6 adresi ataması yapılamamaktadır. Destek verilebilmesi için grafik arayüz ile ağ bağlantısı özellikleri altından veya komut satırından girilebilecek "netsh interface ipv6 install" komutu ile IPv6 desteği yüklenmeli, ardından komut satırı kullanılarak IPv6 adres ve varsayılan ağ geçidi atama işlemi gerçekleştirilmelidir. Örnekte yer alan *Local Area Connection* parametresi *netsh interface ipv6 show interface* komutunun çıktısından elde edilebilir. Bu parametre yerine aynı komutun çıktısı olan *Arayüz Numarası* da kullanılabilir.

```
netsh interface ipv6 install
netsh interface ipv6 set address "Local Area Connection" 2001:db8:2:1::1
```

Windows 7 / Vista

Windows XP ’den farklı olarak, Windows 7 / Vista işletim sistemlerinde IPv6 desteği kurulumda otomatik olarak gelmektedir. IPv6 ayarları grafik arayüz veya komut satırı kullanılarak yapılabilmektedir. Komut satırı kullanılması durumunda kullanılacak komutlar aşağıda verilmiştir. Örnekte yer alan *Local Area Connection* parametresi *netsh interface ipv6 show interface* komutunun çıktısından elde edilebilir. Bu parametre yerine aynı komutun çıktısı olan *Arayüz Numarası* da kullanılabilir.

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

DNS İstemci Yapılandırması

DNS sunucunun istemciler tarafından kullanılabilmesi için, istemci işletim sistemi üzerinde DNS yapılandırılması gerekmektedir. IPv4’te de kullanılan, statik tanımlama ve DHCP sunucusu ile tanımlama yöntemlerinin yanı sıra, IPv6’da DNS sunucusu tanımlamak için iki yeni yöntem daha bulunmaktadır: Herhangi Birine Gönderim (Anycast) DNS Sunucu Kullanımı ve Yönlendirici İlanları (Router Advertisement).

Statik tanımlama, ağ üzerindeki her istemciye DNS sunucusunun adresini girmeyi gerektirir. Bu durumda ilk yapılandırma süresi uzamakta ve kullanıcı hataları oluşabilmektedir. DHCPv6 kullanımı IPv6 adresi dağıtımının yanı sıra, ağ üzerinde hizmet veren DNS, NTP, SIP gibi sunucuların istemcilere tanıtılmasını sağlar.

Herhangi birine gönderim DNS sunucu kullanımı, DNS sunucuların herhangi birine gönderim adreslerini kullanarak, dış ağlara açılmadan, iç ağda DNS sunucusunu istemcilere tanıtmak için kullanılır. Windows işletim sistemlerinin varsayılan ayarları, DNS sorgularını herhangi birine gönderim adreslerine yapmak şeklinde olup, Linux/Unix işletim sistemlerinde DNS sorgusu için herhangi birine gönderim adreslerinin kullanımının tanımlanması gerekebilir. IPv6 adreslerinin de yönlendirici önek ilanı ile dağıtıldığı ağlarda, istemciler açısından en kolay yöntem herhangi birine gönderim DNS sunucu kullanımıdır.

Yönlendirici İlanları ile DNS sunucularını ağa ilan etmek, RFC 5006 ile tanımlanmış olup, bu belgenin hazırlandığı tarihte halen deneysel aşamadadır. İlanların yapılması mümkün olsa da, istemci işletim sisteminde gerekli değişikliklerin yapılabilmesi için mekanizmalar standartlaştırılarak uygulamaya geçirilmemiştir.

Yönlendirme Protokolleri

Yönlendirme, farklı ağ bölümleri arasında paketlerin iletilmesi işlemlerinin bütünüdür. Yönlendirme işlemi, yönlendirici cihazlar tarafından yapılır. Yönlendiriciler, farklı ağlara ait yönlendirme bilgilerini yönlendirme tablolarında tutar, kendilerine gelen bir paketin hedef adresini yönlendirme tablolarında sorgulayarak, uygun rotayı belirler ve paketi bir sonraki yönlendiriciye gönderirler.

Bir IPv6 istemcisi, IPv6 ağındaki başka bir istemciye paket göndermek istediği zaman, yönlendirme tablosuna bakarak hangi arayüzünü ve ağ geçidini kullanacağına karar verir. Varsayılan ağ geçidi, farklı bir ağda yer alan ve ayrı bir yönlendirme bilgisi bulunmayan tüm paketlerin gönderildiği yönlendiricinin adresidir. IPv6 yönlendirme tablosunda aşağıdaki bilgiler yer alır:

1. Adres öneki
2. Arayüz (interface)
3. Bir sonraki adres
4. Aynı öneke sahip birden fazla yönlendirme tanımı için öncelik değeri (preference value)
5. Yönlendirme bilgisinin yaşam süresi
6. Yönlendirme bilgisinin yayınlanma bilgisi
7. Yönlendirme tipi

Yönlendiriciler arasındaki yönlendirme bilgileri, her bir yönlendiriciye tek tek bilgilerin girilmesi şeklinde statik olarak yapılabileceği gibi, dinamik olarak da yapılabilir. Yönlendiricilerin kendi aralarında yönlendirme bilgilerini paylaştıkları protokoller, yönlendirme protokolleri olarak adlandırılır. Yönlendirme protokollerinin amacı, ağdaki en iyi yolu bulmaktır. IETF tarafından tanımlanmış IPv6 yönlendirme protokollerinden

- RIPng (Routing Information Protocol next generation - RFC 2080),
- OSPFv3 (Open Shortest Path First - RFC 5340)
- IS-IS (Intermediate System to Intermediate System - RFC 5308)
- Cisco EIGRP for IPv6

iç ağlarda kullanılan yönlendirme protokolleridir.

Dış ağlar ile iletişim için BGP4+ (Border Gateway Protocol with Multiprotocol Extensions for IPv6 Inter-Domain Routing - RFC 2545) kullanılmaktadır.

Yönlendiriciler üzerinde IPv6 ayarları, IPv4 ile çok benzer şekilde yapılır. Yönlendiricinin işletim sistemine ve üreticisine bağlı olarak değişen yapılandırmalara karşın, temel adımlar aşağıdaki gibidir:

1. Yönlendirici de IPv6 yönlendirmenin etkinleştirilmesi
2. Kullanılacak arayüzde IPv6 etkinleştirilmesi ve IPv6 adresinin girilmesi
3. Statik IPv6 yönlendirme satırlarının girilmesi veya dinamik yönlendirme protokollerinin yapılandırılması

Farklı işletim sistemleri için bu adımların nasıl tanımlanacağı aşağıda verilmiştir.

Cisco IOS

Yönlendirmenin etkinleştirilmesi ve IPv6 adresinin girilmesi:

```
ipv6 unicast-routing
!
interface GigabitEthernet0/1
 ipv6 address 2001:db8:2:1::1/125
 ipv6 enable
```

OSPF yapılandırması:

```
interface GigabitEthernet0/1
 ipv6 address 2001:db8:2:1::1/125
 ipv6 enable
ipv6 ospf 111 area 0
!
ipv6 router ospf 111
router-id 0.0.0.1
area 0 range 2001:db8:2:1::/64
```

BGP yapılandırması:

```
router bgp 1234
 no bgp default ipv4-unicast
neighbor 2001:db8::6 remote-as 2345
!
address-family ipv6
 neighbor 2001:db8::6 activate
network 2001:db8::/32
!
ipv6 route 2001:db8::/32 2001:db8:2:1::2
```

Statik yönlendirme:

```
ipv6 route 2001:db8::/32 2001:db8:2:1::2
```

QUAGGA (Linux/Unix İşletim Sistemleri için)

Yönlendirici keşif mesajları için:

```
interface eth0
        no ipv6 nd suppress-ra
        ipv6 nd prefix 2001:db8:2::/64
```

BGP ayarları için:

```
router bgp 1234
 bgp router-id 0.0.0.1
 neighbor 2001:db8::6 remote-as 2345
!
 address-family ipv6
 network 2001:db8::/32
 neighbor 2001:db8::6 activate
 exit-address-family
```

ospf6d ile OSPFv3 için:

```
interface eth0
  ipv6 ospf6 instance-id 0
!
router ospf6
router-id 0.0.0.1
area 0.0.0.0 range 2001:db8:2:1::/125
interface eth0 area 0.0.0.0
```

BÖLÜM 2: TEMEL SERVİSLERİN IPV6 GEÇİŞİ

İstemcilerin IPv6 geçişinin yanı sıra, sunulan servislerin de IPv6 üzerinden hizmet verir hale getirilmesi gerekmektedir. Günümüzde, yaygın olarak kullanılan servislerin hemen hemen hepsi, IPv6 adresi üzerinden sorunsuz hizmet verebilmektedir.

Bir sunucu üzerinde, IPv6 adresi üzerinden hangi portların hangi uygulamalar tarafından dinleniliyor olduğu bilgisine, *netstat* komutu ile ulaşılabilir.

```
root@testserver:~# netstat -lnptu6
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address   State      PID/Program name
tcp6       0      0 :::80                   :::*              LISTEN     1807/apache2
tcp6       0      0 :::21                   :::*              LISTEN     16849/proftpd: (acc
tcp6       0      0 :::22                   :::*              LISTEN     2692/sshd
tcp6       0      0 ::1:631                 :::*              LISTEN     1956/cupsd
tcp6       0      0 ::1:25                  :::*              LISTEN     2677/exim4
```

Bu bölümde, bazı temel servislerin IPv6 yapılandırmaları ve dikkat edilmesi gereken konular hakkında bilgi verilmiştir.

Alan Adı Servisi - DNS

Alan adı servisi DNS, IP adreslerini oluşturan harf ve rakamlar dizisinin, kolay okunabilir ve hatırlanabilir kelimeler dizisi ile hiyerarşik bir sistemde İnternet üzerinde tekil olacak şekilde her iki yönde eşleştirilmesi işlemidir. Kullanıcıların uzun adresleri girmek yerine, kolay isimler ile servislere ulaşması için, DNS kullanılır. DNS çözümlemesi, iki yönde yapılır: Alan adının IP adresine çevrilmesi ve IP adresinin alan adına çevrilmesi. Örneğin, 193.140.83.52 IPv4 adresi ve 2001:a98:10::52 IPv6 adresi, www.ipv6.net.tr alan adına tanımlanmış, aynı şekilde www.ipv6.net.tr adresi her iki versiyon IP adresine de tanımlanmıştır.

DNS Sunucu Yapılandırması

Linux ve Unix işletim sistemleri için yaygın olarak kullanılan Bind ve Microsoft işletim sistemleri için Windows DNS sunucusu gibi IPv4 için kullanılan DNS sunucularının güncel sürümleri, IPv6 adreslerini de desteklemektedir. DNS sunucusunun güncellendikten sonra IPv6 için yapılandırılması yeterli olacaktır. DNS sunucusu yapılandırılırken IPv4 yapılandırmasından farklı olarak, alan adları çözülürken IPv4 için kullanılan A kaydı yerine

IPv6 için AAAA kaydı girilmesi, ters çözümlemelerde IPv4 için kullanılan *.in-addr.arpa* uzantısı yerine .ip6.arpa uzantısı kullanılması gerekmektedir. Örneğin, ipv6.net.tr alan adı için, .tr hiyerarşik yapısında tanımlanmış sunucu üzerinde, iki alan (zone) dosyası bulunur:

```
zone "ipv6.net.tr"        {
                    type master;
                    file "db.ipv6.net.tr";
};
//
zone "0.1.0.0.8.9.a.0.1.0.0.2.ip6.arpa"   {
                    type master;
                    file "db.2001:a98:10";
};
```

db.ipv6.net.tr dosyası içerisinde, www.ipv6.net.tr alan adına IPv4 ve IPv6 adreslerinin her ikisini tanımlayan ve www6.ipv6.net.tr adresini de aynı alan adına bağlayan aşağıdaki satırlar bulunur:

```
www             IN      A               193.140.83.52
                IN      AAAA            2001:a98:10::52
;
www6            IN      CNAME www
```

Ters çözümleme olarak adlandırılan, IP adresine karşılık alan adı tanımlanması ise, uzun yazılmasının haricinde IPv4 ile tamamen aynıdır. Ters kayıtlar girilirken dikkat edilmesi gereken önemli bir husus, IPv6 adresinin boş alanlar dâhil olmak üzere eksiksiz olarak tersten yazılması gerektiğidir. Örneğin, 2001:a98:10::52 IPv6 adresinin uzun yazılımı 2001:0A98:0010:0000:0000:0000:0000:0052'dır. Bu durumda, 2001:a98:10 kayıtlarının tutulduğu db.2001:a98 dosyası aşağıdaki gibi olmalıdır:

```
$ORIGIN         0.1.0.0.8.9.a.0.1.0.0.2.ip6.arpa.
2.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0    IN      PTR             www.ipv6.net.tr.
```

Web Servisi

IPv6 ile web sayfalarını görüntüleyebilmek için, web sunucusunun ve web tarayıcısının IPv6 destekli olması gerekmektedir. Web sunucularının ve tarayıcıların güncel sürümleri, IPv6 desteklidir. Dikkat edilmesi gereken bir nokta, erişilmek istenilen alan adı için IPv6 alan adı

kayıtlı ise, bazı web tarayıcıların öncelikle IPv6 adresine erişmeyi denedikleri, eğer erişilemez ise IPv4 adresinden erişmeyi denedikleri konusudur. Bu sebeple, DNS sunucularında alan adı kaydı olarak IPv6 adresi de girilmiş web sayfalarının, IPv6 üzerinden erişilebilir olmasına dikkat edilmeli, aksi takdirde kullanıcıların yavaşlık veya erişememe gibi sorunlarla karşılaşabileceği unutulmamalıdır. IPv6 web sayfalarına erişimde dikkat edilmesi gereken bir diğer husus, tarayıcıya alan adı yerine doğrudan IP adresi yazılmak istenildiğinde, IPv4 den farklı olarak, adresin köşeli parantez içerisinde yer alması gerektiğidir:

```
http://[2001:200:dff:fff1:216:3eff:feb1:44d7]/index.html
```

Web servisi, TCP 80 numaralı port üzerinden verilen bir servistir. Şifreli sürümü ise TCP 443 numaralı port üzerinden erişilir. IPv6 üzerinden web servisi verilebilmesi için de, IPv6 adresinin 80 ve 443 portlarından hizmet veren bir web sunucusu yazılımı gerekmektedir. Dünyada en yaygın kullanılan web sunucusu yazılımı olan Apache, sürüm 2 den itibaren IPv6 adresini eksiksiz desteklemektedir. Apache sunucusu varsayılan olarak eğer sunucu üzerinde IPv6 adresi tanımlanmış ise, IPv6 adresi üzerinden de servis vermeye başlar. Apache yapılandırmasında,

```
Listen 80
```

tanımının yer alması, sunucunun üzerinde tanımlı tüm IP sürüm ve adreslerinden 80 numaralı portu üzerinden servis verilmesini sağlamaktadır. Bu durumda IPv4 bağlantılarını kabul eden IPv6 soketleri, IPv4 eşlemli IPv6 adresleri kullanırlar. Bu yapılandırma, BSD ailesinde yer alan işletim sistemlerinde, işletim sisteminin geneline uygulanan kurallar ile çeliştiği için soruna sebep olmaktadır. IPv4 ve IPv6 adreslerine gelen isteklerin, ayrı soketler tarafından kabul edilmesi için, her iki ip protokolü ayrıca belirtilmelidir:

```
Listen 0.0.0.0:80
Listen [::]:80
```

Sunucunun sadece belirli bir IPv6 adresi üzerinden servis vermesi isteniliyor ise, IPv4 yapılandırılmasından farklı olarak adresin köşeli parantez içerisinde belirtilmesi gerekmektedir:

```
Listen [2001:db8:1::23]:80
```

Sunucunun sadece IPv4 üzerinden servis vermesi isteniliyor ise, aşağıdaki satır girilmelidir:

```
Listen 0.0.0.0:80
```

E-Posta Servisi

E-posta sunucularının IPv6 desteği, güncel sürümlerinde yer almaktadır. Yaygın olarak kullanılan e-posta sunucuları, postfix, sendmail, exim olarak sıralanabilir.

Postfix ana yapılandırma dosyası, genellikle */etc/postfix/main.cf* dosyasıdır. Bu dosya içerisinde yer alan *inet_protocols* yönergesi, postfix uygulamasının hangi IP protokolü ile çalışacağını belirler. Bu yönergenin varsayılan değeri, sadece IPv4 çalışması şeklinde olup, isteğe göre sadece IPv6'nın veya her iki protokolün desteklenmesi için bu dosya içerisinde aşağıdaki değişikler yapılabilir:

/etc/postfix/main.cf dosyası:

```
inet_protocols = ipv4          (Varsayılan değer, sadece IPv4 )
inet_protocols = all           (Sunucuda hangi arayüzler tanımlı ise hepsi)
inet_protocols = ipv4, ipv6    (IPv4 ve IPv6)
inet_protocols = ipv6          (sadece IPv6)
```

Ayrıca, giden smtp mesajlaşmalarında IPv6 adresi kullanımı için, *main.cf* dosyası içerisinde bulunan *smtp_bind_address6* yönergesi güncellenmelidir:

/etc/postfix/main.cf dosyası:

```
smtp_bind_address6 = 2001:db8:2:1::1
```

Sendmail varsayılan ayarlarında IPv6 desteklemekte olup, ayarları IPv4 ile aynıdır. Sendmail kullanımında dikkat edilmesi gereken husus, yapılandırma dosyalarına IPv6 adresleri tanımlanırken köşeli parantez yerine, IPv6: önekinin kullanılması gerektiğidir. Örnek:

```
IPv6:2001:db8:2:1
```

FTP Servisi

Dosya transfer protokolü olan FTP, 32 bitlik adreslere sahip IPv4 için tasarlanmış olmakla birlikte, RFC 2428 ile FTP'nin IPv4 ve IPv6 ile çalışabilmesi için yönergeler belirlenmiştir. Bugün yaygın olarak kullanılan FTP sunucu yazılımları, IPv6 adresini desteklemektedir.

Proftp, yaygın olarak kullanılan dosya transfer protokolü yazılımıdır. Proftp yazılımı varsayılan ayarları, çalıştığı sunucu üzerindeki tüm IPv4 ve IPv6 adresleri üzerinden FTP servisini vermeye yönelik hazırlandığı için, sunucunun üzerinde IPv6 adresinin tanımlı olması halinde

IPv6 adresi üzerinden hizmet vermeye başlayacaktır. Proftp'nin IPv6 desteği, ana yapılandırma dosyası olan *proftpd.conf* içerisinde yer almaktadır:

/etc/proftpd/proftpd.conf dosyası:

```
# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6                 on
```

Yaygın olarak kullanılan bir diğer ftp sunucu yazılımı olan vsftpd FTP sunucusu da kurulumla gelen varsayılan ayarları ile IPv6 desteklemektedir. IPv6 desteği için, */etc/vsftpd/vsftpd.conf* dosyası içeriğinde aşağıdaki satır yeralmalıdır:

```
listen_ipv6=yes
```

SSH ve Secure FTP Servisi

SSH servisi için yaygın olarak kullanılan OpenSSH yazılımının güncel sürümü, IPv6 adresini tamamen desteklemektedir. OpenSSH yazılımı varsayılan ayarları, çalıştığı sunucu üzerindeki tüm IPv4 ve IPv6 adreslerinin 22 numaralı TCP portu üzerinden SSH servisini vermeye yönelik hazırlandığı için, sunucunun üzerinde IPv6 adresinin tanımlı olması halinde IPv6 adresi üzerinden hizmet vermeye başlayacaktır.

OpenSSH sunucusunun hangi adresi ve hangi portu dinleyeceği bilgisi, *sshd_config* yapılandırma dosyası içerisinde bulunur. OpenSSH sunucusu yapılandırma dosyalarının genellikle kurulduğu yer olan */etc/ssh* dizini altında bulunan bu dosya içerisinde, *ListenAddress* yönergesi kullanılarak, tüm arayüzler üzerinden servis verilmesi kısıtlanabilir ve istenilen IP adresinde ve istenilen portta servis verilmesi sağlanabilir.

ListenAddress yönergesinin kullanımı aşağıdaki gibidir:

/etc/ssh/sshd_config dosyası:

```
ListenAddress host
ListenAddress IPv4_addr:port
ListenAddress [IPv6_addr]:port
```

Sunucunun sadece belirli bir IPv6 adresi üzerinden servis vermesi isteniyor ise, adresin köşeli parantez içerisinde belirtilmesi gerekmektedir:

/etc/ssh/sshd_config dosyası:

```
ListenAddress [2001:db8:1::23]:22
```

OpenSSH sunucusunda, SFTP servisinin de verilmesi için, *sshd_config* dosyası içerisinde, Subsystem sftp yönergesinin bulunması gerekmektedir.

/etc/ssh/sshd_config dosyası:

```
Subsystem sftp /usr/lib/openssh/sftp-server
```

OpenSSH sunucusunun sadece IPv6 üzerinden gelen istekleri kabul etmesi, IPv4 isteklerini kabul etmemesi için, sunucu başlatılırken -6 parametresi kullanılır. Benzer şekilde, ssh istemcisinin, ssh servisine ulaşılmak istenilen alan adının sadece IPv6 adresini denemesi isteniliyor ise, -6 parametresi kullanılır:

```
$ ssh -6 testuser@sshserver.ulakbim.gov.tr
Warning: Permanently added the RSA host key for IP address '2001:db8:1::23' to the list of known hosts.
```

TCP_WRAPPER Desteği

Sunucu üzerinde verilen servislerin, yazılımların desteklemesi halinde erişim güvenliği için kullanılan tcp_wrapper, servise erişimi denetlemek için iki yöntem uygulamaktadır:

- Kaynak adresine göre erişim denetlemesi
- Kullanıcılara göre erişim denetlemesi

tcp_wrapper erişim denetlemesi için, ilgili servis yazılımının tcp_wrapper desteği ile derlenmiş olması gerekmektedir ki çoğu yazılım, tcp_wrapper desteği ile derlenmiş olarak gelmektedir. tcp_wrapper yapılandırması, iki dosya üzerinden yapılır:

- /etc/hosts.deny
- /etc/hosts.allow

Genel yaklaşım, *hosts.deny* dosyası içinde herşeyi engelleyip, *hosts.allow* içerisinde erişim izinlerini vermek yönündedir. Her iki dosya içerisinde de, erişim denetlemesi olarak kaynak IP adresi kullanılmak istendiğinde, IPv4 ve IPv6 adresleri girilebilmektedir. Örneğin, SSH servisinin erişim güvenliği için kullanılan *hosts.allow* ve *hosts.deny* dosyalarında, IPv4 adresi yapılandırması gibi sunucuya bağlanacak IPv6 adresleri (köşeli parantez içerisinde) girilmelidir:

/etc/hosts.allow dosyası:

```
sshd : [2001:db8:2:1::]/64
ftpd : 192.168.0.0/16 [2001:a98:1F::]/48
exim : ALL : allow
```

BÖLÜM 3: İLERİ SEVİYE IPV6 ÖZELLİKLERİ

Dolaşılabilirlik (MIPv6)

Gelişen teknoloji ile mobil cihazların artması, mobil servislerin verilme ihtiyacını doğurmuştur. Bu ihtiyaç sebebiyle, ulaşılabilirlik, yapılandırma ve gerçek dolaşılabilirlik kavramları gündeme gelmiş, çözüm olarak ise bağlantının sağlandığı ağdan bağımsız olarak aynı IP adresinin kullanılması zorunluluğu ortaya çıkmıştır. IP dolaşılabilirlik özelliği, gezgin istemcinin İnternet'e bağlandığı noktadan bağımsız olarak ev adresi ile ulaşılabilir olmasını sağlamaktadır. Dolaşılabilirlik protokolü tanımı ile gezgin istemcinin bağlandığı konumdan sabit ev adresini alması ve gezgin istemciye gidecek olan paketlerin hangi bağlantılar üzerinden aktarılacağının belirlenmesi sağlanmaktadır.

IPv4 ile dolaşılabilirlik servisinin verilebilmesi için RFC 3344 hazırlanmış, ancak uygulama zorlukları nedeniyle yaygın kullanıma geçememiştir. IPv6 teknolojisi ile sunulan geniş IP adres aralığı sayesinde, her cihazın gerçek IP adresine sahip olabilmesi ve IPv6 ek özellikleri sayesinde, dolaşılabilirlik yeniden tanımlanarak, topolojideki aktör sayısı azaltılmış, gezgin istemci ile bağlı oldukları arasında doğrudan bağlantı kurulabilmesi mümkün olmuştur.

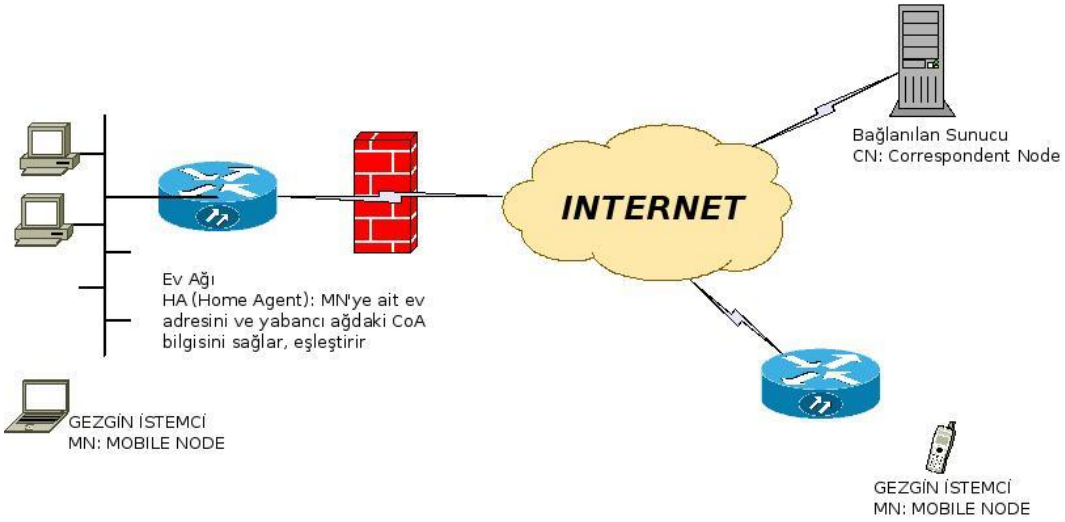
Dolaşılabilir IPv6, Mobile IPv6 kelimelerinin kısaltmasından üretilen MIPv6 olarak adlandırılmaktadır. RFC 3775 ile dolaşılabilirlik desteği tanımlanmış olup, RFC 3776 ile IPSec kullanarak gezgin istemciler ile ev sunucuları arasındaki MIPv6 sinyalleşmesinin korunması tanımlanmaktadır. Dolaşılabilir IPv6 olası kullanım alanları, telematik uygulamaları, izleme ve monitörleme uygulamaları, uzaktan yönetim, acil servis uygulamaları gibi çeşitlendirilebildiği gibi, kullanıcı doğrulama, yetkilendirme ve erişilebilirlik özelliklerinin de kullanılabilmesi hedeflenmektedir.

RFC 3775 ve 3776 ile MIPv6'nın hedefleri şu şekilde tanımlanmıştır:

- Bağlantının yapıldığı konum ile sınırlandırılmamak
- Her daim açık IP bağlantısı sağlamak
- Taşıyıcıdan bağımsız olmak
- Güçlü ve güvenilir gezgin bağlantılar sağlamak
- Uygulamaların dolaşılabilirliğini sağlamak
- Uygulamaların sürekliliğini sağlamak
- Gezgin istemcinin sunucu da olabilmesini sağlamak, (gezgin servislerin verilebilmesi)

Bileşenleri

IPv6 ile dolaşılabilirlik uygulamalarının IETF tarafından tanımlanan değişmez parçaları, Şekil 13'de gösterilmiştir.



Şekil 13: MIPv6 Anahtar Bileşenleri

MN: Mobile Node kelimelerinin kısaltmasıdır, gezgin istemciyi tanımlamaktadır. Bir başka deyişle MN, bağlantıdan veya ağdan bağımsız olarak kullandığı ev IPv6 adresi ile ulaşılabilinen IPv6 istemcidir.

