

IPv6 EL KİTABI

Şubat 2011

[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 bilgiler barındırmaktadır.]

İÇİNDEKİLER

İÇİNDEKİLER.....	2
Bölüm 1: Giriş	1
IPv6 Nedir?.....	1
IPv4'ün Eksiklikleri.....	1
IPv6'nın Avantajları	2
IPv6 Güvenliği	4
Türkiye'de IPv6 ile ilgili Yürütülen Çalışmalar:.....	4
Bölüm 2: IPv6 Temelleri	8
IPv6 Adres Mimarisi.....	8
IPv6 Adres Tipleri.....	9
IPv6 Başlık Yapısı:.....	12
Bölüm 3: IPv6 Ağ Yapılandırması.....	15
IPv6 Adres Tanımlama	15
Durum Denetimsiz Otomatik Adres Yapılandırması:	15
Durum Denetimli Otomatik Adres Yapılandırması: DHCP	16
Statik adres tanımlanması.....	17
ALAN ADI SERVİSİ - DNS.....	18
DNS SUNUCU AYARLARI.....	18
İSTEMCİLERDE DNS AYARLARI	19
YÖNLENDİRME PROTOKOLLERİ	20
Bölüm 4: IPv6 Temel Servisleri	23
WEB SERVİSİ.....	23
E-POSTA SERVİSİ	24
FTP SERVİSİ	25
SSH ve SECURE FTP SERVİSİ	26
TCP_WRAPPER DESTEĞİ	27
Bölüm 5: IPv6 Geçiş Yöntemleri	28
İkili Yığın Geçiş Yöntemi.....	28

İkili Yığın Bileşenleri.....	30
İkili Yığın Yapılandırması.....	30
6to4 Geçiş Yöntemi.....	32
6to4 Yöntemi Bileşenleri.....	33
6to4 İletişim Örnekleri	35
6to4 Yapılandırması	37
Teredo Geçiş Yöntemi.....	38
Teredo Yöntemi Bileşenleri.....	40
Teredo İletişim Örnekleri	40
Teredo Yapılandırması	42
TRT (Transport Relay Translator) Geçiş Yöntemi.....	45
TRT Ağ Yapısı	46
Faithd Yapılandırması.....	46
Kaynaklar:	48

BÖLÜM 1: GİRİŞ

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 (İnternet Engineering Task Force) önderliğinde başlamış ve yeni protokolün IPng (İnternet Protocol next generation) veya İnternet protokolü sürüm 6 (IPv6) olarak adlandırılması kararlaştırılmıştır. Yeni İnternet protokolünün standartları 1998 yılı sonunda yayınlanan RFC 2460 dokümanında 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 IPv6 adreslerinin dağıtım koordinasyonu ile görevli merci olan İnternet 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 İnternet Registries) paylaşmıştır. 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. Fakat 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 Network Adress 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 çok 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 kapsamıyla, yönlendirici trafiği ve yönlendirilecek paket sayısı çok artmıştır. Bu nedenle günümüzde veri işleme hızı önem kazanmıştır. Bir başka deyişle yönlendirmenin veya anahtarlamının 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 nedenle 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 ek başlıklar 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 etkilemez.

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 testinden (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 ek başlıklar 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 Internet Control Message Protocol for IPv6 (ICMPv6) kullanılır. Bu protokol mesajları 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.

IPv6 Güvenliği

IPv6, sahip olduğu diğer avantajların yanı sıra, IPv4’te seçimli olan IPSec desteğinin zorunlu olması gibi özellikler sayesinde IPv4’e oranla daha güvenli olarak değerlendirilmektedir. Bu özellikler, keşif saldırılarına ve IP adreslerini tarayarak yayılan solucanlara karşı direnci artırmakla birlikte, aynı zamanda yeni saldırı yöntem ve araçlarının da ortaya çıkması beklenmektedir. Ayrıca, IPv6 kullanımının henüz yaygınlaşmamış olması, protokol yaygın kullanıldığında IPv6 protokol yapısı ve kullanılan geçiş yönteminden kaynaklanabilecek güvenlik riskleri konusunda belirsizliğe neden olmaktadır.

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.