CoA: Care-of-Address kelimelerinin kısaltmasıdır. MN'nin yabancı ağlardan bağlanırken aldığı geçici adresi tanımlar.

HA: Home Agent kelimelerinin kısaltmasıdır. MN'nin ev ağında bulunan ve MN'nin sabit adresini yabancı ağda iken almasını sağlayan servisi veren sunucudur. Genelde, ev ağındaki yönlendirici bu görevi üstlenmektedir.

CN: Correspondent Node kelimelerinin kısaltmasıdır. MN'nin bağlantı oturumunda ulaşmaya çalıştığı hedef IP adresine sahip sunucudur.

IPv6 Mobility Header: MIPv6 haberleşme paketlerini içermek üzere tasarlanmış IPv6 uzantı başlığıdır. Bu başlık, MN, HA ve CN tarafından, eşleştirme bilgisi için kullanılmaktadır.

Çalışma Yapısı

IETF, RFC2460 ile IPv6 paket yapısını tanımlamıştır. IPv6 paket yapısında ayrılmış olan uzatma başlıkları kullanılarak MN, HA ve CN arasındaki mesajlaşma, adres atama ve yönlendirme amaçlı kullanılacak tüm bilgiler tanımlanabilmektedir.

MIPv6 çalışma yapısına göre, gezgin istemci MN, bir yabancı ağa gittiğinde sırasıyla aşağıdaki işlemler gerçekleşir:

1. MN, bulunduğu yabancı ağdan, geçici adresini (CoA) alır ve ev ağında yeralan HA'ya bilgi gönderir.
2. CN, MN'ye göndereceği paketi sabit adresine gönderir.
3. HA, CN'den kendisine gelen paketleri MN'nin CoA adresine gönderir.
4. MN, cevapları CN'ye doğrudan gönderir.

Bu haberleşme, HA'nın paketleri ilk defa MN'ye göndermesi sırasında yapılır. Ardından MN, CN'ye kendi CoA'sını gönderir ve CN ile MN, ev ağına uğramadan doğrudan görüşmeye başlarlar.

Eşleştirme Önbelleği (Bindings Cache)

Gezgin istemcinin orijinal IPv6 adresi ile misafir olduğu ağda edindiği geçici adres CoA eşleştirilir. Gezgin istemcinin pil bitmesi, kapsama alanı dışına çıkılması gibi geçici sebeplerden dolayı ağ erişiminin kesilmesi durumunda eşleştirme tablosunun silinerek yeni baştan oluşturulmaması için, yaşam süresi belirlenerek yönlendiricilerin önbelleklerinde tutulur. Eşleştirme tablosunda, Ev Adresi, CoA, Yaşam Süresi, HA bilgilerinin yanısıra, arayüz bilgisi ve bazı istatistikler de yer alabilmektedir.

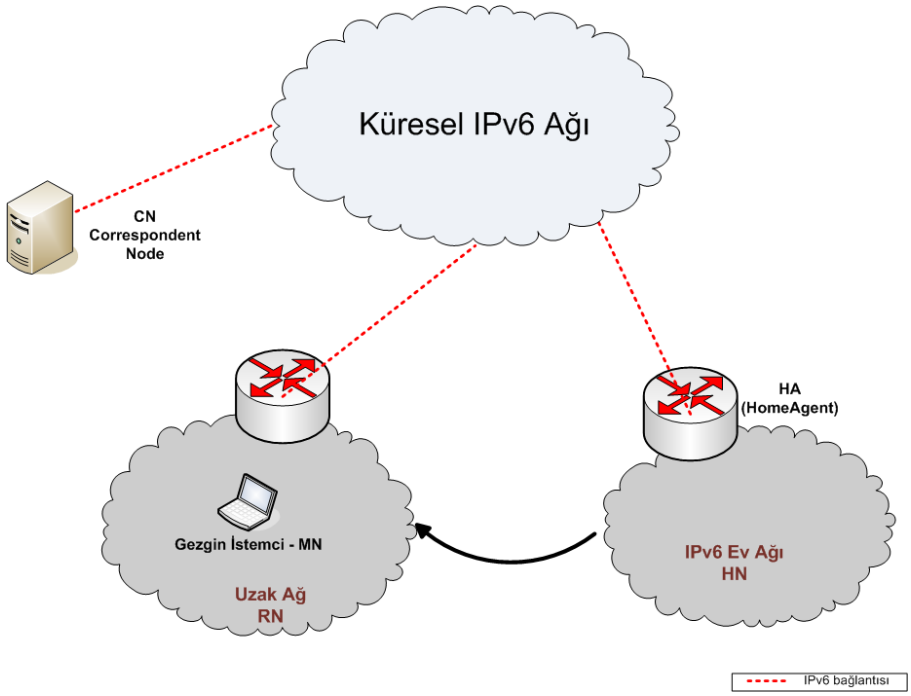
MIPv6 destekli yönlendiriciler üzerinde bir IPv6 paketi yönlendirilirken, hedef IPv6 adresi için öncelikle eşleştirme tablosunun Ev Adresi kısmına bakılır. Tabloda eşleştirme olmaz ise IPv6 yönlendirme tablolarına göre paket yönlendirmesi yapılır. Eşleştirme bulunur ise, paket enkapsüle edilerek CoA ya yönlendirilir. Bu sayede gezgin istemciye uygun yönlendirme (optimal routing) sağlanır.

MIPv6'nın sağlıklı çalışması için önemli bir bileşen olan eşleştirme tablolarının tutarlılığı için MN tarafından gönderilen "eşleştirme güncelleme", HA ve CN tarafından MN'ye gönderilen "eşleştirme alındı bilgisi" ve "eşleştirme isteği" işlemlerini kullanır.

MIPv6 Uygulaması

Dolaşılabilirlik uygulaması, Şekil 14'de verilen bileşenlerden oluşur:

- En az bir ev gözlemcisi (HA)
- En az bir gezgin istemci (MN)
- En az bir karşı sunucu (CN)
- Birbiriyle bağlantısı olan en az iki IPv6 ağı (HN ve RN)



Şekil 14: Dolaşılabilirlik Örneği

MIPv6 Bileşenleri Ayarları

Ev Ağı (HN) ve Ev Gözlemcisi (HA) Ayarları

IPv6 ağında dolaşılabilirlik özelliğini uygulayabilmek için, ev ağının yönlendiricisinin MIPv6 destekliyor olması gerekmektedir. Söz konusu destek yönlendiricinin HA olarak çalışabilmesi için gerekli yazılım desteği ve yeterli miktarda eşleştirme tablosunu önbellekte tutabilecek kadar donanım desteği şeklindedir.

Cisco Yönlendirici

Ev ağının bağlantısını sağlayan arayüze "ipv6 mobile home-agent" komutu girilmesi yeterlidir. Eşleştirme (binding) özelliğinin çalıştırılması için ise genel yapılandırma kipinde "ipv6 mobile home-agent" komutu ve altına "binding" komutu girilmesi yeterlidir. Cisco üzerinde HA ayarları için atılacak adımlar aşağıda verilmiştir:

```
enable
configure terminal
interface FastEthernet0/1
ipv6 mobile home-agent [preference preference-value]
exit
ipv6 mobile home-agent
binding [access access-list-name | auth-option | seconds | maximum | refresh]
end
```

Yönlendirici üzerinde tanımlı genel MIPv6 tanımlarını görmek için, “show ipv6 mobile globals” komutu kullanılır:

```
HomeNetwork#show ipv6 mobile globals
Mobile IPv6 Global Settings:

  1 Home Agent service on following interfaces:
    FastEthernet0/1
  Bindings:
    Maximum number is unlimited.
    1 bindings are in use
    1 bindings peak
    Binding lifetime permitted is 262140 seconds
    Recommended refresh time is 300 seconds
HomeNetwork#
```

Gezgin istemcinin uzak ağa gitmesi ile HA’ya CoA adresi bildirilir ve bu adres eşleştirme tablosuna yazılır. Eşleştirme tablosunu görüntülemek için, “show ipv6 mobile binding” komutu kullanılır. Gezgin istemci ile HA arasında oluşturulan tünel ve paket alışverişine dair trafik bilgisi, “show ipv6 mobile traffic” komutu ile gözlenebilir.

Linux Yönlendirici

PC-Yönlendirici kullanımı durumunda da IPv6 dolaşılabilirlik özellikleri kullanılabilmektedir. Bu bölümde anlatılan ayarlar, Linux işletim sistemi Debian sürümü üzerinde gerçekleştirilmiş olup, ilgili paketlerin kurulması ile diğer Linux sürümlerine de kurulum yapılabilir.

Kurulum için paket yöneticisine MIPv6 paketlerinin yüklenmesi için gerekli depo sunucuları tanımlanmalıdır. /etc/apt/sources.list dosyasına aşağıdaki iki kaynak eklenmelidir.

```
deb http://software.nautilus6.org/packages/debian sid
deb-src http://software.nautilus6.org/packages/debian sid
```

Ardından sistem güncellenerek radvd, linux-mip6 ve mipv6-daemon-umip paketleri kurulmalıdır:

```
apt-get update
apt-get install radvd linux-mip6 mipv6-daemon-umip
```

Yönlendirici ayarları için, /etc/mip6d.conf ve /etc/radvd.conf dosyaları kullanılır.

HA için Örnek mip6d.conf Dosyası

```
## What function do we want this to be?
NodeConfig HA;
## Interface
Interface “eth1”;
## Disable IPsec configuration
UseMnHaIPsec disabled;
## Set Debug
DebugLevel 10;
## Key Management Mobility Capability
```

HA için Örnek radvd.conf dosyası:

```
interface eth1
{
        AdvSendAdvert on;
        MaxRtrAdvInterval 3;
        MinRtrAdvInterval 1;
        AdvHomeAgentFlag on;
        AdvHomeAgentInfo on;
        HomeAgentLifetime 1800;
        HomeAgentPreference 10;
        prefix 2001:a98:13:fefe::1/64
        {
                AdvRouterAddr on;
                AdvOnLink on;
                AdvAutonomous on;
        };
};
```

Ayrıca işletim sisteminin yönlendirme yapabilmesi için gerekli olan kernel ayarları (/etc/sysctl.conf dosyası, net.ipv6.ip_forward=1) ile statik veya dinamik yönlendirmeler girilmelidir. Bu bölümde anlatılan ayarlar yapıldıktan sonra, radvd ve mip6d programları ile Linux yönlendirici üzerinde ev gözlemcisi HA çalıştırılır:

```
radvd –C /etc/radvd.conf
mip6d –c /etc/mip6d.conf
```

Gezgin İstemci Ayarları

Bu bölümde, işletim sistemlerinin gezgin istemci desteği ve yapılandırmaları anlatılmaktadır. İşletim sistemleri içinde Linux/Unix ve türevlerinin MIPv6 desteğinin çeşitli uygulamalar ile birlikte verilmesi sebebiyle, IPv6-GO ortamında da kullanılan Linux işletim sistemi yapılandırması detaylı olarak anlatılmıştır.

Linux/Unix

Linux yönlendirici bölümünde anlatıldığı gibi işletim sistemine MIPv6 desteği verilen gezgin istemcinin, sadece mip6d.conf dosyasında gerekli değişiklikler yapılması yeterlidir. Yapılacak tanımlarda MN fonksiyonunun kullanılacağı belirtilmeli, HA adresi ve ev adresleri aşağıdaki örnekte gösterildiği gibi ilgili arayüz tanımı altına girilmelidir.

H4LINUX Gezgin istemci mip6d.conf dosyası

```
## What function do we want this to be?
NodeConfig MN;
## Interface
Interface “eth0”;
## Disable IPsec configuration
UseMnHaIPsec disabled;
## Set Debug
DebugLevel 10;
## Key Management Mobility Capability
KeyMngMobCapability disabled;
MnHomeLink “eth0” {
      HomeAgentAddress 2001:a98:13:fefe::1;
      HomeAddress 2001:a98:13:fefe:20d:61ff:fe3f:9df3/64;
}
```

Yukarıda verilen ayarlar yapıldıktan sonra mip6d programı ile Linux gezgin istemci üzerinde MIPv6 çalıştırılır:

```
mip6d –c /etc/mip6d.conf
```

MacOSX

MacOSX için MIPv6 desteği işletim sistem içerisinde yer almamaktadır. Ancak MIPv6 desteği KAME projesi altında SHISA Mobile IPv6 olarak Darwin platformunda bulunmaktadır. Darwin ile MIPv6 desteğinin verilebilmesi için kernelin MIPv6 desteği ile yeniden yapılandırılması ve derlenmesi gerekmektedir.

Windows

Microsoft Windows XP ve Windows Server 2003 ile beraber gelen IPv6 yapısında, MIPv6 desteği sadece CN olarak mevcut iken bu işletim sistemleri MN veya HA desteği bulundurmamaktadır. Yeni nesil Microsoft işletim sistemleri olan Windows Vista ve Windows 7 de ise MIPv6 desteği tamamen kaldırılmıştır.

Diğerleri

Bu çalışmanın yapıldığı tarihte, mobil telefon işletim sistemleri olan Windows Mobile, Apple iPhone, Blackberry ve Symbian işletim sistemlerinde MIPv6 desteği bulunamamıştır.

Çoklu Gönderim

IPv6 Çoklu Gönderim Adreslemesi

IPv6 adres aralığının geniş olması aynı zamanda IPv6 çoklu gönderim grupları için kullanılabilecek adres sayısının da büyük oranda genişlemesi anlamına gelmektedir. Bu sayede IPv4 çoklu gönderim uygulamalarında zaman zaman karşılaşılan farklı çoklu gönderim yayınları için aynı grup adresinin kullanılması gibi sorunlar ortadan kalkacaktır.

Aynı zamanda IPv6 adres yapısında yer alan bazı yeni bilgiler sayesinde çoklu gönderim paketlerinin ulaşacağı ağların kısıtlanması, dolayısıyla çoklu gönderim yayının istenen yönetimsel sınırlar içinde kalması sağlanabilecektir.

OSI Veri Bağı Katmanı (L2) Çoklu Gönderim Adresleme

IPv4 çoklu gönderim IP paketlerinin veri bağı katmanındaki adres aralığı IANA tarafından tahsis edilen 01:00:5e ile başlamalıdır [RFC 1112]. IPv6 çoklu gönderim adreslemesinde Ethernet MAC adresleri 33:33 ile başlamalıdır. IPv6 L3 IP adresi L2 MAC adresine çevrilirken IP adresinin en son 4 oktetlik kısmı MAC adresinin 33:33 başlatılarak sonuna eklenir. Örneğin ağdaki tüm yönlendiricileri temsil eden FF02::2 adresinin MAC adresi karşılığı 33:33:00:00:00:02'dir. Çoklu gönderim adres yapısı, Bölüm 1: IPv6 Temelleri ve Yapılandırması, IPv6 Adres Tipleri bölümünde anlatılmıştır.

Çoklu Gönderim Dinleyici Protokolü (Multicast Listener Discovery, MLD)

IPv4'te istemciler ve yönlendiriciler grup üyelik bilgilerini IGMP (Internet Group Management Protocol) aracılığı ile paylaşmaktadır. IPv6'da bu protokol yerini MLD (Multicast Listener Discovery) protokolüne bırakmıştır. MLD protokolünün MLD1 (RFC2710) ve MLDv2 (RFC 3810) olmak üzere iki sürümü bulunmaktadır. MLD1 IGMP2 protokolünden türetilmiştir ve tanım ve yetenek olarak benzerlik göstermektedir. Benzer şekilde MLD2 IGMPv3 ile aynı yetenekleri paylaşmaktadır.

IGMP protokolüne benzer şekilde MLD protokolünün amacı yönlendiricilerin kendilerine doğrudan bağlı ağlardaki çoklu gönderim istemcilerini tespit edebilmelerini sağlamaktır. MLD protokolü aracılığıyla yönlendiriciler kendilerine bağlı ağlardaki istemcileri ve grup adreslerini öğrenmekte ve bu bilgiyi çoklu gönderim yönlendirme protokolü aracılığıyla diğer yönlendiricilerle paylaşarak çoklu gönderim istemci ve sunucuları arasındaki rotayı tanımlayan bir ağaç yapısı oluşturmak için kullanmaktadır.

MLD mesajları ICMPv6 paketleri aracılığıyla iletilmektedir. MLDv1 protokolü ICMPv6 130, 131 ve 132 mesaj tiplerini kullanmakta iken, MLDv2 protokolünde 131 ve 132 geriye dönük uyumluk için kullanılmakta olup ayrıca ICMPv6 tip 132'nin yerine de tip 143 kullanmaktadır. MLDv1 protokolünü kullanan yönlendiriciler FF02::1 çoklu gönderim adresine periyodik olarak ICMPv6 130 mesajları göndererek dahil olunmak istenilen grupları sorgularlar. İstemciler katılmak istedikleri her bir çoklu gönderim grubu için ICMPv6 131 mesajı gönderirler. IPv6'da SSM servisinin kullanılabilmesi için yönlendirici ve istemcinin MLDv2 protokolünü desteklemesi gerekmektedir.

Servis Modelleri

Kaynağı Tanımsız Çoklu Gönderim (Any Source Multicast, ASM)

Bu servis modelinde çoklu gönderim grubuna (G) herhangi bir kaynak veri gönderebilir, kaynağın veri göndermesi için grubun çoklu gönderim adresini bilmesi yeterlidir. Benzer şekilde gruptan veri almak isteyen istemcilerin veriyi alabilmeleri için sadece grubun adresini bilmeleri yeterlidir. Bu servis modelinde, birden fazla istemci aynı anda bir gruba veri gönderebilir ve alabilir. Alıcının veriyi almak için veriyi gönderenin kaynak IP adresini bilmesine gerek yoktur.

Kaynağı Tanımlı Çoklu Gönderim (Source Specific Multicast, SSM)

RFC 4607'de tanımlanan kaynağı tanımlı çoklu gönderim modelinde, istemcinin gönderilen paketi alabilmesi için göndericinin kaynağın IP adresini bilmesi gerekir. Bu modelde çoklu gönderim kanalı, gruba (G) gönderen farklı kaynaklar (K_1, K_2) çifti olarak tanımlanır. Aynı grup adresi için (K_1,G), (K_2, G) farklı kanallardır.

Yönlendirme

Hem IPv4'de hem de IPv6'da çoklu gönderim kontrol paketleri tekil gönderim IP yönlendirme tablosuna göre yönlendirilmekte ve bu amaçla OSPF, IS-IS ya da MBGP gibi protokoller kullanılabilmektedir. Bunun yanı sıra, her bir çoklu gönderim yayını için sunucu/randevu noktası ve istemciler arasındaki ağaç yapıyı oluşturmak üzere bir de çoklu gönderim yönlendirme protokolüne ihtiyaç duyulmaktadır.

Bu konuda standart olarak kabul görmüş olan PIM protokolünün IPv6 için PIM-SM (PIM Sparse Mode) ve PIM-SSM (PIM Single Source Multicast) olmak üzere iki varyantı bulunmaktadır:

PIM Dense Mode (PIM-DM)

Bu yönlendirme modelinde çoklu gönderim adresine bir paket gönderildiğinde yönlendirici üzerindeki tüm ağ arabirimlerinden paketi gönderir (flood). Paketin gönderildiği ağlardan gruba dâhil olmak için herhangi bir katılım isteği gelmez ise, bu ağın bağlı olduğu ağ arabirimden paket gönderilmesi katılım isteği gelinceye kadar kesilir (prune).

PIM-DM modelin efektif olarak kullanılabilmesi için gönderici ve istemci arasındaki hop sayısı fazla olamamalı ve yönlendiriciye bağlı tüm ağlarda göndericinin grup adresine gönderdiği paketleri almak isteyen istemciler bulunmalıdır. Bu nedenle, deneysel IPv6 PIM-DM uygulamaları bulunmakla birlikte uygulamada çoklu gönderim yönlendirme protokolü olarak PIM-SM kullanılmaktadır.

PIM Sparse-Dense Mode (PIM-SM)

PIM-SM protokolü birden fazla çoklu gönderim sunucusu ve istemcisi için bir buluşma noktası teşkil eden bir Randevu Noktası (Randevouz Point, RP) ile istemciler arasında paylaşımlı bir ağaç yapısı oluşturulmasını sağlar. Sunucular yayınlarını bu RP'ye göndererek, paylaşımlı ağaç yapıda yer alan bütün istemcilere dağıtılmasını sağlayabilirler. Ağaç yapının "paylaşımlı" olarak anılmasının sebebi, birden fazla sunucunun aynı grup adresine ulaşmak için aynı RP ve ağaç yapıyı kullanabilir olmasıdır. Bu nedenle PIM-SM, çoklu video konferanslar ve P2P oyunlar gibi birden fazla sunucu ve birden fazla istemci içeren ASM (Any-Source Multicast) modeli yapılar için kullanılan bir protokoldür.

Öte yandan PIM-SSM protokolünde tek bir sunucu söz konusu olduğu için RP kavramı yer almamaktadır. PIM-SSM, istemcilerden aldığı IPv6 çoklu gönderim grup adresi bilgisi ile IPv6 tekil gönderim gönderici adresini kullanarak, her bir sunucu için ayrı bir ağaç yapısı oluşturur.

IPsec

Ağdaki iletişimde güvenliğin sağlanması için gerekli kriterler; gizlilik (confidentiality), bütünlük (integrity), doğrulama (authentication) olmak üzere üç ana başlıkta incelenebilir.

Gizlilik, güvenli ağ iletişiminde bir noktadan başka bir noktaya gönderilen paketlerin istenmeyen kişiler tarafından okunmasının engellenmesi bölümünü kapsamaktadır. Ağ iletişiminde gizlilik simetrik (AES, DES vb.) veya asimetrik (RSA vb.) şifreleme algoritmaları içeren kripto sistemler kullanılarak sağlanabilmektedir.

Bütünlük, gönderilen paketin içeriğinin değiştirilmeden hedefe ulaştığının doğrulanmasıdır. Paket bütünlüğünün korunup korunmadığı özet fonksiyonlar aracılığı ile kontrol edilmektedir. Ortak anahtar kullanımına dayanan HMAC algoritması ile bütünlük kontrolü gerçekleştirilebilir. Bütünlük kontrolü için bir diğer yöntem ise açık anahtar altyapısına dayanan elektronik imza yöntemidir. Her iki yöntemde de özet algoritmaları kullanılarak

mesajın özet değeri kaynak ve hedef noktalarında hesaplanmakta ve karşılaştırılmaktadır. Doğrulama; paketin, gerçekten gönderildiği iddia edilen kaynak tarafından gönderildiğinin doğrulanmasıdır.

İstemcilerin bir ağa uzaktan erişiminin veya iki ağın birbiri arasında iletişiminin güvenli sağlanabilmesi için kiralık hatlar ve benzeri çözümlerden daha az maliyetli ve daha az yapılandırma ihtiyacı olan VPN (Virtual Private Network - Sanal Özel Ağ) teknolojisi tercih edilmektedir. Yapılan bağlantı şekline göre, Uzaktan Erişim Sanal Özel Ağı (Remote Access VPN) ve Alandan Alana Sanal Özel Ağ (Site-to-Site VPN) olmak üzere iki tip VPN teknolojisi bulunmaktadır. Uzaktan Erişim Sanal Özel Ağı; genel kullanıma açık ağda yer alan istemcinin, uzak ağa güvenli bir şekilde bağlantı gerçekleştirmesini sağlamaktadır. Alandan Alana Sanal Özel Ağ ise iki ağ arasında mevcut internet altyapısı kullanılarak, adanmış hat kullanımına ihtiyaç duyulmadan, güvenli bağlantı kurulmasını sağlamaktadır.

VPN ile güvenli ağ iletişimi çeşitli protokoller ve uygulamalar kullanılarak ağın farklı katmanlarında gerçekleştirilebilmektedir. Bu uygulamalar arasında yer alan IPsec OSI ağ (network) katmanında, TLS/SSL ve SSH ise OSI iletim (transport) ve uygulama (application) katmanlarında çalışmaktadır.

IPsec ağ katmanında çalıştığı için ağdaki herhangi bir trafiğin güvenliğinin sağlanması için kullanılabilmektedir. İletim ve uygulama katmanlarında çalışan TLS/SSL ve SSH gibi protokollerin kullanılabilmesi için, ilgili uygulamanın bu protokolleri desteklemesi gerekmektedir.

IPv6 Ağlarında IPsec Kullanımı

Erişim kontrolü, paket bazında bütünlük kontrolü, kaynak doğrulaması, paket sırası bütünlük kontrolü ile tekrarlanan paketlerin tespit ve reddedilmesi, şifreleme ile paket içeriğinin gizlenmesi, IPsec kullanılarak ağda uygulanabilecek güvenlik önlemleri arasında yer almaktadır.

Bahsedilen güvenlik önlemleri Doğrulama Başlığı (Authentication Header - AH) ve Kapsüllenmiş Güvenlik Yük Başlığı (Encapsulating Security Payload - ESP) protokolleri ile sağlanmaktadır. Bu protokollere ek olarak anahtar dağıtımı ve yönetimi ile ilgili olarak İnternet Anahtar Değişimi (Internet Key Exchange - IKE) protokolü de kullanılmaktadır.

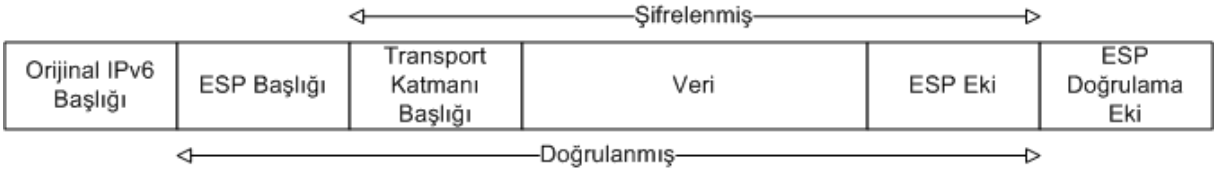
IPsec, IPv6 tasarımının bir parçasıdır. IPv6 ağlarında IPsec kullanımı ESP ve AH uzantı başlıkları ile mümkündür. ESP uzantı başlığı kullanılarak gizlilik (şifreleme ile), paket bazında bütünlük, kaynak doğrulaması güvenlik tedbirleri uygulanabilir. AH başlığı kullanılarak ise ağdaki paketlerin bütünlük kontrolü ve kaynak doğrulaması sağlanabilir. ESP veya AH, paketlerin tekrarlanması temelli saldırılara karşı koruma sağlamaktadır. ESP gizlilik ve doğrulama, AH ise doğrulama sağlamaktadır. Aralarındaki temel fark doğrulama kapsamlarıdır. ESP paket başlığını doğrulamamaktadır. Tünel kipinde orijinal paket başlığı

doğrulanmakta ama yeni üretilen paket başlığı doğrulanmamaktadır. AH ise her iki kipte de bütün paketi doğrulamaktadır. ESP ek başlığı sadece-şifreleme veya sadece-doğrulama yapacak şekilde kullanılabilir. Ancak doğrulama yapılmadan şifreleme güvenli olmadığı için önerilmemektedir. ESP ve AH ek başlıklarının birlikte kullanılması ile ilgili daha detaylı bilgi ve güvenlik önerileri RFC 2406'da yer almaktadır.

IPv6 protokolü ile IPsec desteğinin getirilmiş olması, IPv6 ağlarının tamamında IPsec kullanılacağı yönünde yanlış bir öngörü oluşturmaktadır. Bu yanlış öngörü ile IPv6 ağlarının IPv4 ağlarından daha güvenli olacağı öne sürülmektedir. IPsec desteği zorunlu olmasına rağmen tüm IPv6 ağlarında IPsec kullanımı, yönetilebilirlik ve cihazların işlem gücü açısından mümkün gözükmemektedir.

IPsec kullanımı ortadaki adam ve paket koklama saldırılarına karşı ağı güvenli hale getirmektedir. Ancak ESP ve AH kullanılan bir ağda yönetilebilirlik (paket tabanlı politika uygulanamaması, ağın izlenememesi, ağdaki problemlerin tespit edilememesi, giderilememesi) ve güvenlik (derin paket incelemesinin mümkün olmaması, şifrelenmiş pakete anti virüs taraması yapılamaması) problemleri oluşturmaktadır. Saldırının IPsec kullanan bir istemciden kaynaklanması da mümkündür (trojan, solucan vb. zararlı yazılımlar).

IPsec ağda iki yöntem kullanılarak uygulanabilir. Yöntemlerden ilki olan transport kipinde IPsec kullanarak iletişim sağlayan uç noktaları birbiriyle doğrudan bağlantılıdır. Bu yöntemde orijinal IPv6 başlığı şifrelenmediği veya değiştirilmediği için yönlendirme kurallarında bir değişiklik olmaz. ESP, paket başlığı dışındaki bölümü şifrelemekte ve/veya doğrulamaktadır. AH ise IPv6 başlığı dâhil tüm paketi doğrulamaktadır. Paket başlığında yer alan IP adresleri ve port numaraları değiştirilirse paket bütünlük değeri değişeceğinden doğrulama gerçekleşemez. Transport kipinde ESP ve AH kullanımı paket örnekleri sırasıyla Şekil 15 ve Şekil 16'da verilmiştir.



Şekil 15: Transport kipinde ESP kullanımı paket yapısı

Şekil 16: Transport kipinde AH kullanımı paket yapısı

Tünel kipi, IPsec uygulamasında ikinci yöntemdir. Tünel kipinde istemciden istemciye yolun bir bölümünde yer alan iki ağ cihazı arasında tünel oluşturulur. Arasında tünel oluşturulan cihazlar güvenlik ağ geçidi (security gateway) olarak adlandırılmaktadır. Bu kipte IP paketi

yeni bir IP başlığı oluşturularak sarmalanır. ESP tünel kipinde kullanıldığında yeni bir IP başlığı oluşturulur. Orijinal IP başlığı şifrelenen kısımda kalır ve yeni oluşturulan başlık ile sarmalanır. AH tünel kipinde kullanıldığında ise orijinal başlık hem sarmalanmış pakette, hem de sarmalayan pakette kullanılır. Bu durumda AH tüm paket için doğrulama gerçekleştirir. Tünel kipinde ESP ve AH kullanımı paket örnekleri sırasıyla Şekil 17 ve Şekil 18 'de verilmiştir.

Şekil 17: Tünel kipinde ESP kullanımı paket yapısı

Şekil 18: **Tünel kipinde AH kullanımı paket yapısı**

BÖLÜM 4: IPV6 GEÇİŞ YÖNTEMLERİ

Günümüzde İnternet altyapısında yaygın olarak kullanılan IPv4'ün kademeli olarak yerini yeni nesil İnternet protokolü olan IPv6'ya bırakması beklenmektedir. Gelecekte bütün servisler ve ağ altyapısı IPv6'ya taşındığında bütün cihazlar yalın IPv6 olarak yapılandırabilecektir. Ancak geçiş aşamasında yalın IPv6 desteği sağlanana kadar IPv4 ve IPv6 belirli bir süre birlikte kullanılacaktır. Bu geçiş sürecinde her iki protokolün birlikte kullanımına olanak sağlamak üzere IETF tarafından önerilen geçiş yöntemleri 3 ana başlıkta incelenebilir:

1. İkili Yığın (Dual Stack),
2. Tünelleme (Tunelling)
3. Çeviriciler (Translation)

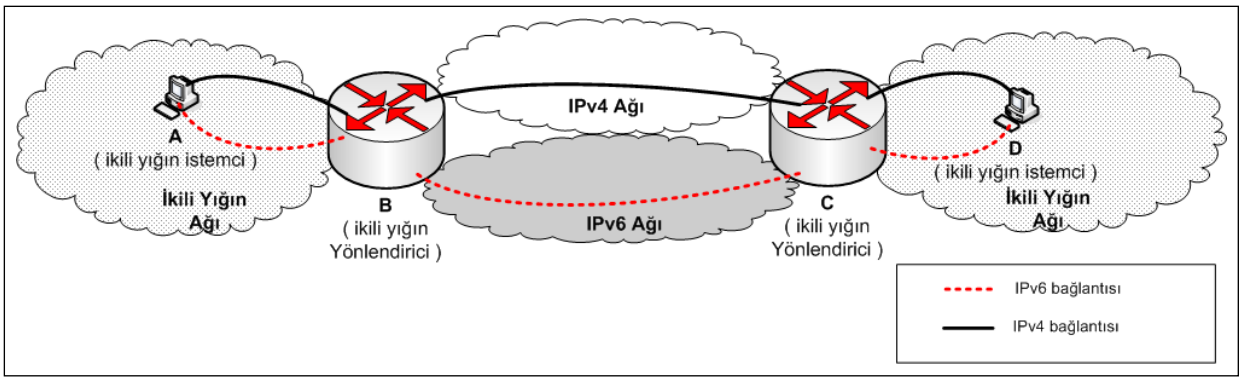
İkili yığın geçiş yönteminin, güvenlik ve performans açısından en uygun geçiş yöntemi olup, çeşitli nedenler ile bu yöntemin kullanılamadığı durumlarda tünelleme ve çevirici yöntemleri kullanılabilir. Tünelleme yöntemlerindeki başlıca problemler tünel uçları arasındaki trafiğin izlenmesi ve kontrol edilmesinin zorluğudur. Bu ve benzeri yönetim ve güvenlik zafiyetlerinden dolayı tünel yöntemlerinin mecbur kalınmadıkça kullanılmaması, kullanıldığında ise ağ yöneticilerinin durumdan haberdar olması sağlanmalıdır. El ile ayarlanmış tüneller, dinamik kurulan tünellere göre, tünel başlangıç ve bitiş noktaları statik olarak belirlendiğinden daha güvenlidir, ancak el ile ayarlanmış tünellerin ağda çok sayıda noktada kullanılması ağ yönetimini zorlaştırmaktadır.

Aşağıda her geçiş yöntemi kısaca tanıtılarak, yaygın olarak kullanılan geçiş yöntemleri ile ilgili temel yapılandırma bilgilerine yer verilmiştir.

İkili Yığın Geçiş Yöntemi

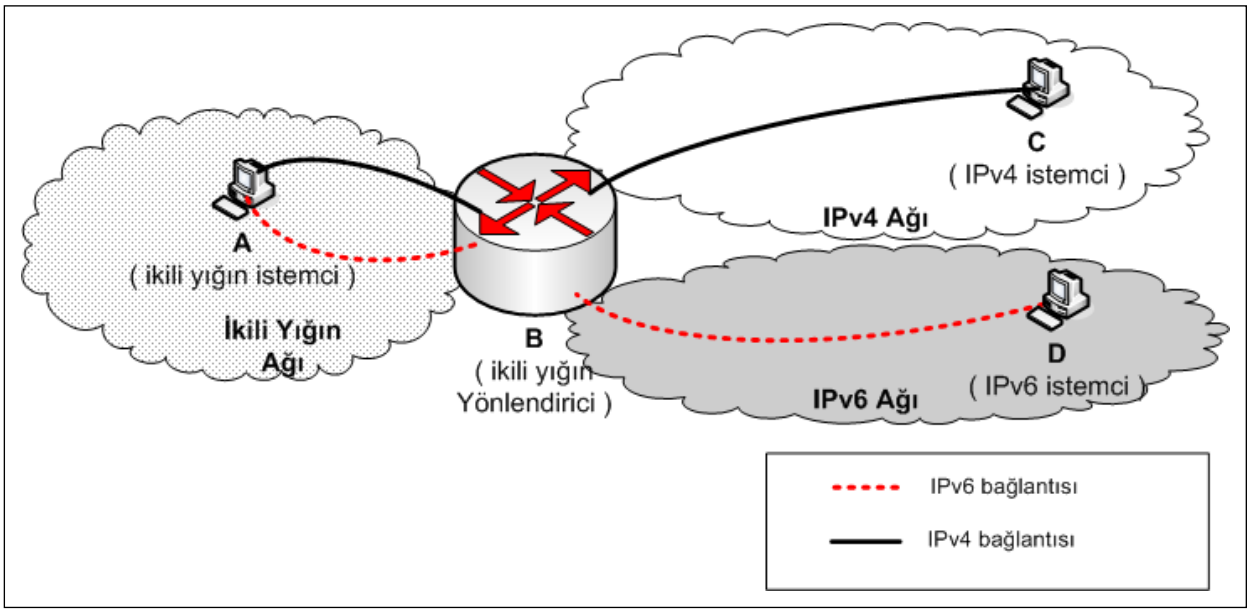
İkili yığın geçiş yöntemi kullanılan ağlarda istemciler, sunucular ve ağ cihazları her iki protokolü de desteklemektedir. Ağdaki her cihazın IPv4 ve IPv6 adresleri vardır.

Şekil 19'da yer alan örnek ikili yığın ağında A, D istemcileri ve B, C yönlendiricileri ikili yığın yöntemini kullanmaktadır. Bu ağ yapısında tüm uçların IPv4 ve IPv6 adresleri vardır. Uçlar aralarındaki iletişimi, IPv4 adresleri ile IPv4 protokolü üzerinden veya IPv6 adresleri ile IPv6 protokolü üzerinden gerçekleştirebilirler. Tüm uçlarda her iki protokol için de yönlendirme bilgisi tutulmaktadır.



Şekil 19: İkili Yığın Ağların Haberleşmesi

Şekil 20'da yer alan örnek ağ yapısında görüldüğü üzere ikili yığın yöntemini kullanan istemci A; IPv4 istemci C ile IPv4 protokolü üzerinden, IPv6 istemci D ile IPv6 protokolü üzerinden haberleşebilmektedir.



Şekil 20: İkili Yığın Ağ ile IPv4 ve IPv6 Uçların Haberleşmesi

İkili Yığın Ağlarda IP Sürümünün Seçimi

İkili yığın yöntemini kullanan ağlarda DNS sunucuları IP kayıtları için A (IPv4) ve AAAA (IPv6) kaydı tutmaktadır. Bu nedenle DNS sunucuları istemcilerin alan adları için yaptığı sorgulara hem IPv4 hem de IPv6 adres bilgisi dönmektedir. Ağ cihazlarına ikili yığın desteği verilmesi durumunda varsayılan iletişim protokolü IPv6'dır. Bu nedenle ikili yığın destekli istemciler, herhangi bir adrese bağlanmak istediklerinde bağlanılan adrese ait IPv6 alan adı kaydının bulunması durumunda bağlantı IPv6 üzerinden gerçekleştirilmeye çalışılır. IPv6 alan adının bulunamaması veya IPv6 üzerinden bağlanılamaması durumunda sunucuya IPv4 üzerinden bağlanılır.

İkili Yığın Bileşenleri

İkili Yığın İstemci

İkili yığın istemci, hem IPv4, hem de IPv6 adresine sahiptir. Bunun için istemcinin ağ katmanında hem IPv4 hem de IPv6 desteği bulunması gereklidir.

Windows Vista, Windows 7, FreeBSD, Debian, Ubuntu işletim sistemlerinde iki protokol desteği varsayılan olarak gelmektedir. FreeBSD'de IPv6 desteğini aktif hale getirmek için *ipv6_enable="YES"* satırı */etc/rc.conf* dosyasına eklenmelidir. Windows XP SP2 ve sonraki sürümlerinde IPv6 desteğini aktif hale getirmek için *netsh interface ipv6 install* komutu kullanılmalıdır.

İkili yığın istemcilerde yönlendirme her iki protokol için ayrı ayrı ayarlanmalıdır. Farklı işletim sistemleri için IP adresi atama ve varsayılan yönlendirme ile ilgili ayarlar ilerleyen bölümlerde verilmiştir.

İkili Yığın Yönlendirici

İkili yığın yönlendiriciler hem IPv4 ağına hem de IPv6 ağına bağlantı sağlamaktadır. İkili yığın yönlendiricilerde her iki protokolün aynı anda çalışması nedeniyle, güvenlik ve yönetim açısından bazı hususlara dikkat edilmelidir. İkili yığın yönlendiriciler her iki protokol için de güncel yönlendirme tablolarını oluşturacak şekilde yapılandırılmalıdır. Aynı zamanda her iki protokol için de güvenlik kuralları oluşturulmalı ve güncellenmelidir. İkili yığın yapılandırma örnekleri ilerleyen bölümlerde verilmiştir.

İkili Yığın Yapılandırması

Cisco IOS

Cisco IOS için IPv4 ve IPv6 adres yapılandırmaları aşağıda verilmiştir. Bu yapılandırmalara ek olarak IPv4 ve IPv6 yönlendirme bilgisi statik olarak girilebilir veya yönlendirme protokollerinden biri kullanılabilir.

```
interface Vlan26
 ip address 172.16.30.17 255.255.255.248
 ipv6 address 2001:db8:1::6/125
 ipv6 enable
!
```

FreeBSD

FreeBSD işletim sistemine IPv4 adresi atamak ve varsayılan yönlendirici adresini tanımlamak için kullanılan komutlar aşağıda belirtilmiştir.

```
/sbin/ifconfig fxp0 inet 172.16.30.211 netmask 255.255.255.248
/sbin/route add default 172.16.30.209
```

FreeBSD işletim sistemine IPv6 adresi atamak ve varsayılan yönlendirici adresini tanımlamak için kullanılan komutlar aşağıda belirtilmiştir.

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

Linux

Linux işletim sistemine IPv4 adresi atamak ve varsayılan yönlendirici adresini tanımlamak için kullanılan komutlar aşağıda belirtilmiştir.

```
/sbin/ifconfig eth0 inet 172.16.30.5 netmask 255.255.255.0
/sbin/route add default gw 172.16.30.1
```

Linux işletim sistemine IPv6 adresi atamak ve varsayılan yönlendirici adresini tanımlamak için kullanılan komutlar aşağıda belirtilmiştir.

```
/sbin/ifconfig eth0 add 2001:db8:1:1::3/64
/sbin/route add --inet6 default gw 2001:db8:1:1::1
```

Windows XP

Windows XP işletim sistemine grafik arayüzü kullanılarak “Ağ Bağlantılarım” başlığından IPv4 adres ve varsayılan ağ geçidi ayarları yapılabilir. Komut satırı kullanılarak ise aşağıda verilen komut kullanılarak IPv4 adres ve varsayılan ağ geçidi atama işlemi gerçekleştirilebilir.

```
netsh interface ip set address "Local Area Connection" static 192.168.0.2 255.255.255.0
192.168.0.1
```

Windows XP işletim sisteminde, ilk kurulumda IPv6 desteği yer almamaktadır. IPv6 desteğinin kullanılabilmesi grafik arayüzü kullanılarak “Ağ Bağlantılarım” başlığında yer alan ilgili ağ bağlantısı özelliklerinden yüklenebilmektedir. Bir başka yöntem ise komut satırından *netsh interface ipv6 install* komutu çalıştırılarak IPv6’nın aktif hale getirilmesidir. IPv6 yapılandırılması komut satırında

netsh interface ipv6 add address InterfaceNameOrIndex IPv6Address

komutu kullanılarak yapılabilmektedir. *InterfaceNameOrIndex* parametresi *netsh interface ipv6 show interface* komutunun çıktısından elde edilebilir. IPv6 adres ve varsayılan ağ geçidi yapılandırılmasının komut satırından yapılabilmesi için gerekli komutlar sırasıyla aşağıda verilmiştir.

```
netsh interface ipv6 install
netsh interface ipv6 set address “Local Area Connection” 2001:db8:1:dede::23
netsh interface ipv6 add route ::/  "Local Area Connection"
```

Windows 7 / Vista

Windows XP ’den farklı olarak, Windows 7 / Vista işletim sistemlerinde IPv6 desteği kurulumda otomatik olarak gelmektedir. IPv4/IPv6 ayarları grafik arayüz veya komut satırında

netsh interface ipv6 add address InterfaceNameOrIndex IPv6Address

komutu kullanılarak yapılabilmektedir. *InterfaceNameOrIndex* parametresi *netsh interface ipv6 show interface* komutunun çıktısından elde edilebilir. IPv4/IPv6 adres ve varsayılan ağ geçidi yapılandırılması komut satırından yapılabilmesi için gerekli komutlar sırasıyla aşağıda verilmiştir.

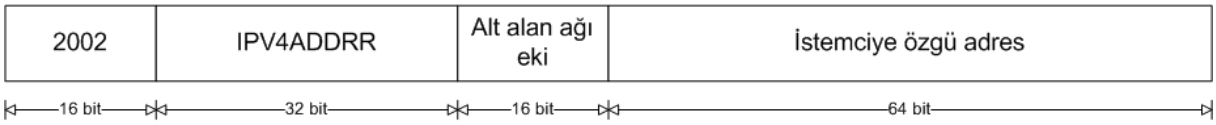
```
netsh interface ip set address "Local Area Connection" static 192.168.0.2 255.255.255.0
192.168.0.1
netsh interface ipv6 set address “Local Area Connection” 2001:db8:1:dede::23
netsh interface ipv6 add route ::/  "Local Area Connection"
```

6to4 Geçiş Yöntemi (Tünelleme)

6to4 geçiş yöntemi, yönlendirici – yönlendirici veya yönlendirici - istemci arasında kurulan tünel ile ağa IPv6 bağlantısı sağlamaktadır. Bu yöntem kullanılarak IPv6 desteği olan ancak yalın IPv6 bağlantısı bulunmayan uçlar IPv6 ağına bağlanabilir. Diğer tünelleme yöntemlerine göre daha çok tercih edilen bir yöntemdir.

6to4 yönteminde; 6to4 istemci, 6to4 yönlendirici ve 6to4 nakledici yönlendirici olmak üzere 3 bileşen bulunmaktadır. 6to4 istemcinin ürettiği IPv6 paketi, 6to4 yönlendiriciler üzerinde IPv4 paketine sarmalanır. IPv4 ağı üzerinden 6to4 nakledici yönlendiriciye ulaşan sarmalanmış paketin sarmalaması açılır ve IPv6 paketi 6to4 nakledici yönlendirici aracılığıyla IPv6 ağına iletilir. Sarmalama ve sarmalama açma işlemleri 6to4 yönlendiricide, 6to4 nakledici (relay) yönlendiricide veya 6to4 istemci/yönlendiricide gerçekleştirilmektedir. 6to4 istemci/yönlendirici, “6to4 Yöntemi Bileşenleri” başlığında anlatılmıştır.

6to4 geçiş yönteminde kullanılan adres yapısı Şekil 21'de verilmiştir. Bu adres yapısında ilk 16 bit, 6to4 öneki (2002) olarak belirlenmiştir. 17. ve 32. bitler arasında, kullanılan 6to4 yönlendiricinin IPv4 adresinin onaltılık düzende gösterimi (IPV4ADDRR) yer almaktadır.



Şekil 21: 6to4 Adres Yapısı

6to4 geçiş yönteminin avantaj ve dezavantajlar aşağıda özetlenmiştir.

Avantajlar:

- Kurulan tünelin kullanımı geçerli oturum sonlandığında biter.
- 6to4 yöntemi kullanan ve yönlendirici ilanlarını kabul ederek otomatik ayarlanabilen bir istemci üzerinde ek herhangi bir ayar yapmaya gerek yoktur.
- 6to4 tünelleri dinamik olduğu için servis sağlayıcı tarafında nakledici yönlendirici yapılandırılması, birden fazla istemcinin bu hizmeti kullanması için yeterlidir.

Dezavantajlar:

- NAT arkasında kalan istemciler, NAT cihazı ile 6to4 yönlendirici aynı cihaz değilse, bu yöntemi kullanamaz.
- 6to4 ağı içerisinde /48 adres bloğu kullanılmaktadır. Bir 6to4 ağında daha fazla adres kullanılamaz.
- Servis sağlayıcılar çok noktadan tek noktaya açılan dinamik tünellerden geçen trafiği takip etmekte zorlanabilir.
- 6to4 IPv6 adres öneki, geçerli IPv4 adresinden türetilmektedir. Bu nedenle yalın IPv6 kullanımına geçildiğinde ağın yeniden adreslenmesi gerekmektedir.

6to4 Yöntemi Bileşenleri

6to4 yönlendirici

6to4 yönlendirici, 6to4 ağı ve IPv4 ağı arasında yer almakta olup, 6to4 istemcilerinden gelen IPv6 paketlerini, IPv4 paketine sarmalar ve IPv4 ağı üzerinden 6to4 nakledici yönlendiriciye iletir.

6to4 yönlendiricinin IPv4 ağına bağlı arayüzüne küresel (yönlendirilebilir) bir IPv4 adresi (IPV4ADDRR) atanmalıdır. Bu adres 6to4 ağına duyurulacak IPv6 adresinin oluşturulmasında kullanılmaktadır.

6to4 yönlendiricinin 6to4 ağına bağlı arayüzüne 2002::/16 önekine sahip 6to4 adresi atanmalıdır. Bu adres 2002:IPV4ADDRR::/48 önekini içermektedir. Bu arayüz ile 6to4 istemcilerin IPv6 adresi alırken kullanacakları önek 6to4 ağına duyurulmaktadır. Örneğin; 6to4 yönlendiricinin IPv4 arayüzünde "172.16.30.193" adresi kullanılmakta ise bu adresin onaltılık düzende gösterimi "ac10:1ec1" şeklindedir. Alt alan ağı ekinin "baba" olduğu durumda 6to4 arayüzünden duyurulacak önek "2002:ac10:1ec1:baba::/64" şeklinde olacaktır.

NOT: 6to4 ağı kurabilmek için IPv4 ağına erişebilen ve küresel IPv4 adresine sahip bir yönlendirici kullanılmalıdır. NAT arkasında yer alan ve sanal IP adresine sahip bir bilgisayar, eğer protokol 41 o bilgisayara yönlendirilmişse bu yöntemi kullanabilir. Bu durumda tek bir istemci kullanılabilir.

6to4 istemci

6to4 istemci, 6to4 yönlendirici tarafından duyurulan 2002:IPV4ADDRR:SUBNETID::/64 önekine sahip IPv6 adresini oluşturur ve kullanır. 6to4 istemci ağa bağlanırken ağ adresini kendisi oluşturur ve varsayılan yönlendirici adresini de yönlendirici ilanı ile otomatik olarak alır. 6to4 ağında, istemci üzerinde herhangi bir sarmalama veya sarmalama açma işlemi yapılmamaktadır.

6to4 istemci/yönlendirici

Bir ağda hem 6to4 istemci hem de 6to4 yönlendirici gibi çalışan cihazlar da bulunabilir. Windows Vista işletim sistemi 6to4 istemci uygulaması istemci/yönlendirici uygulamasına örnek olarak verilebilir. 6to4 istemci/yönlendirici cihazlar 6to4 istemcilerinden farklı olarak sarmalama ve sarmalama açma işlemleri kendi üstlerinde gerçekleştirirler. Başka bir deyişle tünel 6to4 istemci/yönlendirici ile 6to4 nakledici yönlendirici arasında kurulmaktadır.

6to4 nakledici yönlendirici

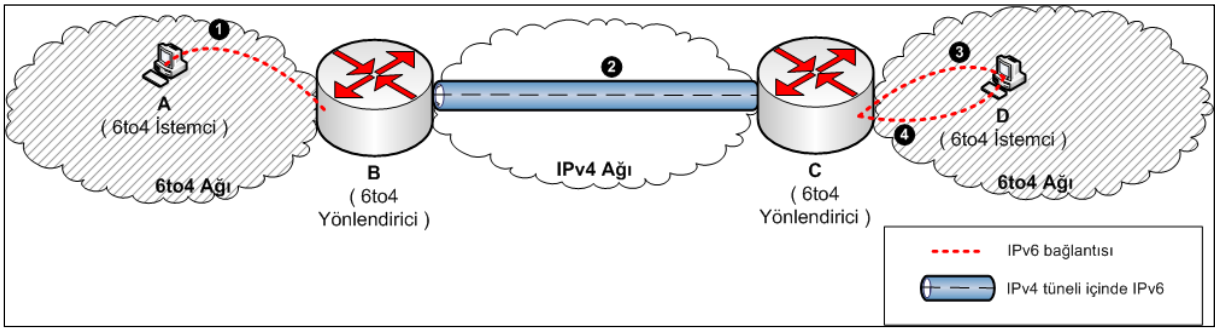
6to4 nakledici yönlendirici, 6to4 ve IPv6 ağları arasındaki iletişim sağlamak için kullanılır. 6to4 nakledici yönlendiricilerde bir adet 6to4 adresine sahip arayüzü ve bir adet IPv6 adresine sahip arayüzü bulunmalıdır.

Nakledici/yönlendirici kullanımı ile ilgili tanımlar RFC 3068'de verilmiştir. RFC 3068 en yakın nakledici yönlendiricinin bulunabilmesi için IPv4 herhangi birine gönderim (anycast) adresi olarak 192.88.99.1 adresinin kullanılmasını önermektedir. 192.88.99.1 herhangi birine gönderim adresinin 6to4 nakledici yönlendirici adresi olarak kullanılması ile 6to4 yönlendiricilerin kendilerine ağ üzerinden en yakın 6to4 nakledici yönlendiricinin adresini bulması amaçlanmıştır. En yakın 6to4 nakledici işletim sistemine göre *traceroute* ya da *tracert* komutu ile tespit edilebilir.

```
[root@R1BSD ~]# traceroute 192.88.99.1
traceroute to 192.88.99.1 (192.88.99.1), 64 hops max, 40 byte packets
 1  172.16.30.17 (172.16.30.17)  0.726 ms  1.827 ms  1.878 ms
 2  172.16.0.157 (172.16.0.157)  0.179 ms  0.157 ms  0.181 ms
 3  172.16.0.14 (172.16.0.14)  0.590 ms  0.563 ms  0.480 ms
 4  172.16.10.250 (172.16.10.250)  6.676 ms  6.746 ms  6.774 ms
 5  62.40.125.153 (62.40.125.153)  17.256 ms  17.203 ms  17.157 ms
 6  62.40.112.193 (62.40.112.193)  29.942 ms  29.899 ms  29.930 ms
 7  62.40.112.41 (62.40.112.41)  37.626 ms  37.580 ms  37.627 ms
 8  62.40.112.38 (62.40.112.38)  45.316 ms  45.470 ms  45.418 ms
 9  62.40.124.34 (62.40.124.34)  47.410 ms  45.773 ms  45.816 ms
10  188.1.145.197 (188.1.145.197)  49.306 ms  49.764 ms  49.210 ms
11  188.1.145.166 (188.1.145.166)  49.413 ms *  49.827 ms
```

6to4 İletişim Örnekleri

İki 6to4 ağının haberleşmesi



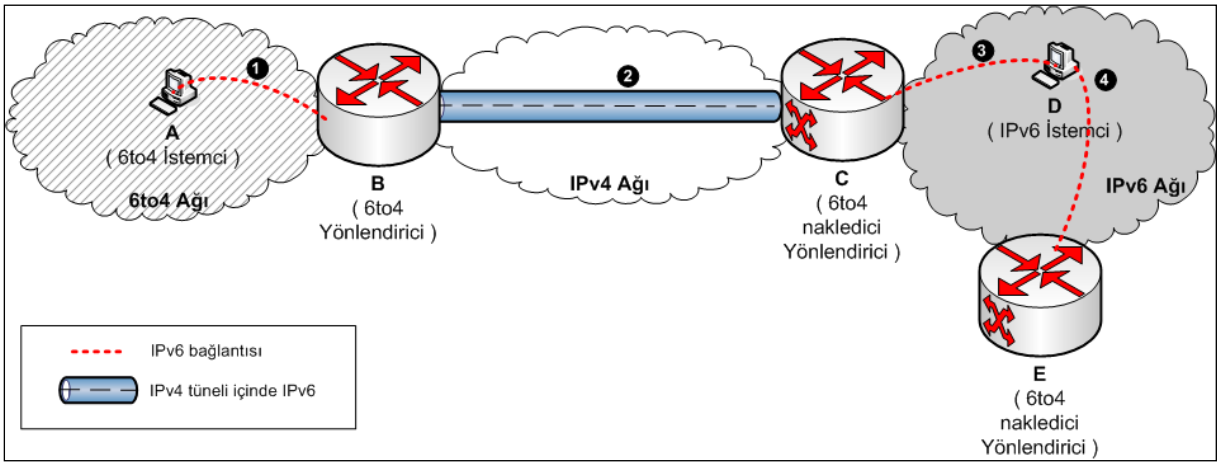
Şekil 22: İki 6to4 Ağının Haberleşmesi

Şekil 22'de iki 6to4 ağının haberleşmesi örnek ağ yapısı üzerinden gösterilmiştir. Bu ağ yapısında farklı 6to4 ağlarında yer alan 6to4 istemcileri A ve D'nin, 6to4 yönlendiriciler B ve C aracılığıyla IPv4 ağı üzerinden haberleşmesinde gerçekleşen aşamalar aşağıda açıklanmıştır.