Türkiye’de IPv6 ile ilgili Yürütülen Çalışmalar:

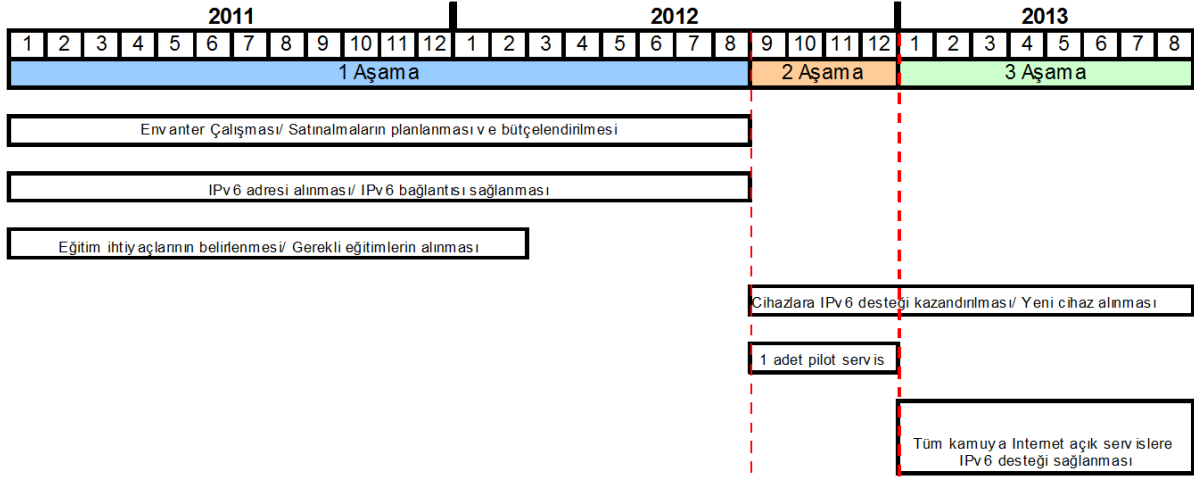
Türkiye’de IPv6 kullanımının yaygınlaştırılması ile ilgili çalışmalar Ulusal Akademik Ağ ULAKNET’in yönetiminden ve işletiminden sorumlu TÜBİTAK ULAKBİM tarafından

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 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 dahil edilmesi sağlanmıştır.

Türkiye'de IPv6 bilgi birikimine katkı sağlamak amacıyla, 2007 yılında Bilgi Teknolojileri ve İletişim Kurumu (BTK) koordinasyonu ile "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 Geçiş 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 karşılaşılabilecek muhtemel yönetim ve güvenlik problemlerine yönelik çözüm önerileri geliştirilmiştir. Proje kapsamında tüm kamu ve İnternet Servis Sağlayıcı kurumlara IPv6 geçiş konusunda anket çalışması yapılmıştır. Ankette kurumlara teknik personel, IPv6 destekli ve destekli olmayan 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, bunlardan 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 dahil edilecektir.

1.3. Kamu kurum ve kuruluşları en geç 31 Ağustos 2012 tarihi itibarıyla 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.

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 metodolojilerine 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 arayüze iletilmektedirler.
- **Çoklu Gönderim (Multicast) Adresleri:** Bu tip adresler, farklı arayüzlerden oluşturulmuş bir grubu tanımlamak için kullanılmaktadır. Hedefi çoklu gönderim adresi olan paketler, gruba dahil olan tüm arayüzlere iletilmektedir.
- **Herhangi Birine Gönderim (Anycast) Adresleri:** Herhangi birine gönderim adresleri de çoklu gönderim adresleri gibi, farklı arayüzlerden oluşturulmuş bir grubu tanımlamaktadır. Herhangi birine gönderim adresine yönelmiş bir paket, çoklu gönderimden farklı olarak sadece grubun en yakındaki üyesine iletilir. Bu adres tipleri özellikle yük dağılımı uygulamalarında kullanılır. Aynı servisi veren birden fazla sunucu bulunması durumunda bu sunucuları aynı gruba dahil 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 Ön eki (İkili Değer)	IPv6 Adres aralığı	Toplam Adres Aralığındaki Oranı	Toplam Adres Aralığındaki Oranı
Rezerve edilmiş	0000 0000	0::/8	1/256	%0.39
Küresel Tekil Gönderim (Global Unicast) Adresleri	001	2000::/3	1/8	%12.5

Atama	Biçim Ön eki (İkili Değer)	IPv6 Adres aralığı	Toplam Adres Aralığındaki Oranı	Toplam Adres Aralığındaki Oranı
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 durumda olan 0::/8 aralığı aşağıda açıklanan özel IPv6 adresleri için kullanılmaktadır.