- **A** , **B**'nin 6to4 arayüzünden gönderdiği yönlendirici ilanı ile 2002::/16 önekine sahip IPv6 adresi ve **B**'nin 6to4 adresini alır.
- A, oluşturduğu IPv6 paketini **B**'ye iletir.
- 6to4 arayüzünden IPv6 paketini alan **B**, IPv6 varış adresinden, IPv4 varış adresini çıkarır. IPv6 paketini IPv4 paketine sarmalar ve sarmalanmış paketi IPv4 arayüzünü kullanarak IPv4 ağına gönderir.
- Sarmalanmış paketi alan **C** paketi açar. IPv6 paketini, 6to4 arayüzünden 6to4 ağına gönderir.
- **D** aldığı IPv6 paketini işler ve aynı yolu kullanarak pakete cevap verir.

6to4 ağının IPv6 ağı ile haberleşmesi

Şekil 23'de verilen örnek ağ yapısında; A'nın (6to4 istemci), D (IPv6 istemci) ile haberleşmesi gösterilmiştir. Bu haberleşmede IPv6 paketinin IPv4 paketine sarmalanması ve IPv4 ağı üzerinden C'ye (6to4 nakledici yönlendirici) iletilmesini, B (6to4 yönlendirici) sağlamaktadır. IPv4 paketine sarmalanmış IPv6 paketinin sarmalamasının açılmasını ve IPv6 paketinin IPv6 ağına iletilmesi C (nakledici yönlendirici) düğümünde gerçekleşmektedir.



Şekil 23: 6to4 Ağının IPv6 Ağı ile Haberleşmesi

Haberleşme esnasında gerçekleşen adımlar aşağıda detaylı olarak açıklanmıştır.

- **A** , **B**'nin 6to4 arayüzünden gönderdiği yönlendirici ilanı ile 2002::/16 önekine sahip IPv6 adresi ve **B**'nin 6to4 adresini alır.
- Oluşturduğu IPv6 paketini **B**'ye iletir.
- 6to4 arayüzünden IPv6 paketini alan **B**, 192.88.99.1 adresini kullanarak en yakın nakledici yönlendiricinin (**C**'nin) IPv4 adresini öğrenir. Tünelin bitiş noktası olarak bu IPv4 adresini kullanır. Başka bir deyişle IPv6 paketini sarmaladığı IPv4 paket başlığındaki varış IPv4 adresi, **C**'nin IPv4 adresidir.
- IPv4 arayüzünden sarmalanmış paketi alan **C**, paketin sarmalamasını açar. IPv6 paketini, IPv6 arayüzünü kullanarak IPv6 ağına gönderir.
- **D** aldığı IPv6 paketini işler. Cevabı kendisine en yakın nakledici yönlendirici (**E**) üzerinden gönderir. En yakın nakledici yönlendirici, paketin gelirken üzerinden geçtiği nakledici yönlendirici olmayabilir.

6to4 istemci/yönlendirici cihazların 6to4 ve IPv6 ağları ile haberleşmesi

6to4 istemci/yönlendirici cihazlarının da 6to4 ağları ve IPv6 ağları ile haberleşmesi 6to4 istemcilerin haberleşmesine benzer şekilde gerçekleşmektedir. 6to4 ağlarının 6to4 ve IPv6 ağları ile haberleşmesi durumlarından farklı olarak sarmalama ve sarmalama açma işlemleri 6to4 yönlendirici yerine, 6to4 istemci/yönlendirici üzerinde gerçekleştirilmektedir.

6to4 Yapılandırması

Bu bölümde IPv4 bağlantısı bulunan uçların 6to4 yöntemini kullanarak diğer 6to4 ağlarına ve IPv6 ağlarına bağlanmaları için yapılandırma bilgileri yer almaktadır.

FreeBSD

FreeBSD işletim sistemi varsayılan ayarlarıyla yönlendirici ilanlarını kabul etmemektedir. 6to4 ağına yerleştirilen FreeBSD istemcinin, otomatik 6to4 adresi alması için, 6to4 yönlendiricinin duyurduğu yönlendirici ilanını kabul etmesi gerekmektedir. FreeBSD işletim sisteminin yönlendirici ilanlarını kabul etmesi için gerekli komut aşağıda verilmiştir.

```
sysctl –w net.inet.ip6.accept_rtadv=1
```

IPv4 ağında yer alan, küresel IPv4 adresine sahip FreeBSD istemcinin 6to4 yöntemini kullanarak IPv6 ağına bağlanabilmesi için istemci/yönlendirici olarak ayarlanması gerekmektedir. Bu, FreeBSD üzerinde tanımlanan tünel arayüzü ile IPv4 paketine sarmalanmış IPv6 paketlerinin 6to4 nakledici yönlendirici üzerinden IPv6 ağına iletilmesi ile gerçekleştirilmektedir. FreeBSD işletim sisteminde tünel kurulumu için komut örneği aşağıda yer almaktadır. Bu örnekte yer alan “172.16.30.211” işletim sisteminin IPv4 adresidir. Bu örnekte 6to4 nakledici yönlendirici olarak en yakın nakledici yönlendiricinin cevap verdiği 192.88.99.1 herhangi birine gönder adresi kullanılmıştır. “2002:c18c:1ed3::1/128” istemciye atanmış 6to4 adresidir. 6to4 adresinde yer alan “c18c:1ed3”, IPv4 adresinin onaltılık tabanda gösterimidir.

```
ifconfig gif0 create
ifconfig gif0 tunnel 172.16.30.211 192.88.99.1
ifconfig gif0 inet6 alias 2002:c18c:1ed3::1/128
route add -inet6 default -interface gif0
```

Linux

6to4 ağına yerleştirilen Linux işletim sitemine sahip istemci, yönlendirici ilanlarını kabul etme özelliği açılmışsa, otomatik olarak 6to4 adresi alacak ve IPv6 ağına bağlanacaktır.

IPv4 ağına yerleştirilen Linux işletim sistemine sahip istemciye IPv6 bağlantısı sağlayabilmek için, işletim sistemine tünel arayüzü tanımlamak gerekmektedir. Tünel arayüzü yapılandırması için gerekli komutlar aşağıda verilmiştir. Bu örnekte 172.16.30.212 istemcinin IPv4 adresidir. IPv4 adresinin onaltılık tabanda gösterimi kullanılarak oluşturulan 2002:c18c:1ed4::1 adresi tünel arayüzüne atanmıştır. Verilen örnek komutların son iki satırı yönlendirme ayarlarını içermektedir. Örnekte IPv6 trafiği (2000::/3) 172.16.30.214 nakledici yönlendiricisine iletilmektedir. Son satırdaki komut kullanılırsa, IPv6 trafiği en yakın nakledici yönlendirici (192.88.99.1) kullanılarak IPv6 ağına iletilecektir.

```
ip tunnel add tun6to4 mode sit remote any local 172.16.30.212 ttl 64
ip link set dev tun6to4 up
ip -6 addr add 2002:c18c:1ed4::1/128 dev tun6to4
ip -6 route add 2000::/3 via ::172.16.30.214 dev tun6to4 metric 1
#ip -6 route add 2000::/3 via ::192.88.99.1 dev tun6to4 metric 1
```

Aşağıda, eski Linux sürümlerinde yer alan "sit0" arayüzü kullanılarak yapılan 6to4 ayarı gösterilmiştir.

```
ifconfig sit0 up
ifconfig sit0 add 2002:9d3c:0001::1570:6000:0001/48
route -A inet6 add 2000::/3 gw ::192.88.99.1 dev sit0
```

Windows XP

Windows XP işletim sistemi yüklü bilgisayarlar 6to4 arayüzünün yapılandırmasını istemcinin küresel IPv4 adresine sahip olduğu fakat doğrudan IPv6 bağlantısına sahip olmadığı durumlarda otomatik olarak gerçekleştirmektedir. Otomatik yapılandırmada tek yapılması gereken 6to4 varsayılan yönlendirici tanımını yapmaktır. Aşağıda gösterilen komut ile, *172.16.30.214* IPv4 adresi varsayılan nakledici yönlendirici olarak tanımlanmaktadır. Statik nakledici yönlendirici yerine, en yakındaki 6to4 nakledici yönlendirici kullanılmak istenirse adres *192.88.99.1* olarak tanımlanmalıdır.

```
netsh int ipv6 6to4 set relay 172.16.30.214
```

Windows Vista / Windows 7

Küresel IPv4 adresine sahip Windows Vista ve Windows 7 işletim sistemleri eğer IPv6 bağlantısına sahip değilse, 6to4 arayüzünü otomatik olarak yapılandırmaktadır. Bu yapılandırmada varsayılan ağ geçidi olarak en yakın 6to4 nakledici yönlendiricinin cevap verdiği 192.88.99.1 (6to4 herhangi birine gönderim adresi) kullanılmaktadır.

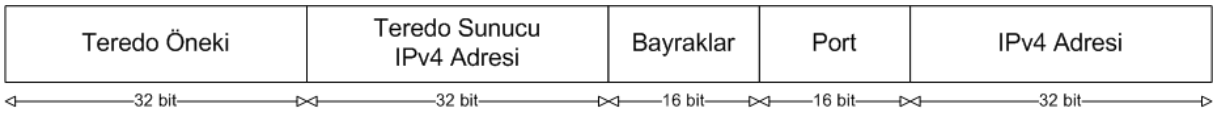
```
netsh int ipv6 6to4 set relay 192.88.99.1
```

Teredo Geçiş Yöntemi (Tünelleme)

Teredo geçiş yöntemi yönlendirici ile istemci arasında kurulan bir tünelleme yöntemidir. Teredo geçiş yönteminin temel amacı NAT veya güvenlik duvarı arkasında kalan istemcilerin IPv6 ağına bağlanmalarını sağlamaktır. Bu yöntemin 6to4 ve ISATAP yöntemlerinin kullanılamadığı durumlarda son çare olarak kullanılması önerilmektedir.

Teredo geçiş yönteminde Teredo sunucu, Teredo istemci ve Teredo nakledici olmak üzere 3 bileşen bulunmaktadır. Tünel, Teredo nakledici ile Teredo istemci arasında kurulmaktadır. Bu yöntemde IPv6 paketi, IPv4 UDP paketine sarmalanarak gönderilmektedir. Bu sayede NAT veya güvenlik duvarı arkasında kalan istemciler de bu tünelleme yöntemi ile IPv6 ağına bağlanabilmektedir.

Teredo yönteminde Şekil 24'te yer alan adres yapısı kullanılmaktadır.



Şekil 24: Teredo adres yapısı

Bu adres yapısında ilk 32 bitlik Teredo öneki *2001::/32* olarak belirlenmiştir. İkinci 32 bitlik bölümde Teredo sunucusuna ait IPv4 adresinin onaltılık düzende gösterimi yer almaktadır. 16 bitlik bayraklar bölümü adres tipini ve NAT yapısını belirtmektedir. Son 48 bit istemciye ulaşacak olan NAT cihazının küresel IPv4 adresini ve istemcinin dinlediği Teredo portuna ulaşacak NAT cihazı portu bilgisini içermektedir. Port bilgisi içeren 16 bitlik bölüm, NAT cihazı port numarası ile FFFFFFFF arasında XOR (Bitsel Özel Veya) işlemi uygulanarak bulunur. Benzer şekilde son 32 bitlik bölüm de NAT cihazının küresel IPv4 adresinin bitlerinin onaltılık düzendeki karşılığı ile FFFFFFFF arasında XOR (Bitsel Özel Veya) işlemi uygulanarak hesaplanır. Teredo istemci üzerinde, kullanılacak Teredo sunucunun adresi tanımlanır ve Teredo istemci IPv6 adresi almak için tanımlanmış Teredo sunucuyu kullanır. Aşağıda bu adres yapısına bir örnek verilmiştir.

Teredo sunucu IPv4 adresi: 65.55.158.116
Onaltılık gösterimi: 41379e74
Teredo istemciye ulaşacak NAT cihazı IPv4 adresi: 172.16.30.213
Onaltılık gösterimi: C18C1ED5
C18C1ED5 XOR FFFFFFFF = 3e73e12a
İstemci Teredo uygulaması portuna ulaşacak NAT cihazı portu: 32767
    Onaltılık gösterimi: 7fff
    7fff XOR FFFF = 8000
Teredo istemci IPv6 adresi. 2001:0:4137:9e74:8000:fb9b:3e73:e12a

NOT: Teredo nakledicinin, istemcinin hangi NAT cihazının arkasında olduğunu bilmesi için NAT cihazının IPv4 adresi ve port numarası IPv6 adresine gömülmüştür. Ancak bazı NAT

cihazları, paketin UDP verisi içinde geçen tüm NAT cihazı küresel IPv4 adreslerini, istemcinin yerel IP adresi ile otomatik olarak değiştirmektedir (SIP veya H.323). Bu şekilde bir değiştirme ile nakledici, NAT cihazının küresel IPv4 adresine erişemeyecektir. Bu kaybı engellemek için küresel IPv4 adresi ve port numarası IPv6 adresi içine gömülürken XOR işlemine tabi tutulmaktadır.

Teredo Yöntemi Bileşenleri

Teredo Nakledici

Teredo nakledici, Teredo istemci ile IPv6 ağı arasındaki bağlantıyı sağlamaktadır. Teredo nakledici IPv6 yönlendirme protokollerini kullanarak Teredo önekini *2001::/32* IPv6 ağına duyurur, ilişkili Teredo sunucu ile iletişim kurar ve 2001::/32 ağına gelen trafiği tünelleyerek ilgili Teredo istemcisine gönderir.

Teredo Sunucu

Teredo sunucu, kendisi ile ilişkilendirilmiş Teredo istemcisinin NAT arkasında olup olmadığını, eğer NAT arkasında ise hangi yapıda bir NAT arkasında olduğunu tespit eder. Buna göre istemciye, içinde kendi IPv4 adresi, NAT cihazının IPv4 adresi ve port bilgisinin bulunduğu bir adres atar. Teredo sunucusu, NAT ve/veya güvenlik duvarı arkasındaki istemciyi durumdan haberdar ederek istemci ile Teredo nakledici arasındaki iletişimi başlatır. Aynı zamanda istemciye belirli aralıklarla UDP paketleri göndererek istemci ile iletişiminin devam ettiğini doğrular.

Ağ yöneticileri, ağın izlenebilirliğini sağlamak üzere ağlarında kendi Teredo sunucularını kurmayı tercih edebilirler. Ancak bu durumda güncel Windows işletim sistemi kullanan istemciler üzerinde otomatik yapılandırma kullanılmayıp, yerel Teredo sunucusu kullanılacak şekilde elle yapılandırılmaları gerekir.

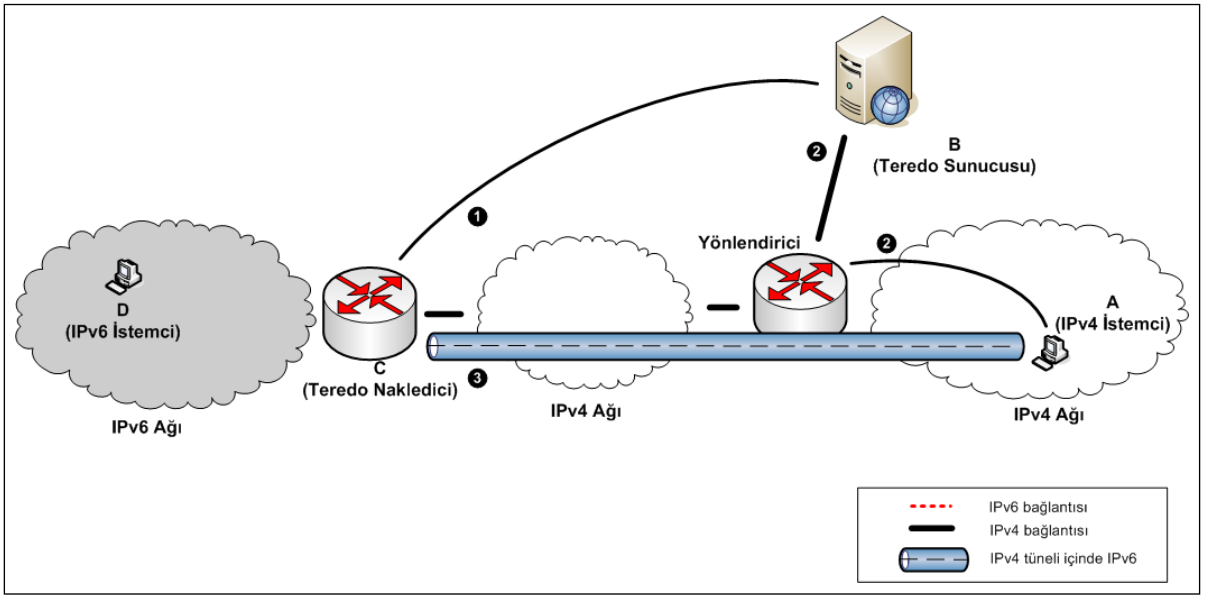
Teredo İstemci

Teredo istemci, küresel IPv4 adresi bulunmayıp NAT ve/veya güvenlik duvarı arkasında yer alan bir cihazdır. Teredo istemcinin IPv6 ağına bağlanırken kullanacağı Teredo sunucu ayarlanmalıdır (NAT arkasındaki güncel Windows işletim sistemine sahip istemciler otomatik olarak teredo.ipv6.microsoft.com adresinde yer alan Teredo sunucusunu kullanmaktadır.) Teredo istemci, Teredo sunucusu aracılığıyla aldığı IPv6 adresini kullanarak Teredo nakledici üzerinden IPv6 ağına bağlanır.

Teredo İletişim Örnekleri

Teredo Nakledicinin/IPv6 İstemcinin Teredo İstemciyle Haberleşmesi

Bir Teredo istemci, Teredo sunucusu aracılığıyla kendisine Teredo önekiyle başlayan bir IPv6 adresi aldıktan sonra, Teredo nakledici ile istemci arasında tünel kurulum aşamaları Şekil 25'te gösterilmiştir. C (Teredo nakledici) NAT yapısını öğrenmek ve NAT arkasındaki A ile iletişim kurabilmek için B (Teredo sunucu) ile haberleşir. Sonuçta Teredo nakledici ve Teredo istemci arasında tünel kurulumu gerçekleşir. Adımlar aşağıda daha detaylı bir şekilde anlatılmıştır.



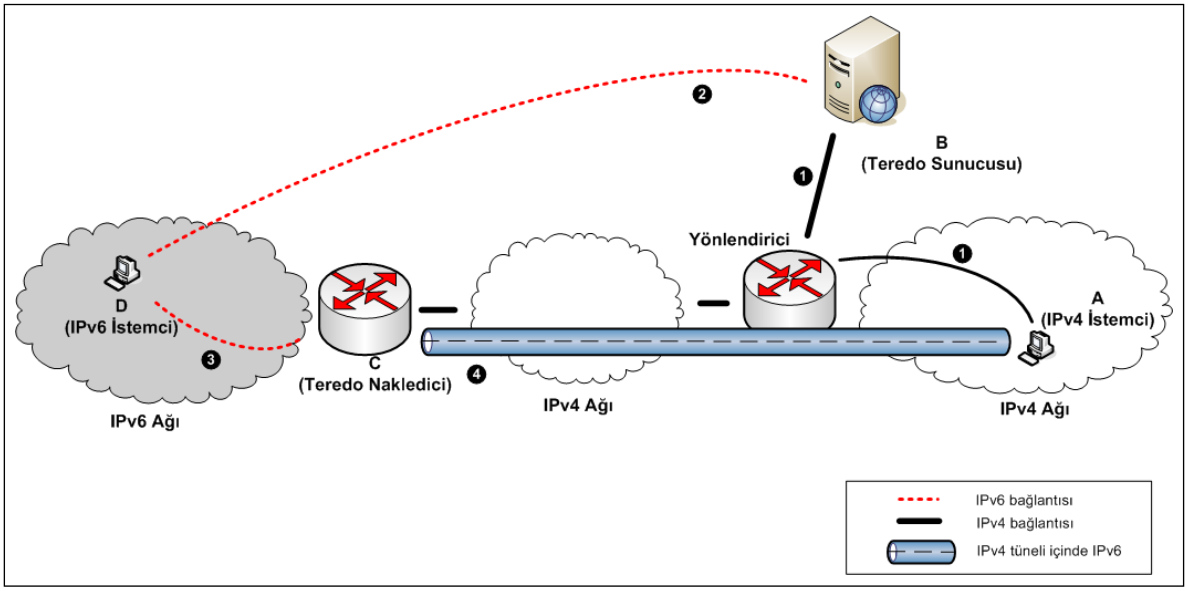
Şekil 25: Teredo nakledicinin/istemcinin Teredo istemciye IPv6 paketi göndermesi

1. C Teredo nakledicisi; istemci A'ya IPv6 paketi göndereceği zaman, öncelikle A'nın IPv6 adresinden A'nın ilişkili olduğu Teredo sunucusunun IPv4 adresini öğrenir. C, NAT yapısını öğrenmek için B'ye IPv6 balon paketi gönderir.
2. Teredo Sunucusu B, kendisine gelen balon paketi A'ya iletir.
3. Böylece NAT arkasındaki A Teredo istemcisi ile C Teredo nakledicisi arasında tünel kurulur.

Balon (Bubble) paketleri, Teredo istemciler ve Teredo nakledici̇ler tarafından NAT yapısını öğrenmek amacıyla kullanılan ve sadece IPv6 başlığı ile boş veri kısmı içeren IPv6 paketleridir.

Bu iletişimde kritik nokta, A'nın durum denetimli (stateful) cihazların (NAT, güvenlik duvarı vs.) arkasında olmasıdır. Bu durumda C ile A arasında iletişim sağlanabilmesi için A'nın durum bilgisi tutan cihazlarda oturum bilgisi oluşturması gerekir. Bu durum "hole punching" olarak adlandırılmaktadır.

Teredo İstemcinin IPv6 İstemci ile Haberleşmesi



Şekil 26: Teredo istemcinin IPv6 istemci ile haberleşmesi

IPv4 ağındaki A Teredo istemcisi, D IPv6 istemcisi ile bağlantı kurmak istediğinde kullanılacak Teredo nakledicinin IPv4 adresini ve port numarasını öğrenmek için B Teredo Sunucusunu kullanır. Şekil 26'da verilen ağ yapısında A'nın D ile iletişiminde gerçekleşen adımlar aşağıda belirtilmiştir.

1- A, hedef IPv6 adresi D olan bir ICMPv6 Echo Request paketi (ping6) oluşturur. Bu paketi IPv4 paketine sarmalar ve Teredo sunucusu üzerinden yollar.

2- B, kendine gelen IPv4 paketinin sarmalamasını açar. Sarmalamayı açarak, ICMPv6 paketini D'ye iletir.

3- D, kendisine gelen pakete cevap olarak ICMPv6 Echo Reply paketi oluşturur ve kendisine en yakın Teredo Nakledici ile bu paketi gönderir.

4- C Teredo nakledicisi, bir önceki bölümde anlatılan şekilde A'nın IPv4 adresini bularak, A ile kendi arasında IPv4 tüneli oluşturur ve paketi iletir.

Teredo Yapılandırması

Bu bölümde farklı işletim sistemleri için Teredo yapılandırmasına yer verilmiştir. Ayrıca FreeBSD ve Linux işletim sistemlerinde kullanılan açık kaynak kodlu Teredo uygulaması Miredo'nun yapılandırılması anlatılmıştır.

Miredo

Miredo uygulaması, FreeBSD sürüm 5.5'ten itibaren ve Linux (çekirdek 2.4 ve 2.6) işletim sistemleri ile çalışmaktadır. Miredo uygulaması kullanılarak bir bilgisayar, Teredo istemci,

nakledici veya sunucu olarak yapılandırılabilir. Her üç durum için de Linux kullanılıyorsa TUNTAP ve IPv6 çekirdek modülleri yüklenmiş olmalıdır. Performans artırımı için Miredo'nun kullandığı dinamik kütük kütüphanesi Judy'nin de kurulması önerilmektedir. FreeBSD portlarından kurulum yapıldığında Judy otomatik olarak yüklenmektedir.

Teredo Nakledici Yapılandırılması

Teredo nakledici küresel bir IPv4 ve IPv6 adresine sahip olmalıdır. Arayüzler arası paket iletimi açılmış olmalıdır. FreeBSD için arayüzler arası IPv4 ve IPv6 paketlerinin iletilmesini aktif hale getirmek için gerekli komutlar aşağıda belirtilmiştir.

```
sysctl –w net.inet.ip.forwarding=1
sysctl –w net.inet6.ip6.forwarding=1
```

/usr/local/etc/miredo/miredo.conf dosyasının örnek içeriği aşağıda verilmiştir. Bu ayar dosyasında yer alan DIR_IPv4_PUBLIC, Teredo nakledicinin küresel IPv4 adresini temsil etmektedir. *Prefix* parametresi ile *2001:: /32* öneki Teredo istemcilerine duyurulmaktadır.

```
RelayType relay
InterfaceName teredo
BindAddress DIR_IPv4_PUBLIC
BindPort 3545
Prefix 2001:0::
InterfaceMTU 1280
```

Teredo Sunucu Yapılandırması

Teredo sunucusu, NAT mimarisini tanımlayabilmek için kullanılan, iki tane küresel IPv4 adresine sahip olmalıdır. Bu iki IPv4 adresinin ardışık olması önerilmektedir. İki IPv4 adresi aynı arayüz üzerinde veya iki farklı arayüz üzerinde tanımlanabilir. Teredo sunucusuna bir adet IPv6 adresi atanmalı ve Teredo sunucusunun IPv6 bağlantısı sağlanmalıdır.

Miredo uygulaması, Teredo sunucu kurmak için kullanıldığında */usr/local/etc/miredo/miredo-server.conf* dosyası aşağıda verilen satırları içermelidir. DIR_IPv4_PUBLIC_1 ve DIR_IPv4_PUBLIC_2 Teredo sunucunun sahip olduğu küresel IPv4 adreslerini temsil etmektedir.

```
Prefix 2001:0::
InterfaceMTU 1280
ServerBindAddress DIR_IPv4_PUBLIC_1
ServerBindAddress2 DIR_IPv4_PUBLIC_2
```

Son adım olarak */usr/local/sbin/miredo-server* komutu root kullanıcısı ile çalıştırılarak Teredo sunucusu çalıştırılır.

Teredo İstemci Yapılandırması

FreeBSD ve Linux

FreeBSD ve Linux işletim sistemlerinin Teredo istemci olarak çalışması için Miredo kullanılabilir. Miredo kurulumu ile ilgili bilgiler Teredo Yapılandırması başlığı altında verilmiştir.

Miredo kurulduğunda varsayılan yapılandırma dosyası */usr/local/etc/miredo/miredo.conf* teredo istemci modunda, Teredo sunucusu olarak *teredo.remlab.net* sunucusunu kullanacak şekilde yapılandırılmıştır. Varsayılan sunucu, *ServerAddress* parametresi ile değiştirilebilir.

Windows XP

Windows XP işletim sistemi kullanan istemciler için Teredo sunucusu aşağıdaki gibi tanımlanır.

```
nets hint ipv6 set teredo client teredo_server refresh_interval client_port
```

Verilen komutta yer alan değişkenlerin temsil ettiği değerler aşağıda açıklanmıştır:

- teredo_server: Kullanılacak Teredo sunucusu.
- refresh_interval: Saniye cinsinden istemci güncelleme aralığı.
- client_port: Teredo istemci tarafından kullanılacak port numarası.

İstemcinin Microsoft'un Teredo sunucusunu kullanacak şekilde yapılandırılması için kullanılan komut aşağıda yer almaktadır.

```
netsh int ipv6 set teredo client teredo.ipv6.microsoft.com
```

Not: Windows XP SP3 üzerinde yapılan testlerde, Teredo arayüzü ve Teredo sunucu yapılandırılması öncesinde 6to4 arayüzü kullanım dışı bırakılmalıdır.

Windows Vista / Windows 7

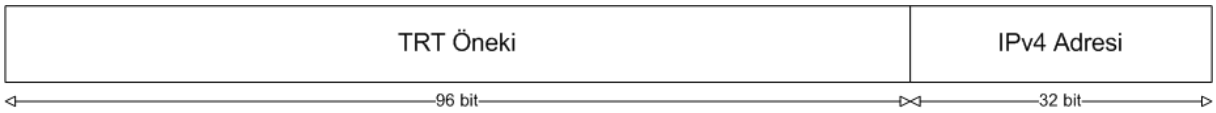
IPv6 bağlantısına sahip olmayan ve sanal IPv4 adresine sahip Windows Vista ve Windows 7 işletim sistemleri Teredo arayüzünü otomatik olarak yapılandırmaktadır. Varsayılan Teredo sunucusu olarak *teredo.ipv6.microsoft.com* adresi ayarlanmaktadır. Bu sunucu ile ilişkilendirilmiş IPv6 adresi istemciye otomatik olarak atanmaktadır. Bu sunucudan farklı bir Teredo sunucusu kullanılmak istenirse aşağıdaki komut kullanılabilir.

```
netsh int ipv6 set teredo client teredo.ipv6.net.tr
```

TRT (Transport Relay Translator) Geçiş Yöntemi (Çeviri)

TRT (Transport Relay Translator) geçiş yöntemi, OSI referans modeli taşıma (transport) katmanında çalışan bir çeviri yöntemidir. IPv6 desteği verilememiş IPv4 cihazlara (örneğin IPv4 web sunucuları) IPv6 protokolünü kullanarak erişmek için kullanılması planlanmıştır.

TRT yöntemini kullanan bir ağda 3 bileşen yer almaktadır. Bunlar IPv6 istemci, IPv4 istemci ve TRT yönlendiricidir. IPv6 ağından IPv4 ağına iletişim sağlamak için TRT IPv6 öneki belirlenerek TRT yönlendiricide çalışan uygulama üzerinde yapılandırılmalıdır. IPv6 ağında bu öneki içeren adrese giden trafik TRT yönlendiriciye iletilmelidir. Bu amaçla, IPv6 ve IPv4 istemciler üzerinde adres ve ağ geçidi yapılandırmasından sonra, TRT öneki için yönlendirme ayarları da yapılmalıdır. Yalın IPv6 istemci, TRT IPv6 önekinin sonuna erişmek istediği IPv4 istemcisinin adresini ekler. TRT yönlendirici, TRT önekine sahip paketleri bir istemciden alır, diğer istemciye yeni bir TCP/UDP bağlantısı açar ve çevrilecek protokolün başlığını paket verisine ekleyerek gönderir. TRT geçiş yönteminde kullanılan adres yapısı Şekil 27'de gösterilmiştir.



Şekil 27 TRT adres yapısı

TRT yönteminin avantaj ve dezavantajları aşağıda belirtilmiştir.

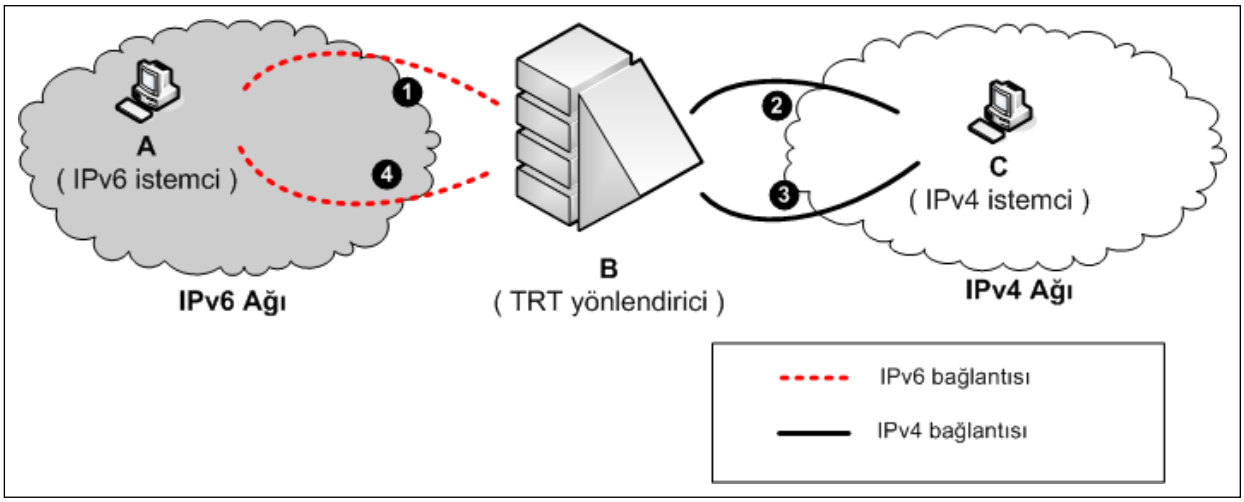
Avantajları

- Yalın IPv6 ve yalın IPv4 kullanan uçlarda ek bir ayarlama gerekmemektedir.
- IPv6 'dan IPv4'e başlık çevirme prensibi ile çalışan çevirme yöntemleri pathMTU ve parçalama işlerini gerçekleştirmelidir. TRT yöntemi bir üst katmanda gerçekleştiği için bu durum söz konusu değildir.

Dezavantajları

- TRT durum bilgisini tutan bir sistemdir. TRT yönlendirici üzerinde o an haberleşen uçların bilgisini tutmaktadır. İki ucun oturumu tek bir TRT yönlendiricisi üzerinden gerçekleşmektedir. Bu da TRT yönlendiricisini tek noktada arıza tehdidine karşı açık hale getirmektedir.
- Paket başlığı değiştiği için IPsec ile uçtan uca güvenlik ve doğrulama yöntemleri TRT ile kullanılamamaktadır.

TRT Ağ Yapısı



Şekil 28: TRT ağ yapısı

Yalın IPv6 ve yalın IPv4 iki istemcinin TRT yönlendiricisi aracılığıyla haberleşmesi Şekil 28'deki örnek ağ yapısı üzerinden anlatılmıştır:

1- A, oluşturduğu IPv6 paketini hedef adresine (TRT öneki + C'nin IPv4 adresi) gönderir. Örneğin: TRT ağında 2001:db8:13:eeee::/96 kullanıldığı durumda "172.16.30.219" adresli IPv4 istemciye bağlantı kurmak isteyen IPv6 istemcisi, veri paketlerini 2001:db8:13:eeee::172.16.30.219 hedef adresine gönderir.
2- TRT önekini içeren paketi alan B, oturumu tutar ve IPv4 ağına yeni bir oturum açar. IPv6 ağından gelen paketi, yeni başlığı ile IPv4 ağına iletir.
3- C, kendisine gelen IPv4 paketini alır ve cevabını B 'ye gönderir.
4- B, önceki durum bilgisine göre gelen paketi daha önceden açılmış oturum aracılığıyla A 'ya gönderir.

Faithd Yapılandırması

Faithd BSD işletim sistemleri için yazılmış bir TRT çeviri yöntemi uygulaması olup, IPv6 ile IPv4 istemciler arasında TCP bağlantılarının yönlendirilmesini sağlar.

IPv4 ile IPv6 ağları arasında çeviri yapmak için FreeBSD işletim sisteminde *faith* sanal arayüzü kullanılmaktadır. *faith* arayüzünün aktif olması için çekirdekte aşağıda belirtilen satır yer almalıdır.

```
device          faith           # IPv6-to-IPv4 relaying (translation)
```

Faithd uygulaması, *faith* arayüzüne gelen TRT önekine sahip trafiği dinler ve protokoller arasında yönlendirilmesini sağlar.

Aşağıda yer alan satırlar "/etc/rc.local" dosyasına eklenmelidir. Bu ayarlar ile yönlendirme tablosunun bozulmaması için yönlendirme ilanı kabulü opsiyonu kapatılmakta; arayüzler arası IPv6 paketi iletimi açılmakta ve faith arayüzü aktif hale getirilmektedir.

```
/sbin/sysctl net.inet6.ip6.accept_rtadv=0
/sbin/sysctl net.inet6.ip6.forwarding=1
/sbin/sysctl net.inet6.ip6.keepfaith=1
```

"/etc/rc.conf" dosyasında faith arayüzü için çeviri öneki tanımlanmalıdır.

```
#### faith ara yuzu ayarlari
ipv6_faith_prefix="2001:db8:13:eeee::"
```

Faith öneki tanımlandıktan sonra bu öneke sahip trafik, TRT yönlendiricisine yönlendirilmelidir.

Önek tanımı yapıldıktan sonra hangi protokollerin çevirisinin yapılacağı belirlenmelidir. Çevirisi yapılacak protokolleri belirtmek için iki yöntem bulunmaktadır.

Yöntem 1: "faithd" çevrilecek olan protokol için manüel olarak çalıştırılır. Bu aşağıda yer alan satırların "/etc/rc.local" veya "/usr/local/etc/rc.d/faithd.sh" benzeri bir başlangıç betiğine eklenmesi ile gerçekleştirilebilir.

```
/usr/sbin/faithd http                              # http trafigini çevirir
/usr/sbin/faithd ftp /usr/libexec/ftpd ftpd -l     # yönlendirilmemiş FTP trafiğini çevirir
```

Yöntem 2: Bu yöntemde ise çevrilecek protokol "/etc/inetd.conf" dosyasına içine yazılır. Bu yöntem için örnek satır aşağıda belirtilmiştir.

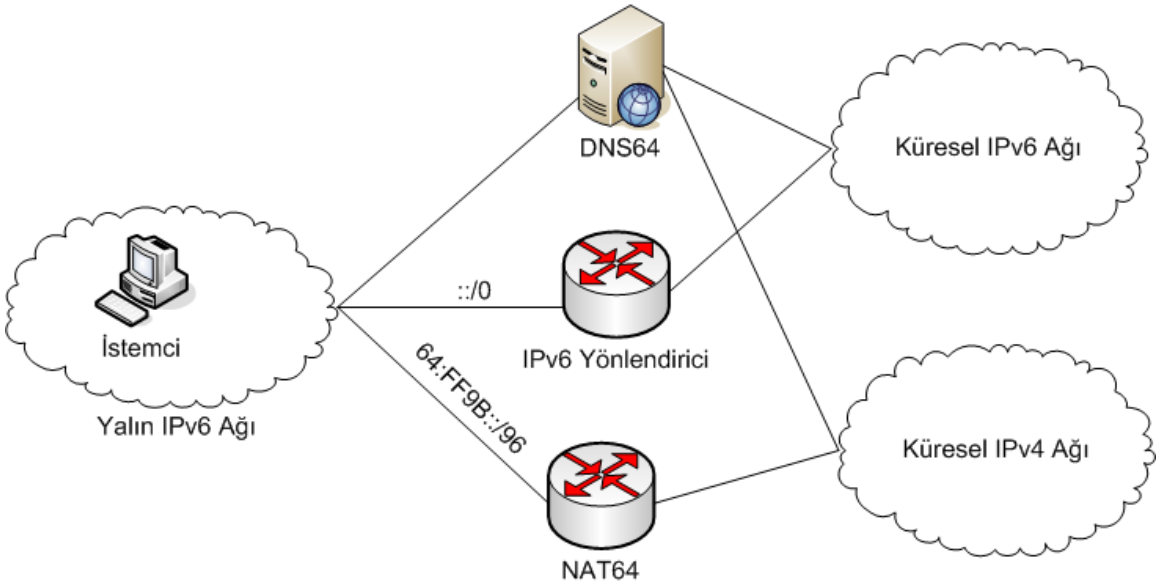
```
ftp    stream  tcp6/faith  nowait  root  /usr/sbin/faithd  ftpd -l
```

NAT64/DNS64 Yöntemi (Çeviri)

Geçiş sürecinde IPv6 bağlantısı sağlanamayan IPv4 sunuculara erişim sağlamak için çeşitli çeviri yöntemleri önerilmiştir. Bu yöntemlerden bir tanesi de paket başlığı bazında çeviri yapan NAT64 yöntemidir. Bu yöntem NAT64 ve DNS64 olmak üzere iki bileşen içermektedir. DNS64 AAAA kaydı olmayan alan adları için belirlenen öneki kullanarak AAAA kaydı

döndürmektedir. DNS64 ile kullanılan öneki içeren paketler NAT64 cihazına yönlendirilir ve burada paketlerin IPv6 – IPv4 çevirimi gerçekleştirilir.

Şekil 29'da NAT64/DNS64 kullanımı gösterilmiştir. Yalın IPv6 ağında yer alan istemci IPv4 ağında yer alan bir sunucuya ulaşmak istediğinde, IPv4 sunucunun AAAA kaydını DNS64 sunucusuna sormaktadır. IPv4 sunucunun AAAA kaydı olmadığı için DNS64 sunucusu belirlenen önek ile bir IPv6 adresi üretir ve cevap olarak döndürür. Varsayılan olarak 64:FF9B::/96 öneki kullanılmaktadır. Bu önek NAT64 çeviri cihazına yönlendirilmektedir. Bu aşamadan sonra iletişim NAT64 cihazı üzerinden devam etmektedir.



Şekil 29: NAT64/DNS64 Kullanım Örneği

NAT64/DNS64 yöntemi uygulaması Ecdysis projesi (http://ecdysis.viagenie.ca) kapsamında yazılan betikler ve yamalar ile kullanılabilmektedir. Ecdysis web sayfasında verilen yamalar kullanılarak Unbound ve Bind açık kaynak kodlu DNS sunucuları, DNS64 sunucusu olarak ayarlanabilmektedir. Ayrıca yine proje sayfasında verilen perl betiği kullanılarak DNS64 uygulaması çalıştırılabilir. Proje kapsamında yazılmış Linux çekirdek modülü veya OpenBSD pf yaması kullanılarak NAT64 çevirici çalıştırılabilmektedir.

DNS64 DNS ALG

Ecdysis projesi kapsamında DNS64 uygulaması 3 farklı yöntem ile kullanılabilmektedir.

dns64.pl Perl Betiği: DNS64 olarak çalışacak sunucu üzerinde çalıştırılacak bu betik 53 numaralı porta gelen UDP paketlerini dinlemektedir. Betik bu porta gelen DNS sorgularını varsayılan DNS sunucusuna (örneğin /etc/resolv.conf dosyasında belirtilen) sormaktadır. Dönen cevap AAAA kaydı içermiyor ve A kaydı içeriyorsa, betik dönen A kaydına (a.b.c.d şeklinde bir IPv4 adresi) belirlenen DNS64 önekini eklemektedir (örneğin 64:FF9B::a.b.c.d).

Sonuçta oluşan adresi ulaşılmak istenen IPv4 sunucunun IPv6 adres kaydı olarak istemciye dönmektedir.

Ubuntu 10.10-server üzerinde yapılan testlerde betiğin çalışması için libio-socket-inet6-perl, libnet-dns-perl, libnetaddr-ip-perl paketlerinin kurulmasının gerekli olduğu görülmüştür. Ek olarak betiğin 53 numaralı portu dinleyebilmesi için root kullanıcısı ile çalıştırılması gerekmektedir.

Betik içinde "my $PREF64 = "64:FF9B::/96";" satırı değiştirilerek DNS64 öneki ayarlanabilmektedir. Bu önekin /96 veya daha kısa bir ağ maskesine sahip olması gerekmektedir. Betik varsayılan olarak sistemde tanımlanan DNS sunucuları kullanmaktadır. Kullanılan DNS sunucuları betik içinde yer alan "my @NAMESERVERS = qw(2001:afaf::301 192.168.10.10);" satırı ile düzenlenebilmektedir.

Dns64.pl betiği içinde gerekli ayarlamalar yapıldıktan sonra aşağıda gösterildiği şekilde çalıştırılıp test edilebilir. Test için AAAA kaydı olmayan bir alan adı kullanılmalıdır. Sonuçta dönen cevabın AAAA kaydı bölümü önek ve IPv4 sunucu adresini içerecektir.

```
# ./dns6to4.pl &
# dig @localhost kazan.ulakbim.gov.tr AAAA
....
;; ANSWER SECTION:
kazan.ulakbim.gov.tr.   3600    IN      AAAA    64:ff9b::c18c:5324
```

Betik yavaş çalışmakta ve birden fazla isteği aynı anda işleyememektedir. NAT64/DNS64 yöntemi deneme amaçlı çalıştırıldığında kullanılabilir.

Bind: Bind uygulaması DNS64 yaması ile veya yamalanmış Bind kaynak kodu Ecdysis web sayfasından indirilip derlenerek DNS64 sunucusu olarak çalıştırılabilmektedir. Bind uygulaması kurulduktan sonra ayar dosyasında (named.conf veya named.conf.options) DNS64 öneki ayarlanmalıdır. Örnek aşağıda gösterilmiştir. Önek ağ maskesi /96 veya daha kısa olmalıdır.

```
options {
   dns64-prefix 64:FF9B::/96;
}
```

Bind uygulaması için gerekli ayarlamalar yapıldıktan sonra bind uygulaması çalıştırılıp, AAAA kaydı olmayan bir alan adı için sorgu gönderilerek uygulama test edilebilir. Örnek uygulama aşağıda verilmiştir.

```
# named -c /etc/bind/named.conf
# dig @localhost kazan.ulakbim.gov.tr AAAA
…
;; ANSWER SECTION:
kazan.ulakbim.gov.tr.   3527    IN      AAAA    64:ff9b::c18c:5324
```

Unbound: Unbound uygulaması DNS64 yaması ile veya yamalanmış Unbound kaynak kodu Ecdysis web sayfasından indirilip derlenerek DNS64 sunucusu olarak çalıştırılabilmektedir. Unbound uygulamasında DNS64 özelliğini aktifleştirilmesi için unbound.conf dosyasında "*module-config*" ve "*dns64-prefix*" değerleri ayarlanmalıdır. "*module-config*" özelliği değeri "*dns64*" ile başlamalıdır. Ayar dosyasında "*dns64-prefix*" değeri ile DNS64 öneki tanımlanmalıdır. İki ayar örnek aşağıda verilmiştir. DNSSEC kullanılmıyor ise "*module-config*" özelliğinde yer alan "*validator*" değeri kaldırılabilir. Önek için belirtilen ağ maskesi /96 veya daha kısa olmalıdır.

```
module-config: "dns64 validator iterator"
dns64-prefix: 64:FF9B::/96
```

Unbound uygulaması için gerekli ayarlamalar yapıldıktan sonra Unbound uygulaması çalıştırılıp, AAAA kaydı olmayan bir alan adı için sorgu gönderilerek uygulama test edilebilir. Örnek uygulama aşağıda verilmiştir.

```
# unbound -c unbound.conf
# dig @localhost kazan.ulakbim.gov.tr AAAA
…
;; ANSWER SECTION:
kazan.ulakbim.gov.tr.   3527    IN      AAAA    64:ff9b::c18c:5324
```

NAT64 IP Çevirici

NAT64 IP çeviricisi Ecdysisi projesi kapsamında TCP, UDP ve ICMP paketlerini IPv6 – IPv4 protokolleri arasında çevirecek şekilde yazılmıştır. NAT64 çevirici Linux kernel modülü veya OpenBSD pf kullanılarak uygulanabilir. Çalışan linux ve Fedora RPM paketleri ile uygulanmış NAT64 yöntemlerine Ecdysis web sitesi üzerinden erişilebilir.

Linux Modülü: Linux modülünün çalıştırılabilmesi için çekirdek versiyonu 2.6.31 veya daha yüksek olmalıdır. Ecdysis web sitesinden çekirdek modülü indirilerek derlenmelidir.

```
# make
# make install
```

Ubuntu 10.10 server üzerinde Linux modülü derlendikten sonra "*depmod -a*" komutu çalıştırılarak modül listesinin güncellenmesi gerekmektedir.

Modül derlendikten sonra "*nat64-config.sh*" dosyası değiştirilerek kullanılacak IPv4 adresi, NAT64 öneki ve NAT64 öneki ağ maskesi ayarları yapılabilir. NAT64 uygulaması "*nat64-*config.sh" betiğine kullanılacak IPv4 adresi belirtilerek çalıştırılabilir.

```
# ./nat64-config.sh 10.10.10.1
```

Betik çalıştırıldığında çekirdek modülünü aktif hale getirecek, NAT64 arayüzünü oluşturacak, NAT64 öneki için gerekli yönlendirme bilgisini yönlendirme tablosuna ekleyecek ve IPv4, IPv6 paket iletme özelliklerini açacaktır.

OpenBSD PF: pf uygulamasına NAT64 desteği, Ecdysis web sitesinde yer alan çalıştırılabilir dağıtım veya kaynak kodlarını içeren dağıtım kullanılarak yaılabilir. Çalıştırılabilir dağıtım kullanıldığında, "install.sh" betiği çalıştırılmalıdır. Bu betik çekirdek, pfctl, systat, tcpdump araçlarını güncellemekte ve eski sürümlerini ".old" uzantısı ile yedeklemektedir. Kaynak kodu içeren dağıtım kullanıldığında OpenBSD derleme ve yükleme işlemleri gerçekleştirilmelidir. Pf'e NAT64 desteği verildikten sonra Tablo8'de verilen satır pf ayar dosyasına (örn: /etc/pf.conf) eklenmelidir. PREFIX değişkeni, kullanılacak NAT64 öneki (örn: 64:FF9B::/96) olarak tanımlanmalıdır. a.b.c.d yerine kullanılacak NAT64 IPv4 adresi yazılmalıdır. NAT64 paketleri için bu kuraldan başka kural eklenmesi tutarlı olmayan sonuçlar verdiği için önerilmemektedir.

```
nat64 from any to PREFIX -> a.b.c.d
```

Karşılaşılan Problemler

Çeviri yöntemi olan NAT64/DNS64 kullanımında bazı problemlerle karşılaşılmaktadır.

- DNS64 kullanımı ile DNSSec kullanımının uyumlu olmadığı durumlar bulunmaktadır. Eğer DNSSec doğrulamasını istemci gerçekleştiriyor ve istemci DNS64 uygulamasından haberdar değilse, AAAA kayıtlarındaki IP adresleri önek ile üretildiği için doğrulanamayacaktır. İstemci DNS64 uygulamasından haberdar ise ve gelen AAAA kaydını A kaydına çevirip doğrulamayı gerçekleştirise bu problem düzeltilebilmektedir. Bir diğer çözüm ise DNSSec 'in istemci yerine DNS sunucusunda gerçekleştirilmesidir. DNS64 sunucusu AAAA kaydını üretmeden önce doğrulama yapacağından belirtilen problem ile karşılaşılmayacaktır.
- Web sayfalarında bulunan ve IP adresi kullanılarak verilen bağlantılara erişilememektedir.
- DNS64 yaması, AAAA kaydına boş cevap dönen sorgular için öneki kullanarak AAAA kaydı üretmektedir. Eğer bir alan adı sorgusuna hata mesajı dönüyorsa DNS64 bu adres için AAAA cevabını IPv6 istemcisine dönememektedir.

Paket veri kısmında IPv4 adreslerini taşıyan (FTP, SIP vb.) ve kendi protokolüne sahip uygulamalar bu yöntem ile çalışmamaktadır.

BÖLÜM 5: GÜVENLİK DUVARI VE IPV6

Yeni nesil internet protokolü IPv6 tasarımında kolay kurulabilme, otomatik adres yapılandırması, geniş adres aralığı gibi kullanımını çekici kılacak özellikler barındırmaktadır. IPv6 ile birlikte adres verilebilecek uç sayısının artması, başlık yapısının sadeleştirilmesi, ara düğümlerde paket parçalanmasına izin verilmemesi gibi özellikler IPv6'nın IPv4'e oranla daha güvenli olarak değerlendirilmesini sağlamıştır. IPv6'nın "güvenli" bir protokol olarak nitelendirilmesi, IPsec ile olmuştur. IPv6 tasarlanırken zorunlu tutulması planlanan IPsec desteği sayesinde her bir veri paketi şifrelenerek iletilebilecek, SSL gibi uygulamaların aksine transport seviyesinde şifreleme yapılabilecekti. Uygulamalara IPsec desteğinin verilmesini gerektiren bu tasarım, gerçek dünyada uygulamalardan yeterli destek görememiş, VPN uygulaması halini almıştır. Sonuç olarak IPv6 için tasarlanan IPsec, IPv4 için de kullanılan bir opsiyonel özellik halini almış, IPv6 için bir güvenlik avantajı olmaktan çıkmıştır.

Internet Protokolü'nün doğası gereği IPv4'te de var olan güvenlik zaafiyetlerinin yanısıra, IPv6 tasarımı ile yeni güvenlik zaafiyetleri de oluşmuştur. SQL enjeksiyonu, kullanılan servis yazılımının açıkları, şifresiz iletişim ile üçüncü kişilerce verilerin ele geçirilmesi, dağıtık servis dışı bırakma saldırıları gibi IP sürümünden bağımsız, uygulamalardan kaynaklı güvenlik zaafiyetlerinin yanı sıra, IPv6 ile birlikte yeni gelen özellikler de zaafiyet barındırmaktadır. IPv6 protokolü ve IPv6 protokolüne geçiş yöntemleri, yeni ve derinlemesine incelenmemiş saldırı teknikleri ve araçları oluşmasına yol açmakta, IPv6 kullanımının çok yüksek olmaması protokolün yaygın kullanıldığında oluşabilecek güvenlik riskleri konusunda belirsizliğe neden olmaktadır. Zaafiyetleri, güvenlik duvarı kullanımı ile azaltmak mümkün olmakla birlikte, tam bir güvenlik için iletişimin tüm bileşenleri birlikte değerlendirilmeli, zincirin tüm halkaları sağlamlaştırılmalıdır.

Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi kapsamında, IPv6'ya geçiş aşamasında karşılaşılabilecek güvenlik sorunları konusunda ayrıntılı çalışmalar yürütülmüş olup, elde edilen sonuçlar "Minimum Güvenlik Belgesi" adlı bir belgede kapsamlı olarak belgelendirilmiştir. Söz konusu belgeye, http://www.ipv6.net.tr/ adresinden erişilebilir.

Güvenlik Duvarı (Firewall) Nedir?

Güvenlik duvarının en basit hali paket filtrelemedir. Paket filtreleme veya erişim listesi, uygulanan arayüz üzerinde giriş veya çıkış yönünde, bir protokolün belirli bir portunun belirli IP adresleri için engellenmesi olarak özetlenebilir. Örnek vermek gerekirse, TCP ve UDP protokollerinin 137-139 portlarının tüm IP adreslerine engellenmesi ile iç ağdaki bilgisayarlar üzerinde paylaşılmış dizinlere İnternet üzerinden erişilmesi engellenir. Benzer şekilde, kurumsal bir web sunucusunun, 80 (http) ve 443 (https) portlarına izin verilip diğer tüm

portların engellenmesi, bu sunucunun üzerinde çalışan diğer yazılımlarda ortaya çıkabilecek bir zaafiyetin güvenlik riski oluşturmasını engeller. Örneklerden de anlaşılabileceği üzere paket filtrelemek, çalışılan uygulamaların net olarak tanımlanabildiği durumlarda kullanılabilir.

Güvenlik duvarları, protokollerin özelliklerine göre yapılandırılabilir. TCP ve UDP protokollerinin farklı kaynak ve hedef port numaraları olabilir. ICMP'nin tip ve kod alanları bulunmaktadır. Bu alanlar kullanılarak erişim denetiminin sağlanması mümkündür. Ayrıca TCP, tasarımı gereği iletişimi takip eden durum denetimine sahip olduğundan, durum denetimli güvenlik duvarı yapılandırılması mümkün olmaktadır. İletişimin başlayacağı tarafın seçilerek, izin verilen iletişimin haricinde gelen paketlerin reddedilmesi, esnek ve daha doğru bir güvenlik duvarı yapılandırmasını sağlamaktadır. Paket filtreleme örneğinde verilen, iç ağdaki bilgisayarların dosya paylaşım portunun engellenmesi yerine, içeriden başlayan iletişime izin verilmesi ve bunun haricindeki tüm paketlerin reddedilmesi, hem iç ağdaki bilgisayarların başka portlarında çalışabilecek uygulamaları İnternet'ten korumakta, hem de paket filtreleme ile engellenen portların da kullanılabilmesini sağlamaktadır. Benzer şekilde, kurumsal web sunucusunun web servisinin verildiği portlara dışarıdan gelen iletişime izin verilmesi ve bunun haricindeki tüm paketlerin reddedilmesi, iletişim durumu dışında web portlarına gelebilecek paketleri de engelleyeceği için daha güvenli olmaktadır.