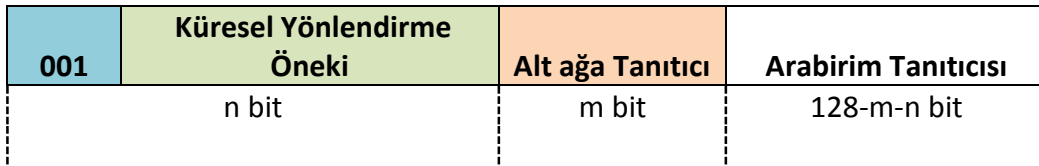
Belirsiz Adres (Unspecified Address): 0:0:0:0:0:0:0:0 veya :: şeklinde gösterilen ve IPv4'teki karşılığı 0.0.0.0 olan adrestir. Belirsiz Adres herhangi bir cihaza verilemez. Bu adres genelde soket bağlantılarında kullanılmaktadır.

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 ayrılmaz.

IPv4 Eşlemlili IPv6 Adresleri (IPv4-Mapped Addresses): ::ffff:0:0/96 aralığı içerisinde yer alan IPv6 adresleridir. Bu adres aralığı, IPv4 ve IPv6 paket başlıkları arasında RFC 2765 ile tanımlanan SITT (Stateless IP/ICMP Translation) algoritmasını kullanarak dönüşüm sağlamak için ayrılmıştır. Bu algoritma, sadece IPv6 adresine sahip arayüzlerin, sadece IPv4 adresine sahip arayüzler ile iletişimini sağlamak için kullanılmaktadır. Adres dönüşümünde kullanılan IPv4 adresinin küresel olarak yönlendirilebilen adresler olması gerekmektedir. Ancak bu dokümanda yer alan adres dönüşümü örneğinde IPv4 adresi olarak 192.168.0.5 kullanılacaktır. Bu IPv4 adresinin 16'lık sistemde gösterimi COA8:0005 şeklindedir. Dolayısıyla bu adres için IPv4 eşlemlili IPv6 adresi ::ffff:0:COA8:5 olur.

Küresel Tekil Gönderim Adresleri: 001 biçim ön ekine 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 Ön Eki" ve "Küresel Yönlendirme Ön Eki" nden 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

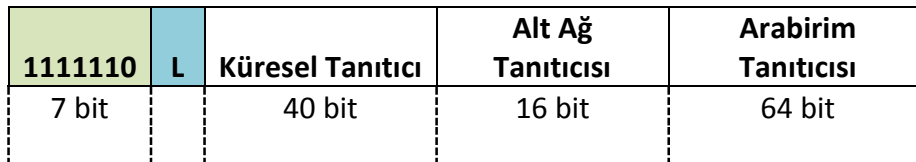
olmakla birlikte bu örnek için 16 bittir. Son bölüm olan “Arabirim Tanıtıcısı” ise genellikle 64 bitliktir.



Şekil 2: Küresel Tekil Gönderim Adres Yapısı

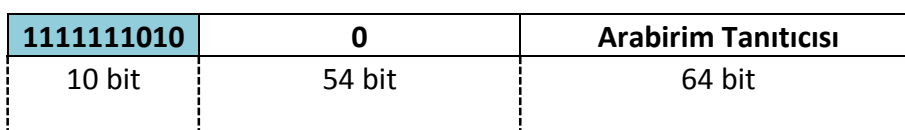
Küresel tekil gönderim adresleri arasından yer alan 2001::/32 adres aralığı IPv4 ve IPv6 arayüzleri arasında iletişim için kullanılan özel bir geçiş mekanizması olan Teredo Tünelleme yöntemi için ayrılmış durumdadır. Bunun yanı sıra 2002::/16 aralığı 6to4 geçiş yöntemi için ayrılmıştır.

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 ağ yöneticileri tarafından 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.



Şekil 3: Eşsiz Yerel Tekil Gönderim Adres Yapısı

Bağlantı Yerel Tekil Gönderim Adresleri: 1111 1110 10 biçim ön ekine sahip ve FE80 ile başlayan adreslerdir. Biçim ön ekini 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.



Şekil 4: Bağlantı Yerel Tekil Gönderim Adres Yapısı

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

11111111	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:

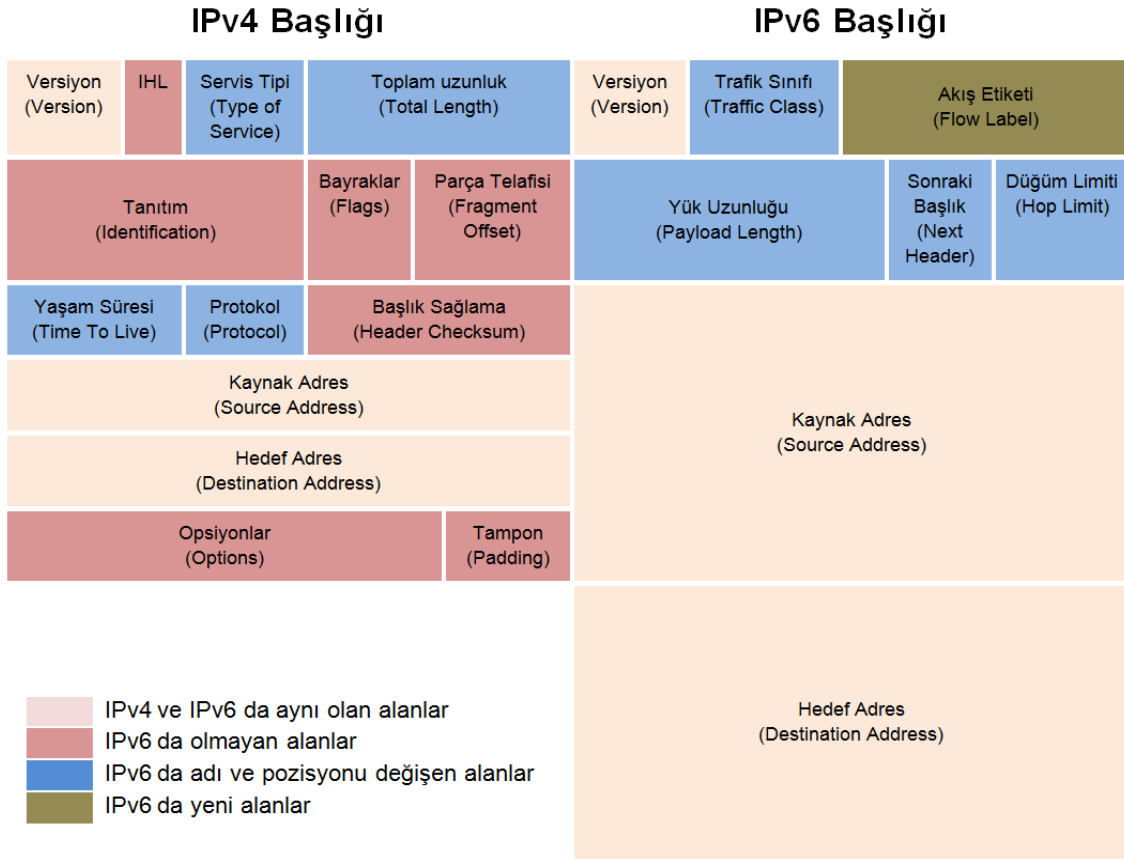
- Bayrak bölümündeki ilk bit = 0 → adres geçicidir.
- Bayrak bölümündeki ilk bit = 1 → adres kalıcıdır.
- Kapsam bölümündeki bitlerin değeri = 1 → adres arayüz-yerel bir adrestir.
- Kapsam bölümündeki bitlerin değeri = 2 → adres bağlantı-yerel bir adrestir.
- Kapsam bölümündeki bitlerin değeri = 4 → adres yönetici-yerel bir adrestir.
- Kapsam bölümündeki bitlerin değeri = 5 → adres site-yerel bir adrestir.
- Kapsam bölümündeki bitlerin değeri = 8 → 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 başlık yapısındaki en önemli yeniliklerden biri, içerisindeki alanlarda henüz tanımlanmamış ve ihtiyaç anında geliştirilecek yeni uygulamalara destek amaçlı kullanılacak alanların bulunmasıdır. Ayrıca IPv4 başlık bilgisinin hantal olan yapısı revize edilmiş, gereksiz olan ya da görevleri üst katmanlara devredilebilen kısımlar çıkarılmıştır. Günümüz ağlarının gereksinimlerini karşılamak için adres bilgisi ile ilgili kısımlar da genişletilmiştir. Başlık yapıları incelendiğinde, IPv6 ve IPv4 protokolleri arasındaki farklar daha açık bir şekilde ortaya çıkmaktadır (Şekil 6).