Günümüzde güvenlik duvarı kavramı, çoğu son kullanıcı tarafından da bilinmektedir. Ev ağlarının bağlantısında kullanılan modem ve yönlendirici cihazlar üzerinde, genellikle güvenlik duvarı bulunmaktadır. Ayrıca istemciler üzerinde de Windows Firewall, Zone Alarm gibi kişisel güvenlik duvarları kurulumu yapılmaktadır. IPv6 geçişinde dikkat edilmesi gereken bir diğer konu da, eski güvenlik duvarı alışkanlıklarından farklı olarak IPv6 da gerçek IP adresi kullanılması sebebiyle kural listelerinin yeniden yapılandırılması gerektiğidir. IPv4 de adres kısıtlılığı sebebiyle kullanılan NAT yapısı, NAT içerisinde yer alan istemcilere İnternet üzerinden doğrudan erişimi özel bir tanım yapılmamışsa engellemekte idi. Dolayısıyla NAT içerisinde yer alan istemciler, NAT yapısı gereği durum korumalı güvenlik duvarı (stateful firewall) korumasında gibi korunaklı idiler. Kullanmak istedikleri özel port veya protokoller için NAT üzerinde port eşlemesi yaparak iç ağdaki istemciye yönlendirmekte idiler. Her iki sürüm içinde gerçek IP kullanımında durum korumalı güvenlik duvarı yapılandırılmalı, servis verilecek uygulamalar için ise bu güvenlik duvarında gerekli izinler verilmelidir.

Söz konusu durumun ilk ortaya çıkışı, IPv4 üzerinden tünel ile IPv6 ağına bağlanılması tekniği olan Teredo özelliğinin bazı işletim sistemlerinde varsayılan olarak kurulu gelmesi ile olmuştur. NAT arkasında olan ve dolayısıyla tüm portları IPv4 İnternet'e kapalı olan istemciler üzerinde otomatik kurulan Teredo ile IPv6 ağına korunmasız, IPv4 güvenlik duvarlarının haricinde tüm portları açık olarak erişilir bağlanmaya başlamıştır. Bazı ev tipi yönlendiricilerin üzerinde de Teredo özelliğinin açık olması ile durum ciddiyet kazanmış, güvenlik uyarıları yayınlanmıştır (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-1338). Bu güvenlik açığının sonucu olarak güvenlik duvarlarında IPv6 desteğinin

verilmesi ve IPv6 için kural listelerinin yapılması, en azından durum korumalı engellenmesi şeklinde tavsiyeler yayınlanmıştır.

Durum korumalı güvenlik duvarlarının yönettiği istemci-sunucu mimarisindeki iletişimin yanı sıra, istemciler arasında kontrol-veri protokolleri de günümüz uygulamaları arasında yer almaktadır. Aktif FTP, BitTorrent, bazı sohbet programları, SIP (VoIP protokolü), RTSP (ses ve görüntü aktarımı) gibi örnekleri olan bu tarz istemciden istemciye (peer-to-peer) uygulamaların güvenlik açısından yönetimi zorlaşmaktadır. Bu protokoller için güvenlik duvarlarında izin verilebilmesi, durum korumalı güvenlik duvarında adres/port delikleri açılması ile mümkün olabilmekte, bu durum da yine güvenlik zaafiyetine sebep olmaktadır. NAT yapısında da geçerli olan ve port eşlemesi ile açılabilen bu durum uygulama seviyesi ağ geçitleri (ALG - Application Layer Gateway) kullanımı ile gözlenebilmektedir. Uygulama seviyesi güvenlik duvarları, saldırı tespit sistemleri ile bu gibi protokollerin trafiği incelenerek güvenlik sorunu olacağı düşünülen paketler düşürülür, gerekirse iletişim tamamen kesilebilir.

IPv6 Güvenlik Duvarı Yapılandırılması

Önceki bölümde anlatılan gerekçelerden dolayı, IPv6 geçişi sonrasında güvenlik duvarı kullanılması zorunludur. Günümüzde IPv6 güvenlik duvarı olarak kullanılabilecek çeşitli ticari ve özgür ürünler bulunmaktadır. Hazır ürünlere ilaveten ihtiyaçlar doğrultusunda özelleştirilmiş esnek güvenlik duvarları, BSD ve Linux işletim sistemleri ile kurulabilecek PC Yönlendiriciler ile mümkündür.

Güvenlik duvarı yapılandırılırken, korunacak olan ağın, istemcinin veya sunucunun ihtiyaçları göz önüne alınarak, sadece kullanılan servislere ait protokole ve portlara izin verilmeli, geri kalan herşey engellenmelidir. Güvenlik duvarı bir istemci veya sunucu üzerinde ise yönlendirici paketleri engellenmelidir. Yönlendiriciler üzerinde ise, yönlendirilecek ağın haricinde çıkışa ve girişe izin verilmemelidir.

İstemciler arası kullanılan protokollere izin verilecek ise, DPI uygulamaları kurulmalı, uygulama seviyesinde paket incelemesi ile filtreleme yapılmalıdır. Güvenliğin, iletişim zincirinde yer alan tüm öğelerde ele alınması gerektiği unutulmamalı, zincirin tüm halkalarında güvenlik önlemleri alınmalıdır. Bunun için yönlendiricilerin yanı sıra istemci ve sunucularda da ihtiyaca uygun güvenlik duvarı uygulanmalıdır. Yönlendirici dışındaki güvenlik duvarlarında yönlendirici özellikleri kapatılmalıdır.

ICMPv6'nın tüm IPv6 düğümlerinin iletişimleri için temel bir protokol olarak tasarlanması nedeniyle tüm düğümlerin ICMPv6'yı eksiksiz desteklemesi zorunluluğu ortaya çıkmıştır. Güvenlik duvarlarında ICMPv6 paketlerinin tamamını filtrelemek IPv6 protokolünün sağlıklı çalışmasını engeller. Ağda verilmeyen servislere ait ICMPv6 mesaj tiplerinin ağa girmesine izin verilmesi güvenlik açıklarına neden olacaktır. IANA 155-199 arası ICMPv6 mesaj tipleri

için henüz bir atama yapmamıştır. Ayrıca 200 ve 201 numaralı mesaj tipleri de deneyler için ayrılmıştır. Bu tiplerdeki ICMPv6 mesajlarının filtrelenmesi gerekmektedir. "Tip 138 Yönlendiricileri Yeniden Numaralandırma" ve "Tip 139, 140 Düğüm Bilgisi Sorgusu ve Cevabı" mesajlarına özel ilgi gösterilmeli ve bu mesaj tipleri ile ilgili ağda özel uygulamalar yapılmıyorsa, sınır güvenlik cihazlarında engellenmelidir.

ICMPv6 tip numaraları Bölüm 1: IPv6 Temelleri ve Yapılandırması, ICMPv6 başlığında açıklanmıştır. IPv6 iletişiminin sağlıklı yapılabilmesi için kesinlikle engellenmemesi gereken ICMPv6 mesajı tipleri ve isimleri Tablo 6'da verilmiştir.

Tablo 6. İzin Verilmesi Gereken ICMPv6 Tipleri

Mesaj Tipi	Mesaj Adı
1	Hedef Erişilemez
2	Paket Çok Büyük
3	Zaman Aşımı
4	Parametre Problemi
133	Yönlendirici Talebi
134	Yönlendirici İlanı
135	Komşu Talebi
136	Komşu İlanı

Hedef IP'si bir 'çoklu gönderim grubu' olan paketlerin kendi kapsama alanları dışındaki alanlara geçişine izin verilmeden güvenlik duvarı veya yönlendiricilerde düşürülmeleri gerekmektedir. Bu kısıtlamanın yapılmadığı IPv6 ağlarında hedef adresi çoklu gönderim grubu olan ICMP paketleri ile saldırı öncesi keşif çalışmaları, IPv4 ağlarından çok daha kolay bir şekilde gerçekleştirilebilir.

Uzantı Başlıkları

Uzantı başlıkları ağ güvenliği için dikkatle incelenmeli, güvenlik açığı oluşturabilecek özellikler engellenmelidir. Örneğin dolaşılabilirlik başlığı, eğer iç ağda dolaşılabilirlik desteği verilmiyor ise engellenebilir. Bazı uzantı başlıkları ise kesinlikle engellenmelidir. Yönlendirme başlığı RH, RFC2460 belgesinde tanımlanmış olup, Tip 0 kullanımında tespit edilmiş güvenlik açıkları bulunmaktadır. Tip 0 kaynağın yolladığı paketin rotasını tanımlamasını sağlar ve IPv4 paketleri için yapılan "Gevşek Kaynak Yönlendirmesi (Loose Source Routing)" ile aynı özellikleri taşımaktadır. Tip 1 kullanım dışı olarak tanımlanmış, Tip 2 ise Dolaşılabilirlik uygulaması için Tip 0 filtrelemesi amacıyla tanımlanmıştır. Çıkan güvenlik açıklarından dolayı Tip 0'ın IPv6 cihazlarda işlenmemesi, ayrıca ağ cihazlarında ise düşürülmesi kesinlikle önerilmektedir. Bazı cihaz ve işletim sistemlerinde RH için girilebilecek komutlar, Tablo 7'de verilmiştir.

Tablo 7 . İşletim Sistemleri RH Tip 0 Durumu

İşletim Sistemi	Yöntem
Cisco IOS	no ipv6 source-route
Juniper	Henüz açıklanmış bir engelleme bulunmamaktadır.
Linux	Kernel 2.6 dan itibaren kaldırılmıştır. Yönlendirici olması durumunda paketleri engellemek için, kural listesinin başına aşağıdaki kurallar eklenir: ip6tables -A INPUT -m rt--rt-type 0 -j DROP ip6tables -A FORWARD -m rt--rt-type 0 -j DROP ip6tables -A OUTPUT -m rt--rt-type 0 -j DROP
FreeBSD	Kernel 6.2'den itibaren kaldırılmıştır. Eski çekirdekler için yama: http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/netinet6/route6.c.diff?r1=1.12&r2=1.13 sysctl net.inet6.ip6.rthdr0_allowed=0
OpenBSD	OpenBSD 4.0-stable için yama: ftp://ftp.openbsd.org/pub/OpenBSD/patches/4.0/common/012_route6.patch OpenBSD 3.9-stable için yama: ftp://ftp.openbsd.org/pub/OpenBSD/patches/4.0/common/012_route6.patch

Sınır Yönlendirici Filtre Önerileri

Bu bölümde, iç ağın dış ağlarla iletişiminin sağlandığı sınır yönlendirici üzerinde uygulanabilecek filtreler önerilmektedir.

Güvenlik Duvarı Kuralları Önerisi

1. İç ağ adreslerinizi içeri kaynak yönünde engelleyin. İç ağınızdaki adreslerin dışarıdan gelmesi, sahte IP (spoofing) trafiği olarak tanımlanır, engellenmelidir.
2. İç ağ adresleriniz dışında kalan adresleri dışarı kaynak yönünde engelleyin.
3. Kullanmadığınız uzantı başlıklarını engelleyin.
    a. Dolaşılabilirlik uygulaması için kullanılan başlıkları dolaşılabilirlik servisini vermiyorsanız engelleyin.
    b. Yönlendirme başlığı tip 0 olan paketleri engelleyin.
4. Tünelleme yapan iç ağ adresleriniz dışında kalan iç ağ aralığına, tünel adres aralıklarını engelleyin (6to4 aralığı: 2002::/16, Teredo 2001::/32).
5. Internet için ayrılan alanlar 2000::/3 ve küresel çoklu gönderim adresleri gibi, iletişimde bulunulacak IPv6 adres aralığı dışında kalan IP adreslerini engelleyin.
    a. Eşsiz yerel tekil gönderim adresleri (fc00::/7).
    b. Rezerve edilmiş aralık (0::/8).
    c. Bağlantı Yerel Tekil (fe80::/10).
6. TCP, UDP, ICMPv6 ve ESP gibi, iç ağınıza dışarıdan erişilmesi gereken protokollere izin verin, kalan tüm protokolleri engelleyin.
7. Sunucularınızı ve servis portlarınızı tanımlayarak,
    a. Sunucular haricinde iç ağa dışarıdan iletişim başlatılmasını
    b. Sunucu servis portlarının haricindeki portlara iletişim başlatılmasını

engelleyin (durum koruması). Sunucuların servis portlarına izin verirken, DoS saldırılarından korunmak için, bağlantı limiti, servis verilen IP aralığı gibi kısıtlamalar uygulayın.

8. Çoklu gönderim adreslerini belirleyerek, kapsam dışından gelen veya kapsam dışına çıkan paketleri engelleyin.
9. ICMPv6 başlıklarından sadece gerekli olanlarına izin verin, kalanını engelleyin.
10. İç ağdaki tüm IP adreslerinin dışarı doğru durum korumalı iletişim başlatmasına izin verin.

ICMPv6 Filtresi

Korumacı bakış açısı ile ICMPv6 mesajlarına nasıl davranılacağı hakkında öneriler, Tablo 8'de verilmiştir. Uygulamada ağınızın ihtiyaçları gözönünde bulundurularak sadece belirli tiplere izin verilmeli, geri kalanlar engellenmeli, en azından limitlenmelidir. İlk 4 tip ICMPv6 mesajı Tablo 6'da izin verilmesi egreken ICMPv6 tipleri olarak nitelendirilse de, ağınızın dışarıdan tespit edilmesine sebep oldukları için kapatılması, en azından limitlenmesi önerilmektedir.

Tablo 8. ICMPv6 Filtre Önerileri

ICMPv6 Tipi		İçeriye	Dışarıya	Açıklama
1	Hedef Erişilemez	İzin ver	Engelle	Ağın haritasını çıkarmak ve tespit etmek için kullanılabilir. Dışarıya doğru sadece güvenilir ağlara izin verilmelidir.
2	Paket Çok Büyük	İzin ver	İzin ver	Ağın sağlıklı çalışması için gereklidir.
3	Zaman Aşımı	İzin ver	Engelle	İzin verilmesi gerektiği önerilse de, ağın haritasını çıkarmak ve tespit etmek için kullanılabilir. Dışarıya doğru sadece güvenilir ağlara izin verilmelidir.
4	Parametre Sorunu	İzin ver	İzin ver / Engelle	İç ağın haritasını çıkarmak ve tespit etmek için kullanılabilir. İstemciler için engellenmelidir, ağ cihazları için açılabilir.
128	Yankı İsteği	Engelle	İzin ver	İç ağın haritasını çıkarmak ve tespit etmek için kullanılabilir. İstemciler için engellenmelidir, ağ cihazları için açılabilir.
129	Yankı cevabı	İzin ver	Engelle	İç ağın haritasını çıkarmak ve tespit etmek için kullanılabilir. İstemciler için engellenmelidir, ağ cihazları için açılabilir.
130-132	MLD	Engelle	İzin ver	İç ağda ihtiyaç duyulur, dışarıya engellenebilir.
135-136	ND	İzin ver	İzin ver	Ağın sağlıklı çalışması için gereklidir.
133-134	RD	İzin ver	İzin ver	Ağın sağlıklı çalışması için gereklidir.
135	Redirect	İzin ver	İzin ver	Ağın sağlıklı çalışması için gereklidir.
139-140	Düğüm Bilgisi Sorgusu	Engelle	Engelle	Uygulamada henüz kullanım alanı az olduğundan, kapatılabilir.
141-142	Ters komşu keşfi	Engelle	Engelle	Uygulamada henüz kullanım alanı az olduğundan, kapatılabilir.
144-147	Dolaşılabilirlik başlıkları	Engelle	Engelle	Dolaşılabilirlik desteği vermedi iseniz, kapatılmalıdır.

Örnek Yapılandırmalar

IPv6 Adres Filtreleme

OpenBSD PF:

```
pass in log on $ext_if inet6 proto tcp from $admins to ($ext_if) port ssh
block in on $ext_if inet6 proto {tcp, udp} from any to ($ext_if) port ssh
pass in on em0 inet6 proto tcp from 2001:a98:1f:6::5/64 to 2001:a98:1f:4::2 port http
```

Linux IP6TABLES:

```
ip6tables -A FORWARD -i eth0 -p tcp -d 2001:a98:1f:4::2 --dport 22 -j ACCEPT
ip6tables –A INPUT –i eth0 –p tcp –d 2001:a98:1f:4::2 --dport 22 -j DROP
ip6tables –A INPUT –p tcp –d 2001:a98:1f:4::2 --dport 80 -j ACCEPT
```

Multicast Filtreleme

Linux IP6TABLES:

```
# Join mesaj limiti
ip6tables -t mangle -A PREROUTING -i eth0 -p pim
      -m pim6 --pim6-type join -m limit --limit 1/minute
# Join/Prune mesajlar
ip6tables -t mangle -A PREROUTING -i eth0 -p pim
 -m pim6 --pim6-type join --pim6-group ff0e:abcd::/32 -j DROP

ip6tables -t mangle -A PREROUTING -i $eth0 -p pim
 -m pim6 --pim6-type join,prune --pim6-group ff0e::/16 -j PIMRELAY
# Register mesaj limiti
ip6tables -t mangle -A PREROUTING -p pim
 -m pim6 --pim6-type register -m limit --limit 10/second

# Register mesajlar
ip6tables -t mangle -A PREROUTING -i $eth0 -p pim -m pim6
 --pim6-type register --pim6-reg-group ff3e:30:2001:388:c035::/96 -j PIMRELAY
```

Linux Güvenlik Duvarı Betiği

```
#!/bin/sh

# Guvenlik duvarlari icin CERT tarafindan hazirlanan listeden uyarlanmistir.
# Kural listesi gosterim amaclidir. Kendi yapiniza uygun liste olusturunuz.
# Uygulamadan once kurallari gozden gecirip test ediniz.
#

# TCP Disariya acik portlar. passive FTP icin 33300:33400 araligini acin
TCP_ACIK="ssh 1812:1814 domain"
UDP_ACIK="domain 1812:1814"

#Servis portlarina 60 saniye icerisinde yapilabilecek maksimum baglanti sayisi:
# (DoS saldirilarina karsi)
MAX_SYN="20"

# TCP ve UDP *ic aga* kapali portlar.
# Ornekte, VNC ve X-Windows portlari, ssh tunel yapabildikleri icin secilmistir.
TCP_KAPALI="5900:5910,6000:6063"
UDP_KAPALI=""


# Once yuklu kurallari temizle:
########################################
ip6tables -F INPUT
ip6tables -F FORWARD
ip6tables -F OUTPUT
ip6tables -F


# Ana zincirleri kur:
########################################
ip6tables -P INPUT DROP
ip6tables -P FORWARD DROP
ip6tables -P OUTPUT DROP


# localhost trafigine tum protokoller icin izin ver:
########################################
ip6tables -A INPUT -s ::1 -d ::1 -j ACCEPT


# ICMPv6 GELEN - izin verilecek tipler:
########################################
ip6tables -A INPUT -p icmpv6 --icmpv6-type destination-unreachable -j ACCEPT
ip6tables -A INPUT -p icmpv6 --icmpv6-type packet-too-big -j ACCEPT
ip6tables -A INPUT -p icmpv6 --icmpv6-type time-exceeded -j ACCEPT
ip6tables -A INPUT -p icmpv6 --icmpv6-type parameter-problem -j ACCEPT
```

```
# ICMPv6 GELEN - limitlenerek izin verilecek tipler:
#######################################
ip6tables -A INPUT -p icmpv6 --icmpv6-type echo-request -m limit --limit 900/min -j ACCEPT
ip6tables -A INPUT -p icmpv6 --icmpv6-type echo-reply -m limit --limit 900/min -j ACCEPT


# ICMPv6 GELEN - Sicrama limiti 255 ise izin verilecek tipler:
#######################################
ip6tables -A INPUT -p icmpv6 --icmpv6-type router-advertisement -m hl --hl-eq 255 -j ACCEPT
ip6tables -A INPUT -p icmpv6 --icmpv6-type neighbor-solicitation -m hl --hl-eq 255 -j ACCEPT
ip6tables -A INPUT -p icmpv6 --icmpv6-type neighbor-advertisement -m hl --hl-eq 255 -j
ACCEPT
ip6tables -A INPUT -p icmpv6 --icmpv6-type redirect -m hl --hl-eq 255 -j ACCEPT


# ICMPv6 GELEN - uymayan paketleri dusur:
#######################################
ip6tables -A INPUT -p icmpv6 -j LOG --log-prefix "filtrelenen ICMPv6"
ip6tables -A INPUT -p icmpv6 -j DROP


# ICMPv6 GİDEN - Disariya dogru izin verilecek tipler:
#######################################
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type destination-unreachable -j ACCEPT
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type packet-too-big -j ACCEPT
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type time-exceeded -j ACCEPT
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type parameter-problem -j ACCEPT


# ICMPv6 GİDEN - Yerel agda Komsu Kesfi paketlerini limitle:
#######################################
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type neighbour-solicitation -m hl --hl-eq 255 -j
ACCEPT
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type neighbour-advertisement -m hl --hl-eq 255 -j
ACCEPT
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type router-solicitation -m hl --hl-eq 255 -j ACCEPT


# ICMPv6 GİDEN - RA ve Redirect paketlerini filtrele
# Yonlendirici olarak calisan sistemlerde acik olmali
#######################################
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type router-advertisement -j LOG --log-prefix
"ICMPv6 RA"
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type redirect -j LOG --log-prefix "ICMPv6 redirect"
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type router-advertisement -j REJECT
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type redirect -j REJECT


# ICMPv6 GİDEN - Geri kalan tum paketlere izin ver:
#######################################
ip6tables -A OUTPUT -p icmpv6 -j ACCEPT
```

```
# ICMPv6 GİDEN – Yonlendirmeyi filtrele
#######################################
ip6tables -A FORWARD -p icmpv6 -j REJECT

# TCP Kuralları
# Bildirilen portlari filtrele
#######################################
ip6tables -A INPUT -m multiport -p tcp --dport $TCP_KAPALI -m hl --hl-eq 255 -j REJECT
ip6tables -A OUTPUT -m multiport -p tcp --dport $TCP_KAPALI -m hl --hl-eq 255 -j REJECT
ip6tables -A INPUT -m multiport -p tcp --dport $TCP_KAPALI -m hl --hl-lt 255 -j DROP
ip6tables -A OUTPUT -m multiport -p tcp --dport $TCP_KAPALI -m hl --hl-lt 255 -j DROP


# Durum tespitli kurallar
#######################################
ip6tables -A OUTPUT -p tcp -j ACCEPT
ip6tables -A OUTPUT -p udp -j ACCEPT
ip6tables -A INPUT -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT
ip6tables -A INPUT -p udp -m state --state ESTABLISHED,RELATED -j ACCEPT

# TCP ve UDP servis portlari ve DoS korumasi
#######################################
for port in $TCP_ACIK; do
   $ip6tables -A INPUT -p tcp --dport $port -m state --state NEW \
      -m recent --set --name "$port"
   $ip6tables -A INPUT -p tcp --dport $port -m state --state NEW \
      -m recent --name "$port" --update --seconds 60 \
      --hitcount $MAX_SYN -j DROP
   $ip6tables -A INPUT -p tcp --dport $port -j ACCEPT
done

for port in $UDP_ACIK; do
   $ip6tables -A INPUT -p udp --dport $port -j ACCEPT
done


# NEW,INVALID etiketli paketleri filtrele (durum korumasi)
#######################################
ip6tables -A INPUT -m state --state NEW,INVALID -j DROP


# TCP ve UDP Yonlendirmeyi kapat
#######################################
ip6tables -A FORWARD -p tcp -j REJECT
ip6tables -A FORWARD -p udp -j REJECT
```

BSD Güvenlik Duvarı Betiği

```
ext_if="em0“
int_if=“em1”
v6_net=“2001:a98:1f:3::/64“
admins={200:a98:1f:3::10, 2001:a98:1f:3::11}
set skip on {lo0}
set block-policy drop
set loginterface $ext_if
scrub in all  # fragmante paketleri duzelt
block log all    # gelen/giden tum trafik blokla
pass out from $v6_net to any  # v6_net listesinde bulunanalari disari cikar

# minimum ICMPv6 paketlerine izin ver
pass in on $ext_if inet6 proto icmp6 icmp6-type \
{echoreq,echorep,unreach,toobig,timex,paramprob, neighbrsol, neighbradv}

# admin listesinde olanlara SSH izni ver
pass in log on $ext_if inet6 proto tcp from $admins to ($ext_if) port ssh

# web sunucusuna gelirse izin ver
pass in inet6 proto tcp from 2001:a98:1f:6::5/64 to 2001:a98:1f:4::2 port http
```

Cisco IOS

```
ipv6 access-list sinir-yonlendirici-giris
remark belirli ICMP tiplerine giris yonunde izin ver
  permit icmp any 2001:a98:60::/48 destination-unreachable
  permit icmp any 2001:a98:60::/48 packet-too-big
  permit icmp any 2001:a98:60::/48 parameter-problem
  permit icmp any 2001:a98:60::/48 echo-reply
remark uzak agdan pinglenmesine izin ver
  permit icmp 2001:a98:20::/48 2001:a98:60::/48 echo-request
remark RD Haric, ND ve MLD ICMP tiplerine izin ver
  permit icmp any any nd-na
  permit icmp any any nd-ns
  permit icmp any any mld-query
  permit icmp any any mld-reduction
remark kalan ICMPleri engelle, kalan herseyi ac
  deny icmp any any log
  permit any any
```

BÖLÜM 6: AĞ TRAFİĞİ ANALİZİ

MRTG ile Hat Kullanım Grafiklerinin Elde Edilmesi

Multi Router Traffic Grapher, ağ bağlantılarında kullanılan hatların kullanım grafiklerinin oluşturulmasına yarayan bir araçtır. MRTG, Perl ve C programlama dillerini kullanır, UNIX ve Windows işletim sistemleri altında çalışabilir. Üzerine MRTG kurulan bir monitör sunucusu, ağa bağlanmakta kullanılan yönlendiriciden hat kullanım bilgilerini Simple Network Management Protocol (SNMP) kullanarak alır ve grafiksel olarak gösterime sunar.

Bu bölümde ilgili grafiklerin oluşturulması için yönlendirici tarafında ve monitör sunucusunda yapılması gereken ayarlar anlatılacaktır.

Yönlendirici SNMP Ayarları

Unix ve BSD

Unix ve BSD tabanlı yönlendiricilerde hat kullanımı bilgilerinin tutulması ve sorgu yapan istemcilere sağlanması için NET-SNMP paketini kullanılmaktadır. BSD tabanlı yönlendiricilerde aşağıdaki şekilde kurulum yapılabilir:

```
$ cd /usr/ports/net-mgmt/net-snmp ; make -DBATCH -DWITH_IPV6 install clean
```

Sonrasında snmpd başlatılmadan önce */etc/snmpd.conf* ayar dosyasında bazı değişiklikler yapılması gerekmektedir. Bu değişiklikler ile sunucudan sorgu yapacak istemcilerin güvenlik amacıyla kullanacağı community değerinin değiştirilmesi gerekmektedir. Değişikliklerden sonra ayar dosyasının hali şu şekilde olacaktır:

```
syslocation  "Grup No"
syscontact  "System Admin"
sysservices 0
rocommunity6   ulakbim
rocommunity    ulakbim
```

Snmpd hem IPv4 hem de IPv6 dinleyebilmesi için IPv6 ve IPv4 trafiği udp 161 portunu dinleyecek şekilde çalıştırılır. Kovan her yonlendirici icin aşağıdaki komut ve argumanlar ile snmpd calıştırır.

```
$/usr/local/sbin/snmpd -c /etc/snmpd.conf   udp6:161 udp:161
```

Cisco

Cisco yönlendiricilerde aşağıdaki satırlar eklenerek cihazın ulakbim community değeri ile yapılan sorgulara cevap vermesi sağlanır.

```
snmp-server community ulakbim RO 100
snmp-server ifindex persist
snmp-server location Ankara-Turkiye
snmp-server contact Admin admin@xyz.gov.tr
```

Bu ayarlarda ilk satırda yer alan RO snmp istemcilerinin sadece okuma için (Read Only) erişebilmesini sağlarken 100 ise bu erişimde uygulanacak erişim kontrol listesi (Access Control List - ACL) göstermektedir. 100 nolu ACL'de sadece SNMP istemcisi olarak kullanılacak cihazlara izin verilmesi güvenlik açısından önemli bir tedbir olacaktır.