Şekil 6: IPv4 ve IPv6 Başlık Yapısı

Her iki protokolde de bulunan 4 bitlik “Versiyon” 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 opsiyonel 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 değişikliklerinden biri de yönlendirici gibi ara elemanlarda parçalama (Fragmentation) ve hata kontrolü yapılmamasıdır. Bu görevler bir üst seviyedeki protokol olan TCP’ye bırakılmıştır. Bu değişiklik sayesinde bu işlevleri yerine getirmekte kullanılan “Tanıtım”, “Bayraklar”, “Parça Telafisi” ve “Başlık Sağlama” bölümleri IPv6’da yer almamaktadır.

8 bitlik “Yaşam Süresi” ve “Düğüm Limiti” bölümleri farklı adlandırılmış olsalar da aynı işlevi görmektedirler. Bu bölüm bir veri paketinin bilgisayar ağı 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 “Ek Başlıklar” (Extension Headers) kısmı ile ilgili bilgiler de taşıyabilmektedir. IPv6’ın sunduğu ek özelliklerden olan ve ihtiyaç anında opsiyonel olarak kullanılabilen “Ek Başlıklar” kısmı standart IPv6 başlık yapısının dışına çıkarılarak, ağ cihazlarının paketleri daha hızlı yönlendirmesi sağlanmıştır.

BÖLÜM 3: IPV6 AĞ YAPILANDIRMASI

IPv6 Adres Tanımlama

İnternet Protokol sürüm 6 adreslerinin otomatik tanımlanması, Durum Denetimli (Stateful) veya Durum Denetimsiz (Stateless) olmak üzere iki şekilde yapılabilir. Durum Denetimsiz Otomatik Adres Yapılandırması RFC 2462’de tanımlanmış olup, ağ üzerinde yer alan yönlendiricinin ağa sürekli olarak gönderdiği bilgiler aracılığı ile yapılır. Durum Denetimli Otomatik Adres Yapılandırması ise, RFC 3315 ile tanımlanmış olan Dinamik İstemci Kontrol Protokolü (DHCP) kullanılarak yapılabilir. Otomatik adres tanımlamanın yanı sıra, istemcilere statik olarak IPv6 adreslerinin tanımlanması da mümkündür.

Durum Denetimsiz Otomatik Adres Yapılandırması:

Ağ üzerinde Yönlendirici Keşif Mesajları gönderen bir yönlendirici bulunuyor ise, IPv6 ağına bağlanan bir istemci bu mesajları kullanarak otomatik adres yapılandırması yapabilir. İstemci ağa bağlandığında, bağlantı-yerel adresini kullanarak yönlendirici talep (router solicitation) mesajını çoklu gönderim adresi üzerinden gönderir. Doğru yapılandırılmış yönlendirici bu talebe, ağ katmanındaki yapılandırma parametrelerini içeren bir mesaj ile cevap verir ve istemcinin doğru parametrelerle ağa otomatik olarak bağlanması sağlanır.

Cisco yönlendiriciler üzerinde, ilgili arayüz altında “ipv6 nd” komut seti ile duyurusu yapılacak adres öneki tanımlanır. Örneğin, 2001:db8:1:2::/64 öneki için Cisco yönlendirici üzerine girilecek komutlar aşağıdaki gibidir.