Monitör Makinesine MRTG Kurulumu

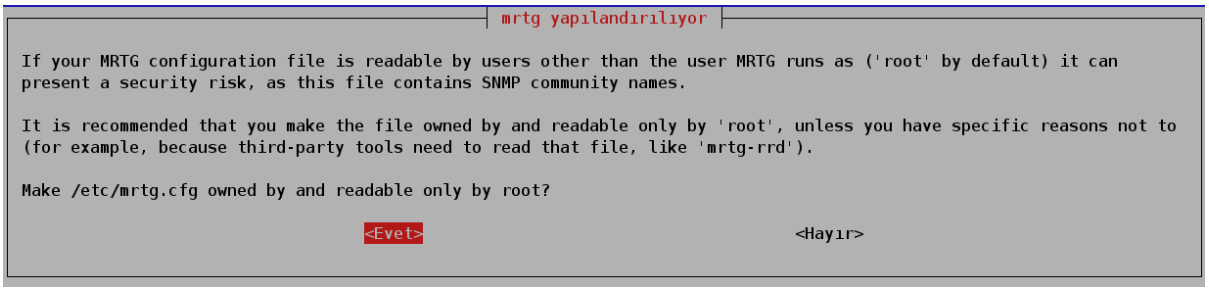
Kurulacak MRTG'nin oluşturduğu grafiklerin izlenmesi için öncelikle monitör cihazında bir web sunucusu çalışmalıdır. Linux tabanlı bir monitör sunucusunda için Apache web sunucusunun kurulumu şu şekilde yapılabilir:

```
$ apt-get update
$ apt-get install build-essential
$ apt-get install apache2
```

Kurulum tamamlandıktan sonra MRTG kurulumuna geçilebilir:

```
$ apt-get install mrtg
Paket listeleri okunuyor... Bitti
Bağımlılık ağacı inşa ediliyor.
Durum bilgisi okunuyor... Bitti
Aşağıdaki ek paketler de yüklenecek:
  libio-socket-inet6-perl libsnmp-session-perl libsocket6-perl
Önerilen paketler:
  mrtg-contrib
Aşağıdaki YENİ paketler kurulacak:
  libio-socket-inet6-perl libsnmp-session-perl libsocket6-perl mrtg
0 yükseltildi, 4 yeni kuruldu, 0 kaldırılacak ve 0 yükseltilmeyecek.
İndirilmesi gereken dosya boyutu 552kB
Bu işlemden sonra 1.749kB ek disk alanı kullanılacak.
Devam etmek istiyor musunuz [E/h]?
```

Bu sorunun "Evet" olarak cevaplanması sonucunda kurulum başlayacak ve oluşturulacak ayar dosyasının izinleri için Şekil 30'daki ekran belirecektir.



Şekil 30: MRTG Ayar Dosyası İzinleri

"Evet" cevabı *mrtg.conf* dosyasını 640 izinleri ile oluşturacakken Hayır cevabı bu izinin 644 olarak belirlenmesini sağlayacaktır. Bu ayar dosyasının hat kullanımı hakkında bilgi veren başka programlar tarafından kullanılması düşünülmüyor ve ileride bahsedilecek cron ayarları sadece root için yapılacaksa bu seçenekte "Evet" cevabının verilmesi önerilmektedir.

Kurulum aşamasında ve sonrasında kontrollerin yapılabilmesi için gerekli komutları barındıran snmp paketinin monitör makinesinde kurulması gerekmektedir.

```
$apt-get install snmp
```

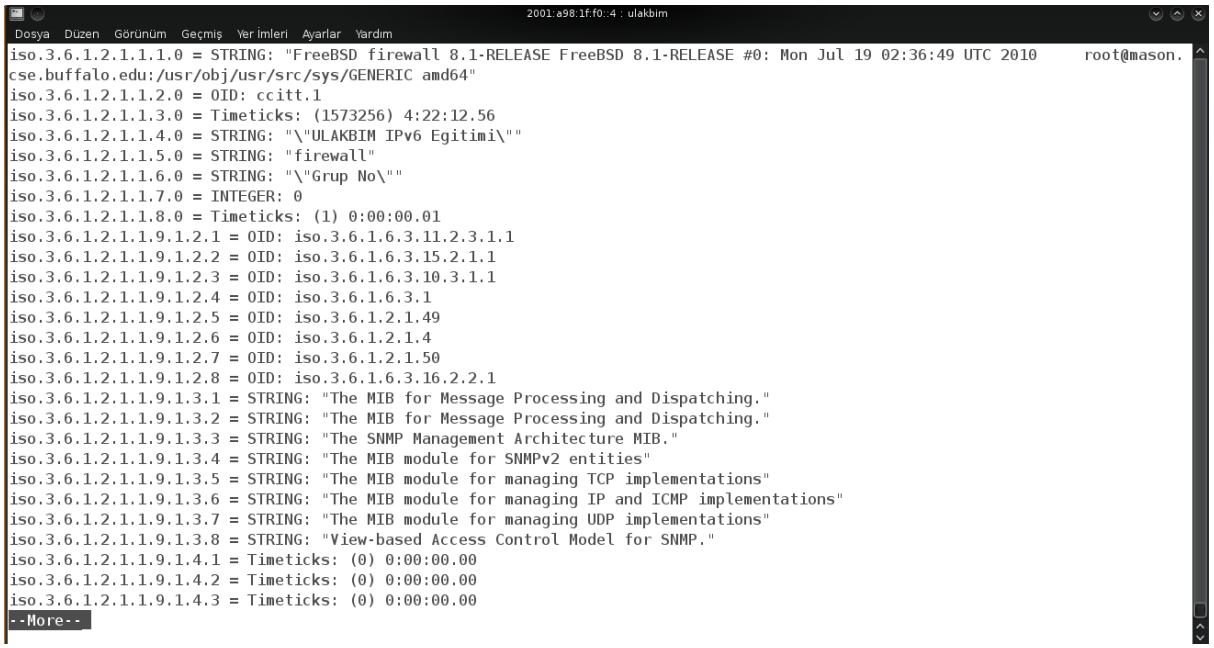
MRTG ve SNMP' nin BSD tabanlı sunucularda kurulması için aşağıdaki komutlar kullanılabilir:

```
$ cd /usr/ports/net-mgmt/net-snmp ; make -DBATCH -DWITH_IPV6 install clean
$ cd /usr/ports/net-mgmt/net-snmp && make -DBATCH -DWITH_IPV6 install
$ cd /usr/ports/net-mgmt/mrtg/&& make -DBATCH -DWITH_IPV6 -DWITH_SNMP
install clean
```

Daha sonra SNMP ile trafik verilerini çekip MRTG ile grafik haline getirmek istediğimiz yönlendirici ile SNMP iletişiminin sağlık olduğunun kontrolü için snmpwalk komutu kullanılabilir. Burada dikkat edilmesi gereken konu 2001:a98:1f:f0::1 adresli yönlendiricide belirlenen SNMP sürümü ile monitör makinesinde sorgu için kullanılan ve –v parametresinden sonra verilen sürümün aynı olmasıdır. Ayrıca aşağıdaki sorguda yer alan community_string değeri bir önceki bölümde yönlendiricilerde belirlenen değerle aynı olmalıdır.

```
$snmpwalk -v 2c  -c ulakbim udp6:[2001:a98:1f:f0::1]
$snmpwalk -v 2c -c ulakbim 10.1.4.1
```

Bu sorguya yönlendirici aşağıdaki ekran görüntüsüne benzer bir cevap dönecektir.



Şekil 31: SNMPWALK Sorgusuna Yönlendiricinin Cevabı

Yönlendirici ve monitör arasındaki SNMP iletişimi doğrulandıktan sonra MRTG için ayar dosyasının yapılandırmasına geçilebilir. MRTG'nin ayar dosyalarını üreten "*configmaker*" ve web sayfalarını üreten "*indexmaker*" betikleri bulunmaktadır. MRTG'ye ait *"configmaker"* betiğini kullanılarak yönlendiricilere bağlanılır, yönlendirici üzerindeki arayüzlere ait bilgiler çekilir ve bu bilgilerden MRTG'nin grafik oluşturmak için kullanacağı ayar dosyası olan *mrtg.conf* oluşturulur. Yine MRTG'nin *"indexmaker"* betiği de oluşturulan ayar dosyasını okuyarak MRTG grafiklerinin görüntülenebilmesini kolaylaştıran web dizin ve dosya yapısını oluşturur.

```
$which cfgmaker
/usr/bin/cfgmaker
$/usr/bin/cfgmaker  --enable-ipv6 --global "Options[_]: growright, bits" --global
"WorkDir: /var/www/mrtg" ulakbim@10.1.4.1 > /usr/local/etc/mrtg.conf
$mkdir /var/www/mrtg
$/usr/bin/indexmaker --title "Hat Kullanim Grafikleri" /usr/local/etc/mrtg.conf --
output /var/www/mrtg/mrtg.html
$ls -la /var/www/mrtg/mrtg.html
-rw-r--r-- 1 root root 3595 2011-04-12 12:28 /var/www/mrtg/mrtg.html
```

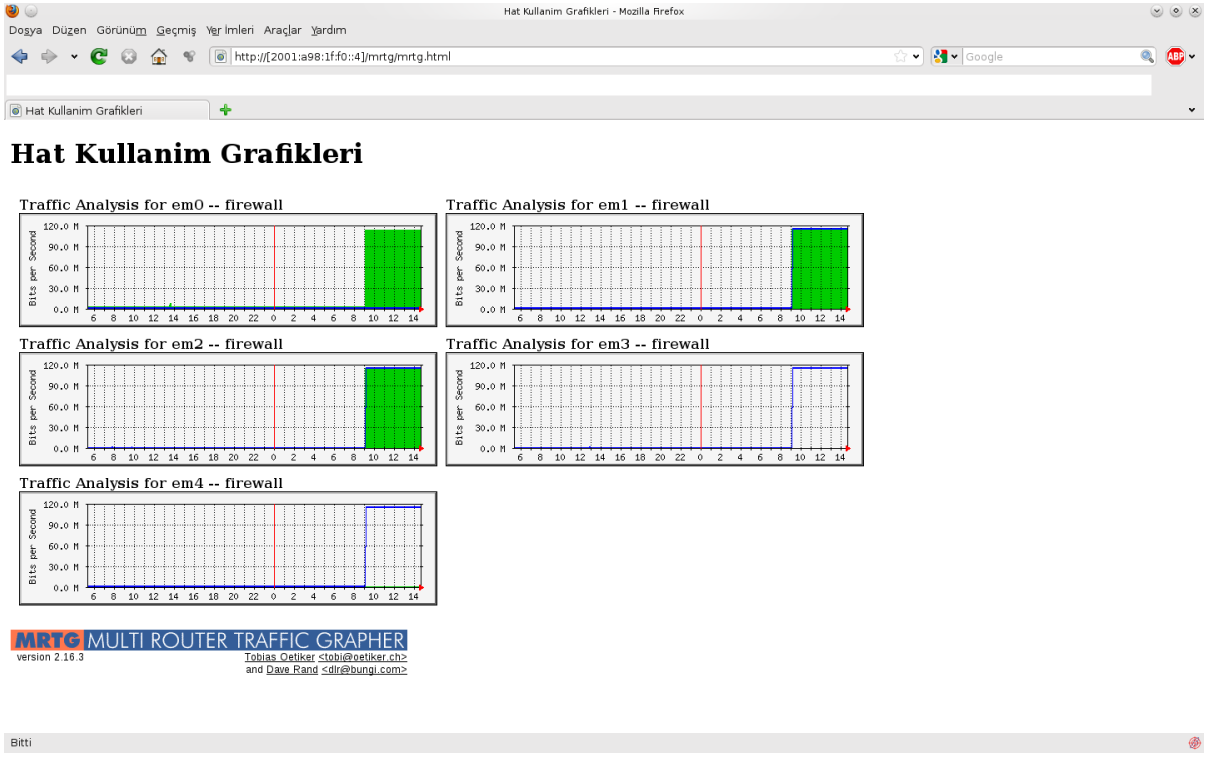
MRTG aşağıda gösterildiği gibi de elle çalıştırılabilir:

```
$ which mrtg
/usr/bin/mrtg
$env LANG=C  /usr/bin/mrtg   /usr/local/etc/mrtg.conf
```

Crontab her 5 dakikada bir MRTG'yi ilgili ayar dosyası ile çalıştırmak ve grafikleri güncellemek üzere değiştirilir. Aşağıdaki satırların crontab'a yazılması gerekmektedir.

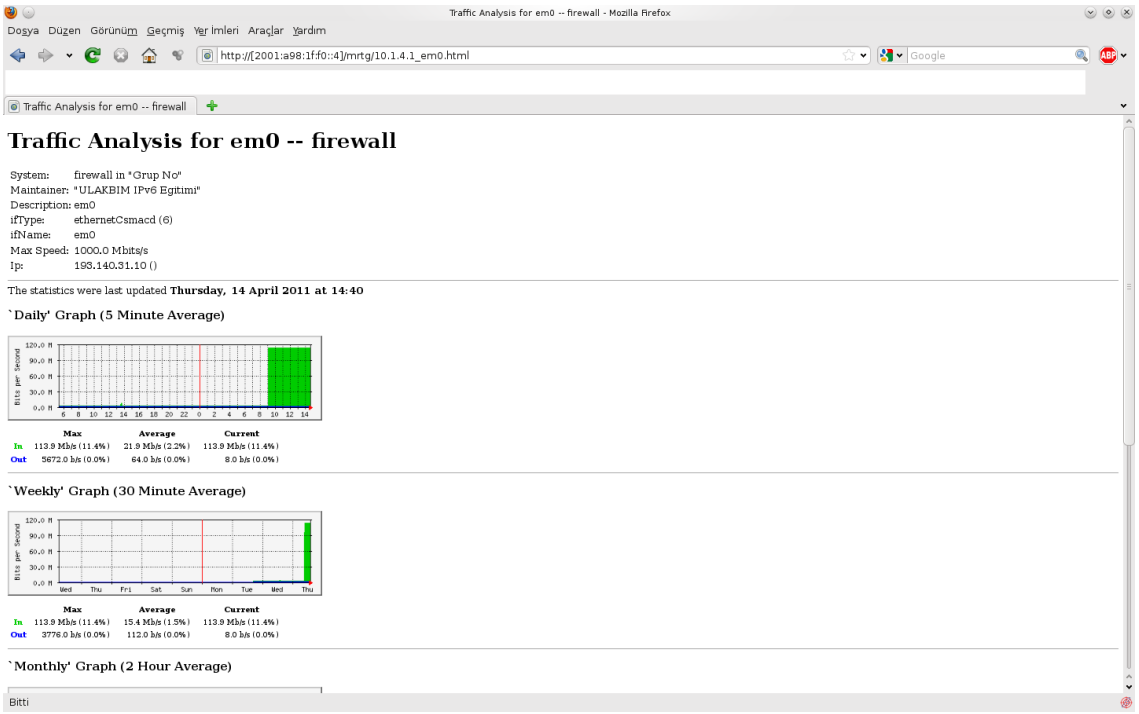
```
5,10,15,20,25,30,35,40,45,50,55 * * * * env LANG=C /usr/bin/mrtg
/usr/local/etc/mrtg.conf
```

Kurulum tamamlandıktan sonra Monitör cihazının web sayfasına bağlanılarak MRTG grafiklerine ulaşılabilir. *http:///[2001:a98:1f:f0::4]/mrtg/mrtg.html* adresi görüntülendiğinde aşağıdaki anasayfa ile karşılaşılacaktır.



Şekil 32: MRTG Grafikleri Anasayfası

Şekilden de görüleceği üzere yönlendirici üzerinde bulunan 5 arayüz için (em0, em1, em2, em3 ve em4) trafik bilgileri düzenli olarak çekilmekte ve grafiksel olarak gösterilmektedir. Bu arayüzlerden herhangi birisi için oluşturulan uzun süreli grafikler ve detaylar için ana sayfadaki günlük grafiklere tıklamak yeterli olacaktır.



Şekil 33: em0 Arayüzü Trafik Detayları

Şekil 33'de görülen bilgilerden bazıları ya da tümü sistemler hakkında hassas bilgiler içerdiğinden gizlenmek istenebilir. Bu durumda configmaker tarafından otomatik oluşturulan */usr/local/etc/mrtg.conf* dosyasında değişiklik yapılarak gizlenmek istenen bilgilerin silinmesi gerekmektedir.

NfSen ile Yönlendirici Akış İzi (Flow) İncelenmesi

Bu bölümde ağ yönlendirici cihazlarının oluşturduğu ve üzerinden geçen trafiğe ait izleri barındıran akış izinin (flow) depolanması ve incelenebilmesi için yapılması gerekenler anlatılmaktadır. Bu izlerin tutulması ağ trafiğinin detaylı incelenmesi ve kaynak kullanımları konusunda ölçümler yapılabilmesini sağlamaktadır. Ayrıca kurulumu anlatılacak olan NfSen ile de bu izlerin bir arayüz yardımıyla detaylı analizi yapılabilmektedir.

Cisco tarafından geliştirilmiş açık bir protokol olan NetFlow, IP trafiği kayıtlarının toplanmasını sağlar. NetFlow kayıtları 5 temel içerikten oluşur: Kaynak IP adresi, hedef IP adresi, kaynak kapısı (PORT) ve hedef kapısı (PORT) ve protokol.

Örnek Kayıt:

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes
2011-03-29 06:34:01.571	4294967.295	UDP	2001:470:0:f0::2.59555	->	2001:a98:10::251.53	1	91
2011-03-29 06:34:01.571	4294967.295	UDP	2001:a98:10::251.53	->	2001:470:0:f0::2.59555	1	206
2011-03-29 06:34:02.664	4294967.295	UDP	2001:470:0:fa::2.15780	->	2001:a98:10::252.53	1	93
2011-03-29 06:34:02.664	4294967.295	UDP	2001:a98:10::252.53	->	2001:470:0:fa::2.15780	1	140

Netflow Akış İzlerinin Oluşturulması ve Sunucuya Yönlendirilmesi

Cisco

Yönlendirici cihaza bağlanıp enable moduna geçtikten sonra aşağıda verilen komutlar ile yönlendiricinin NetFlow dokuzuncu sürüm akış izleri 10.1.4.4 adresli sunucunun 9996 nolu kapısına yönlendirilmesi sağlanmıştır. IPv4 ve IPv6 protokollerine ait tüm trafiğin akış izi ilgili sunucuya iletilecektir.

```
Router#conf t
Router(config)#ipv4 flow-export version 9 origin-as
Router(config)#ipv6 flow-export version 9 origin-as
Router(config)# ipv6 flow-export destination 10.1.4.4 9995
Router(config)# ipv4 flow-export destination 10.1.4.4 9996
Router(config)# ip flow-export source Loopback0
```

Bir sonraki adım, akış izi toplamak istediğimiz yönlendirici arayüzlerinde gerekli ayarların yapılmasıdır.

```
Router#conf t
Router(config)#interface FastEthernet0/0
Router(config-if)#ipv6 flow ingress
Router(config-if)#ipv4 flow ingress
```

Önemli Not: Bu analizlerin yapılacağı birçok ağda yönlendirici ile kayıtların tutulacağı makine (örneğimizde 10.1.4.4 IP'li) arasında güvenlik duvarı bulunmaktadır. Bu durumun geçerli olduğu ağlarda, güvenlik duvarı üzerinde gerekli izinlerin tanımlanması önemlidir. Yukarıdaki örnekte akış izi verileri için kaynak IP adresi yönlendiricinin Loopback0 arayüzü tanımlanmıştır. Bu işlem için *"ip flow-export source Loopback0"* komutu kullanılmıştır. Güvenlik duvarı üzerinde ise, kaynak adresi Loopback0, hedef adresi 10.1.4.4 ve hedef UDP portları 9995-9999 arasında yer alan olan paketler için izin kuralları yazılmıştır.

BSD ve Unix

Ağ BSD ya da Unix tabanlı yönlendiricilerden ya da güvenlik duvarlarından akış izi alınması için softflowd programı kullanılmaktadır. Linux işletim sistemi Debian sürümü için örnek kurulum aşağıda verilmiştir.

```
$ apt-cache search softflowd
softflowd - Flow-based network traffic analyser
$ apt-get install softflowd
```

Softflowd FreeBSD portlarında yer almaktadır ve kolayca kurulumu yapılabilmektedir. Örnek kurulum komutları aşağıda verilmiştir.

```
$cd /usr/ports/net-mgmt/softflowd
$make install
```

Softflowd kurulduktan sonra üzerindeki arayüzlerden geçen trafiğe ait izlerin aktarılması için aşağıda verilen komutlar çalıştırılır. Burada interface ağ izi kaydı alınacak arayüzü, *MonitorIPv6address* bu kayıtların aktarılacağı sunucu ve *port_number* kayıtların aktarıldığı sunucunun dinlediği portu göstermektedir.

IPv6:

```
/usr/local/sbin/softflowd -v 9 -i interface -m 1000 -n[MonitorIPv6address]:port
$/usr/sbin/softflowd -v9 -i em0 -m 1000 -n[2001:a98:1f:f0::4]:9995
$/usr/sbin/softflowd -v9 -i em1 -m 1000 -n[2001:a98:1f:f0::4]:9996
$/usr/sbin/softflowd -v9 -i em2 -m 1000 -n[2001:a98:1f:f0::4]:9997
$/usr/sbin/softflowd -v9 -i em3 -m 1000 -n[2001:a98:1f:f0::4]:9998
$/usr/sbin/softflowd -v9 -i em4 -m 1000 -n[2001:a98:1f:f0::4]:9999
```

IPv4:

```
$/usr/local/sbin/softflowd -v 9 -i em0 -m 100000 -n10.1.4.4:9995
$/usr/local/sbin/softflowd -v 9 -i em1 -m 100000 -n10.1.4.4:9996
$/usr/local/sbin/softflowd -v 9 -i em2 -m 100000 -n10.1.4.4:9997
$/usr/local/sbin/softflowd -v 9 -i em3 -m 100000 -n10.1.4.4:9998
$/usr/local/sbin/softflowd -v 9 -i em4 -m 100000 -n10.1.4.4:9999
```

Netflow Kayıtlarının Saklanması ve Analizi İçin NfSen kurulumu

Bu bölümde Nfsen (Netflow Sensor) uygulamasının Linux işletim sistemi Ubuntu sürümü için kurulum ve gerekli ayarlar anlatılacaktır. Benzer şekillerde herhangi bir Linux dağıtımı ya da BSD işletim sisteminde de rahatlıkla kullanılabilir. (FreeBSD'de nfsen bir port olarak bulunmaktadır).

```
$ uname -a
Linux g0monitorubuntu 2.6.35-22-server #33-Ubuntu SMP Sun Sep 19 20:48:58 UTC
2010 x86_64 GNU/Linux
```

1-PHP e Apache

PHP ve Apache programlarının kurulumu için aşağıdaki komutlar kullanılır.

```
$ apt-get update
$apt-get install build-essential
$ apt-get install apache2
$ apt-get install php5 php5-cli
```

Kurulum tamamlandıktan sonra,“*.php*” dosyalarının sunucu tarafından işlenebilmesi için */etc/apache2/mods-available/dir.conf* dosyasında değişiklik yapılması gerekmektedir. Dosyanın son hali şu şekilde olmalıdır:

```
<IfModule mod_dir.c>
    #DirectoryIndex index.html index.cgi index.pl index.php index.xhtml index.htm
    DirectoryIndex index.html index.htm index.shtml index.cgi index.php index.php3
index.pl index.xhtml
</IfModule>
```

2-RRd Tools

RRd tools kurulumu için aşağıdaki komutlar kullanılmaktadır.

```
$ apt-get install rrdtool
$ apt-get install librrds-perl
$ apt-get install libpng12-dev libfreetype6-dev libart-2.0-dev bison flex
```

3-NfDump

Nfdump kurulumu için de aşağıdaki komutun girilmesi yeterlidir.

```
$apt-get install nfdump
```

Kurulumun sağlıklı olması için sunucu üzerinde kurulu Perl sürümü 5 ve üzeri olmalıdır. Bu nedenle *“perl –version”* komutu çalıştırılarak sürüm kontrol edilmeli, daha eski bir sürüm var ise yeni sürüm kurulumu yapılmalıdır.

Nfdump bazı Perl modüllerine ihtiyaç duymaktadır, aşağıda verilen modüllerin kurulumu yapılmalıdır.

```
$perl -MCPAN -eshell
cpan> install Mail::Header
cpan> install Mail::Internet
```

4-Nfsen

Adım adım Nfsen kurulumu ve ayarlarının bulunduğu belgelere *http://nfsen.sourceforge.net/* adresinden ulaşabilirsiniz.

Nfsen için belgenin hazırlandığı tarihte en güncel sürüm olan 1.3.5’i aşağıdaki adresten edinebilirsiniz.

http://sourceforge.net/projects/nfsen/files/stable/nfsen-1.3.5/nfsen-1.3.5.tar.gz/download

Nfsen kurulumuna geçmeden önce kaynak arşivi açılmalı ve varsayılan olarak gelen ayar dosyası *nfsen.conf* adıyla kopyalanmalıdır.

```
$tar zxvf nfsen-1.3.5.tar.gz
```

```
$cd nfsen-1.3.5
$cp etc/nfsen-dist.conf etc/nfsen.conf
$mkdir /data
```

İlgili ayar dosyasında aşağıdaki değişiklikler yapılmalıdır. Bu ayarların yapılması için *vi* editörü kullanılabilir.

```
$ vi etc/nfsen.conf
```

```
$BASEDIR = "/data/nfsen";
$HTMLDIR    = "/var/www/nfsen/";
$PREFIX  = '/usr/bin';
$USER    = "www-data";
$WWWUSER  = "www-data";
$WWWGROUP = "www-data";
%sources = (
   'kaynak1'    => { 'port' => '9995', 'col' => '#0000ff', 'type' => 'netflow' },
   'kaynak2'    => { 'port' => '9996', 'col' => '#ff00ff', 'type' => 'netflow' },
   'kaynak3'    => { 'port' => '9997', 'col' => '#ffff00', 'type' => 'netflow' },
   'kaynak4'    => { 'port' => '9998', 'col' => '#00ff00', 'type' => 'netflow' },
   'kaynak5'    => { 'port' => '9999', 'col' => '#00ffff', 'type' => 'netflow' },
);
```

```
:wq (değişiklikleri kaydederek çıkın)
```

Not: *"%sources"* bölümünde, Netflow bilgisini yollayan kaynakların ve akış izlerinin gönderildiği port numaralarının girilmesi gerekmektedir. Örnekte 5 ayrı ağ cihazından gönderilen ağ kayıtları için gerekli tanımlar yer almaktadır.

Bu dosyadaki değişiklikleri kayıt ettikten sonra Nfsen kurulumu yapılabilir. Kurulum için aşağıdaki komut kullanılır.

```
$./install.pl etc/nfsen.conf
```

Bu komut çalıştırıldığında, Nfsen tarafından kullanılacak Perl modülünün dizini sorulacaktır.

```
Perl to use: [/usr/bin/perl]
```

Sonrasında Nfsen'in kullanacağı php ve html dosyaları, *nfsen.conf* dosyasında belirlediğimiz hedef dizinlere kopyalanacak veya oluşturulacaktır.

Bu komut sonrasında *nfsen.conf* dosyasının CONFDIR altında da konduğunu bir kontrol edelim.

```
$ls -la /data/nfsen/etc/nfsen.conf
-rw-r--r-- 1 root www-data 9335 2011-03-25 14:27 /data/nfsen/etc/nfsen.conf
```

Nfsen index dosyası otomatik olarak oluşturulmadığından aşağıdaki komut ile bu sorun giderilebilir.

```
$echo -e "<?php\n\theader(\"Location: nfsen.php\");\n?>" >
```

```
/var/www/nfsen/index.php
```

Aşağıdaki komut ile Nfsen'i başlatabilir.

```
$/data/nfsen/bin/nfsen start
```

Nfsen'in doğru bir şekilde başlatıldığını ve yönlendirici tarafından yollanan kayıtların saklanmaya başlandığını doğrulamak için aşağıdaki komutlar kullanılabilir.

```
$cd /data/nfsen/profiles-data/live/kaynak1/
$ls -la nfcapd.current
-rw-r--r-- 1 www-data www-data 276 2011-03-31 10:25 nfcapd.current
```

Nfcapd.current dosyası en güncel trafik izlerinin saklandığı dosyadır ve eğer akış izleri doğru bir şekilde saklanıyorsa büyüklüğü artmalıdır. Bu dosya her 5 dakikada bir yine */data/nfsen/profiles-data/live/kaynak1* dizini altında oluşturulmuş olan *yıl/ay/gün* şeklindeki dizine *nfcapd.yılaygunsaat* formatında kopyalanacaktır.

```
$cd /data/nfsen/profiles-data/live/kaynak1/2011/03/31
$ls
nfcapd.201103310000  nfcapd.201103310145  nfcapd.201103310330
nfcapd.201103310515  nfcapd.201103310700  nfcapd.201103310845
nfcapd.201103310005  nfcapd.201103310150  nfcapd.201103310335
nfcapd.201103310520  nfcapd.201103310705  nfcapd.201103310850
nfcapd.201103310010  nfcapd.201103310155  nfcapd.201103310340
nfcapd.201103310525  nfcapd.201103310710  nfcapd.201103310855
nfcapd.201103310015 nfcapd.201103310200  nfcapd.201103310345
nfcapd.201103310530  nfcapd.201103310715  nfcapd.201103310900
nfcapd.201103310020  nfcapd.201103310205  nfcapd.201103310350
nfcapd.201103310535  nfcapd.201103310720  nfcapd.201103310905
nfcapd.201103310025  nfcapd.201103310210  nfcapd.201103310355
nfcapd.201103310540  nfcapd.201103310725  nfcapd.201103310910
```

Nfsen'in bilgisayar her açıldığında başlatılması için */etc/rc.local* dosyasına */data/nfsen/bin/nfsen* start satırının eklenmesi gerekmektedir.

Kullandığınız profile'ın şu an ki durumunu izlemek için aşağıdaki komutu kullanabilirsiniz.

```
$/data/nfsen/bin/nfsen -l live
name live
tstart Wed Mar 28 16:55:00 2007
tend Thu Mar 29 10:15:00 2007
updated Wed Mar 28 16:50:00 2007
filter <none>
expire 0 hours
```

```
size 0
maxsize 0
sources deneme
type live
locked 0
status OK
```

Eğer locked değeri 1 ise aşağıdaki komut ile tekrar analiz başlatılabilir.

```
$./nfsen -m live -U
```

Tüm nfsen komutları */data/nfsen/bin* altında çalıştırıldığından bu dizini genel yola (PATH) eklemek faydalı olabilir:

```
$export PATH=$PATH:/data/nfsen/bin
```

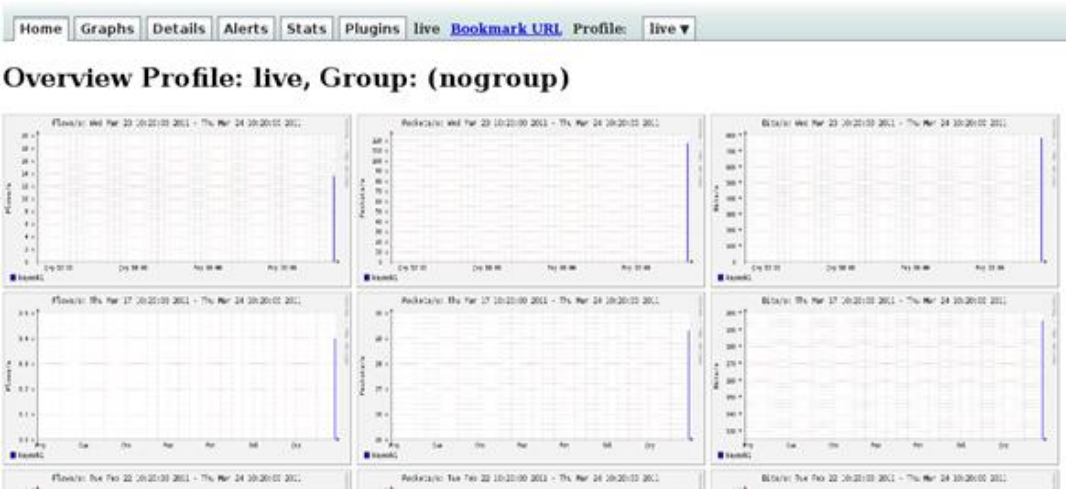
Yeni kaynakların ağ izlerinin depolanması ve işlenmesi istendiğinde */data/Nfsen/etc/nfsen.conf* dosyasında değişiklik yapılması gerekmektedir. Bu değişiklerin geçerli olması için *nfsen.conf* dosyası kayıt edildikten sonra aşağıdaki komut ile Nfsen yeniden yapılandırılmalıdır.

```
$/data/nfsen/bin/nfsen reconfig
```

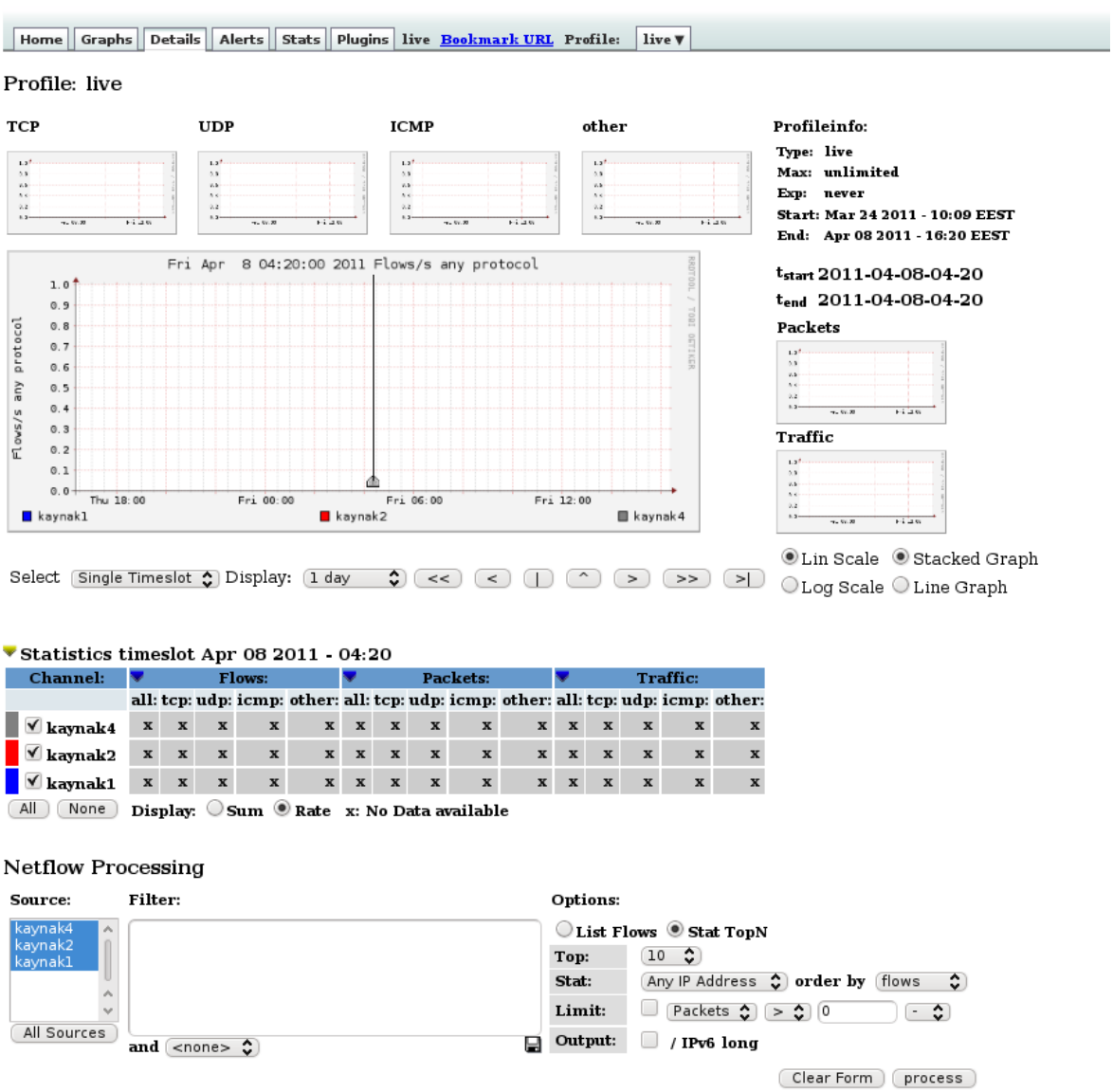
NfSen ile Analiz

Nfsen kurulu sunucu üzerinden *http://localhost/nfsen/nfsen.php* adresi ile, IPv4 uzak istemcilerinden *http://10.1.4.4/nfsen/nfsen.php* adresi ile ya da IPv6 uzak istemcilerinden *http://[2001:a98:1f:f0::4]/nfsen/nfsen.php* adresi görüntülediğinde NfSen arayüzüne ulaşılacaktır (Şekil 34).

Şekil 35 de görülen Details bölümünden, grafik üstünde ilgilendiğimiz zaman aralığını seçerek ilgili kayıtlar ayıklanabilir. Bunun için sayfanın alt bölümünde yer alan Netflow Processing bölümünün kullanılması gerekmektedir. Source bölümde ayarlar dosyasında UDP portlarına göre ayrılmış olan kaynaklar listelenir.



Şekil 34: Nfsen Giriş Sayfası



Şekil 35: Nfsen Üzerinden Kayıtların Ayıklanması

Buradan bir kaynak seçtikten sonra Filter bölümde özel olarak ilgilenilen bir kayıt bölümü için (IP adresi, arayüz, AS, Port v.s) filtreleme yapılabilir. Bu alanın kullanım şekli Nfdump verisinin kullanım şekli ile aynıdır.

Aşağıdaki adres filter bölümünde ayıklama ile ilgili detaylar içermektedir.

(*http://nfdump.sourceforge.net/)*

Bazı alanlar için filtreleme yöntemleri şöyledir. Başlıkların altında verilen komutlar teker teker ya da birlikte Filters bölümüne yazılarak ilgili başlığa göre filtreleme yapılabilir. Filtreleri beraber uygulamak için aşağıdaki yazım şekli kullanılabilir.

(Filtre1) and (Filter2) (Filtre1) or (Filtre2)

Protokol sürümü:

Ipv4 **ipv4** Ipv6 **ipv6**

Protokol tipi:

TCP, UDP, ICMP, GRE, ESP, AH, RSVP yada PROTO <protokol_numarası>

IP Adresi:

Kaynak Ipsi için: **IP a.b.c.d** Kaynak ya da hedef: **HOST a.b.c.d**

Ağ Adresi:

NET a.b.c.d m.n.r.s (m.n.r.s ağ maskesi) **NET a.b.c.d / num** (Ya da / gösterimi ile)

Port Numarası:

PORT [**operator**] **port_no** (operator olarak =,>,< kullanılabilir)

Yönlendiricideki Ağ Arayüzü:

[inout] **IF arayuz_no** (başına eklenecek in ya da out ile trafiğin yönünü debelirtebilirsiniz)

Kayıtta Yer Alan Paket Sayısı:

packets [operator] **sayı** [scale] (scale değeri **k,m,g** olabilir. Kilo, mega ve giga için)

Byte değerine göre:

bytes [operator] **sayı** [scale]

Saniyedeki Paket Sayısı: (Packets per second):

pps [operator] **num** [scale]

Trafik izinin oluştuğu süre:

duration [operator] num

Saniyelik Bite Göre (Bits per second):

bps [operator] **num** [scale]

Paketlerine Byte cinsinden büyüklüğüne göre (Bytes per packet):

bpp [operator] **num** [scale]

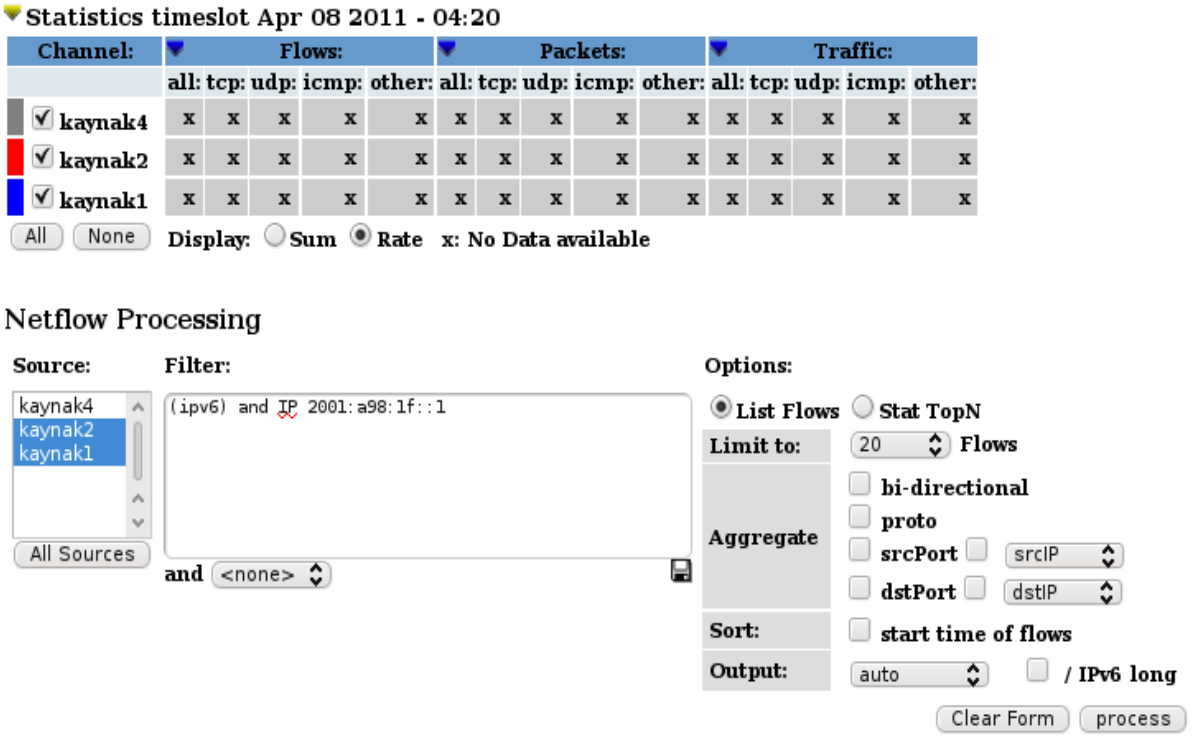
AS numarası

[SourceDestination] **AS sayı**

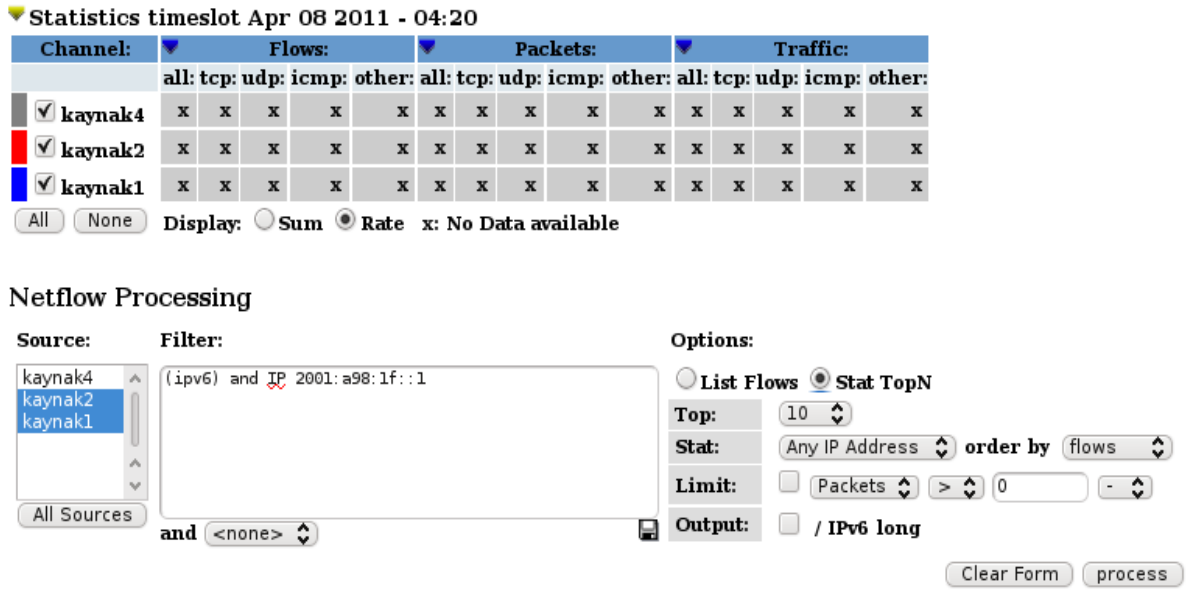
Akış izinin kaynağı ve üzerinde uygulanacak filtreler belirlendikten sonra "Process" seçeneği seçilerek kayıtlar işlenebilir. Bu aşamada da iki adet seçenek bulunmaktadır: List ve Stat TopN (Şekil 36 ve Şekil 37).

List seçeneğini seçilen kaynaktan gelen akış izlerine hazırladığınız filtrenin uygulanmasını ve sonuçların görüntülenmesini sağlamaktadır. Sonuçlarda yer alacak izlerin sayısını ve formatını belirlemenin yanında, ortaya çıkan bu izleri "Aggregate" bölümünde seçtiğiniz bir başlık bölümüne göre (kapı, hedefe ya da kaynak IP adresi) saydırılabilir. Bu seçeneğin en temel kullanımı belirli bir zaman aralığında bir IP adresine ait trafik izlerinin izlenmesidir.

Akış izlerinin işlenmesinde ikinci seçenek olan Stat TopN istatistik bilgilerini sağlamaktadır. Seçilen zaman aralığında kapılar ya da IP adresleri oluşturdukları flow, paket ya da trafik büyüklüğüne göre listelenebilmektedir. Kaynak IP, hedef IP, Kapı, AS numarası v.s. için çıkacak istatistikler byte, ağ izi sayısı, pps v.s. için sıralatılabilir.



Şekil 36: List Flow



Şekil 37: Stat TopN

Önemli Not:

Üzerinde çalışılan ağ ile ilgili tüm trafiğin bilgilerini barındıran akış izlerinin tutulması ve analiz edilmesi ağ yönetimi için çok önemlidir. Bununla birlikte bu kayıtlar hassas bilgiler içerdiğinden ağ yöneticileri dışındaki kişilerin erişimine izin verilmemelidir. Bunun için en pratik çözüm olarak *.htaccess* dosyası yardımı ile web sunucusuna erişimi kullanıcı tabanlı yapmaktır. Ayrıca sunucuya ssh erişimini kısıtlamak için gerekli tanımlar yapılmalıdır.

KAYNAKLAR:

- A. Conta, S. Deering, “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”, RFC2463, Aralık 1998
- Alan Adı Sunucusu – DNS, http://en.wikipedia.org/wiki/Domain_Name_System, Şubat 2011 tarihinde erişilmiştir.
- Apache Web Sunucusu, http://httpd.apache.org/docs/2.0/tr/bind.html, Şubat 2011 tarihinde erişilmiştir.
- B. Carpenter, K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, Şubat 2001
- BIND Yapılandırması, http://www.isi.edu/~bmanning/v6DNS.html, Şubat 2011 tarihinde erişilmiştir.
- Bradner, B., Mankin, A., “The Recommendation for the IP Next Generation Protocol”, RFC 1752, Ocak 1995
- C. Hopps, "Routing IPv6 with IS-IS", RFC 5308, Eylül 2008
- C. Huitema, "An Anycast Prefix for 6to4 Relay Routers", RFC 3068, Haziran 2001
- C. Huitema, “Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)”, RFC 4380, Şubat 2006
- Cisco, “6Bone Connection Using 6to4 Tunnels for IPv6”, Şubat 2011 tarihinde erişilmiştir.
- D. Kegel, "NAT and Peer-to-Peer Networking", http://www.alumni.caltech.edu/~dank/peer-nat.html, Temmuz 1999
- E. Davies, S. Krishnan, P. Savola, “IPv6 Transition/Coexistence Security Considerations”, RFC 4942, Eylül 2007
- E. Nordmark, R. Gilligan, “Basic Transition Mechanisms for IPv6 Hosts and Routers”, RFC 4213, Ekim 2005
- E.Nordmark, "Stateless IP/ICMP Translation Algorithm (SIIT)", RFC 2765, Şubat 2000
- G. Malkin, R. Minnear, "RIPng for IPv6", RFC 2080, Ocak 1997
- Getting Connected with 6to4, http://onlamp.com/pub/a/onlamp/2001/06/01/ipv6_tutorial.html?page=3, Şubat 2011 tarihinde erişilmiştir.
- Information Sciences Institute University of Southern California, "Internet Protocol DARPA Internet Program Protocol Specification", RFC 791, Eylül 1981
- Internet Protocol Version 6 Address Space, http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml#note2, Şubat 2011 tarihinde erişilmiştir.
- IPv4 address exhaustion, http://en.wikipedia.org/wiki/IPv4_address_exhaustion, Şubat 2011 tarihinde erişilmiştir.

- IPv6 configuration for Windows, http://6to4.version6.net/?show_ip=172.16.30.213&lang=en_GB, Şubat 2011 tarihinde erişilmiştir.
- IPv6 configuration guide for FreeBSD users, http://www.kame.net/~suz/freebsd-ipv6-config-guide.txt, Şubat 2011 tarihinde erişilmiştir.
- IPv6 Day, Teredo Servers, http://www.ipv6day.org/action.php?n=En.GetConnected-Teredo
- J. Amoss, D. Minoli, "Handbook of IPv4 to IPv6 Transition, Methodologies for Institutional and Corporate Networks", 2008 by Taylor & Francis Group
- J. Arkko, Ed., J. Kempf, B. Zill, P. Nikander, “Secure Neighbor Discovery (SEND)”, RFC 3971, Mart 2005
- J. Davies, “TCP/IP Fundamentals for Microsoft Windows Chapter 15 – IPv6 Transition Technologies”, Kasım 2006, http://technet.microsoft.com/en-us/library/bb727021.aspx
- J. Hagino, K. Yamamoto, “An IPv6-to-IPv4 Transport Relay Translator”, RFC 3142, Haziran 2001
- J. Jeong, S. Park, L. Beloeil, S. Madanapalli, "IPv6 Router Advertisement Option for DNS Configuration", RFC 5006, Eylül 2007
- Kamu Kurum ve Kuruluşları için IPv6’ya Geçiş Planı, http://www.resmigazete.gov.tr/eskiler/2010/12/20101208-7.htm, Şubat 2011 tarihinde erişilmiştir.
- M. Allman, S. Ostermann, C. Metz, "FTP Extensions for IPv6 and NATs", RFC 2428, Ekim 1998
- Miredo : Teredo IPv6 tunneling for Linux and BSD, http://www.remlab.net/miredo, Şubat 2011 tarihinde erişilmiştir
- OpenBSD Manual Pages, “faith - IPv6-to-IPv4 TCP relay capturing interface”, http://www.openbsd.org/cgi-bin/man.cgi?query=faith&sektion=4, Şubat 2011 tarihinde erişilmiştir.
- P. Marques, F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing", RFC 2545, Mart 1999
- P. Nikander, Ed., J. Kempf, E. Nordmark, “IPv6 Neighbor Discovery (ND) Trust Models and Threats”, RFC 3756, Mayıs 2004
- P. Savola, C. Patel, “Security Considerations for 6to4”, RFC 3964, Aralık 2004
- P. Srisuresh, B. Ford, D. Kegel, “State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)”, RFC 5128, Mart 2008
- Postfix E-Posta Sunucusu, http://www.postfix.org/IPV6_README.html, Şubat 2011 tarihinde erişilmiştir.
- Q. Zheng et al., “A New Worm Exploiting IPv4-IPv6 Dual-stack Networks”, Proc. 5th ACM CCS WORM’07, Kasım 2007

- Quagga Routing Software Suite, GPL licensed IPv4/IPv6 routing software. http://www.quagga.net, Şubat 2011 tarihinde erişilmiştir.
- R. Coltun, D. Ferguson, J. Moy, A. Lindem, "OSPF for IPv6", RFC 5340, Temmuz 2008
- R. Draves, “Default Address Selection for Internet Protocol version 6 (IPv6)”, RFC 3484, Şubat 2003
- R. Hinden, S. Deering, “Internet Protocol Version 6 (IPv6) Addressing Architecture”, RFC3513, Nisan 2003
- R.Droms,J.Bound, B.Volz, T.Lemon, C.Perkins, M.Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, Temmuz 2003
- S. Kawamura, M. Kawashima, “A Recommendation for IPv6 Address Text Representation”, RFC5952, Ağustos 2010
- S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, Kasım 1998
- S.Deering, R.Hinden, "Internet Protocol, Version 6 (IPv6)Specification", RFC 2460, Aralık 1998
- S.Thomson, T.Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, Aralık 1998
- Softflowd, Flow analiz aracı, http://www.mindrot.org/projects/softflowd, Şubat 2011 tarihinde erişilmiştir.
- Source and Destination Address Selection for IPv6, Şubat 2006, http://www.microsoft.com/technet/community/columns/cableguy/cg0206.mspx
- Tcpdump Ağ trafiği analiz aracı, http://www.tcpdump.org, Şubat 2011 tarihinde erişilmiştir.
- The Faith TRT for FreeBSD and NetBSD, http://www.networkdictionary.com/Networking/Faith-TRT-FreeBSD-and-NetBSD.php
- The IPv6 Portal, “Connectivitiy Teredo”, http://www.ipv6tf.org/index.php?page=using/connectivity/teredo, Şubat 2011 tarihinde erişilmiştir.
- The IPv6 Portal, “Connectivity 6to4 configuration”, http://www.ipv6tf.org/index.php?page=using/connectivity/6to4, Şubat 2011 tarihinde erişilmiştir.
- Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi Web Sitesi, http://www.ipv6.net.tr, , Şubat 2011 tarihinde erişilmiştir.
- W. Dale, “IPv6 6to4 Relay Routing Service”, http://helpdesk.doit.wisc.edu/ns/page.php?id=9462, Haziran 2009
- RFC 1035, DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, http://www.ietf.org/rfc/rfc1035.txt
- RFC 2671, Extension Mechanisms for DNS (EDNS0), http://www.ietf.org/rfc/rfc2671.txt

- RFC 2672, Non-Terminal DNS Name Redirection, http://www.ietf.org/rfc/rfc2672.txt
- draft-ietf-behave-dns64-06, DNS64: DNS extensions for Network Address Translation from IPv6 Clients to IPv4 Servers, http://www.viagenie.ca/ietf/draft/draft-ietf-behave-dns64-06.txt
- draft-ietf-behave-v6v4-framework-06, Framework for IPv4/IPv6 Translation, http://www.viagenie.ca/ietf/draft/draft-ietf-behave-v6v4-framework-06.txt
- draft-ietf-behave-v6v4-xlate-09, IP/ICMP Translation Algorithm, http://www.viagenie.ca/ietf/draft/draft-ietf-behave-v6v4-xlate-09.txt
- draft-ietf-behave-v6v4-xlate-stateful-08, Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, http://www.viagenie.ca/ietf/draft/draft-ietf-behave-v6v4-xlate-stateful-08.txt
- http://tr.wikipedia.org/wiki/SNMP