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

Linux ve BSD yönlendiricileri üzerinde, rota bilgilendirme sunucusu olarak radvd kullanılır. radvd yapılandırması genellikle /etc/radvd.conf dosyası ile yapılır. 2001:db8:1:2::/64 öneki için örnek yapılandırma dosyası, aşağıdaki gibidir:

```
interface eth0
{
  AdvSendAdvert on;
  MinRtrAdvInterval 3;
  MaxRtrAdvInterval 10;
  prefix 2001:db8:1:2::/64
  {
    AdvOnLink on;
    AdvAutonomous on;
    AdvRouterAddr on;
  };
};
```

[Durum Denetimli Otomatik Adres Yapılandırması: DHCP](#)

Durum denetimli adres yapılandırılması, Dinamik İstemci Kontrol Protokolü sürüm 6 DHCPv6 aracılığı ile kullanılabilir. IPv6 ağlarında DHCP kullanılmasına sebep olabilecek bazı durumlar:

- Durum denetimsiz adres yapılandırmasına uygun olmayan uygulamaların kullanımına olanak vermek,
- 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.

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;
    };
};
```

Statik adres tanımlanması

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 ara yüzü 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 kurulmuş 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
```

ALAN ADI SERVİSİ - 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 AYARLARI

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:

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 kullanımımızdır.

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

YÖNLENDİRME PROTOKOLLERİ

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)

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 4: IPV6 TEMEL SERVİSLERİ

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.

WEB SERVİSİ

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 olarak 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 eşlemlili 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,

```
Listen 0.0.0.0:80
```

satırı girilmelidir.

E-POSTA SERVİSİ

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 değişiklikler yapılabilir:

/etc/postfix/main.cf dosyası:

```
# You must stop/start Postfix after changing this parameter.
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:

```
/etc/postfix/main.cf:
smtp_bind_address6 = 2001:db8:2:1::1
```

Sendmail, varsayılan ayarlarında IPv6 desteklemekte olup, ayarları IPv4 ayarları 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 SERVİSİ

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.

Proftpd, yaygın olarak kullanılan dosya transfer protokolü yazılımıdır. Proftpd 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. Proftpd'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 diğerk ftp sunucu yazılımı olan vsftpd FTP sunucusu da IPv6 desteklemektedir. Varsayılan ayarlarla, sunucu üzerindeki tüm IP adresleri üzerinden FTP servisini veren yazılımın, IPv6 desteğı için, yapılandırma dosyası olan *vsftpd.conf* dosyasında ağıdaki satır bulunmalıdır.

/etc/vsftpd/vsftpd.conf dosyası:

```
listen_ipv6=yes
```

SSH ve SECURE FTP SERVİSİ

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 ağıdaki 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 DESTEĞİ

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 5: 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 yapılandırılabilecektir. 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)

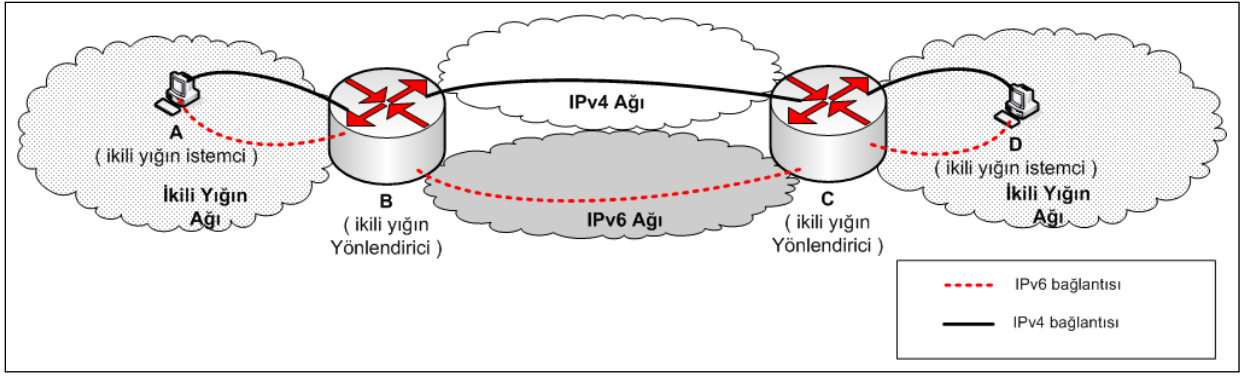
İkili yığın geçiş yönteminin, güvenlik ve performans açısından en uygun geçiş yöntemi olup, çeşitli nedenler ile bu yöntemin kullanılmadığı durumlarda tünelleme ve çevirici yöntemleri kullanılabilir. Tünelleme yöntemlerindeki başlıca problemler tünel uçları arasındaki trafiğin izlenmesi ve kontrol edilmesinin 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

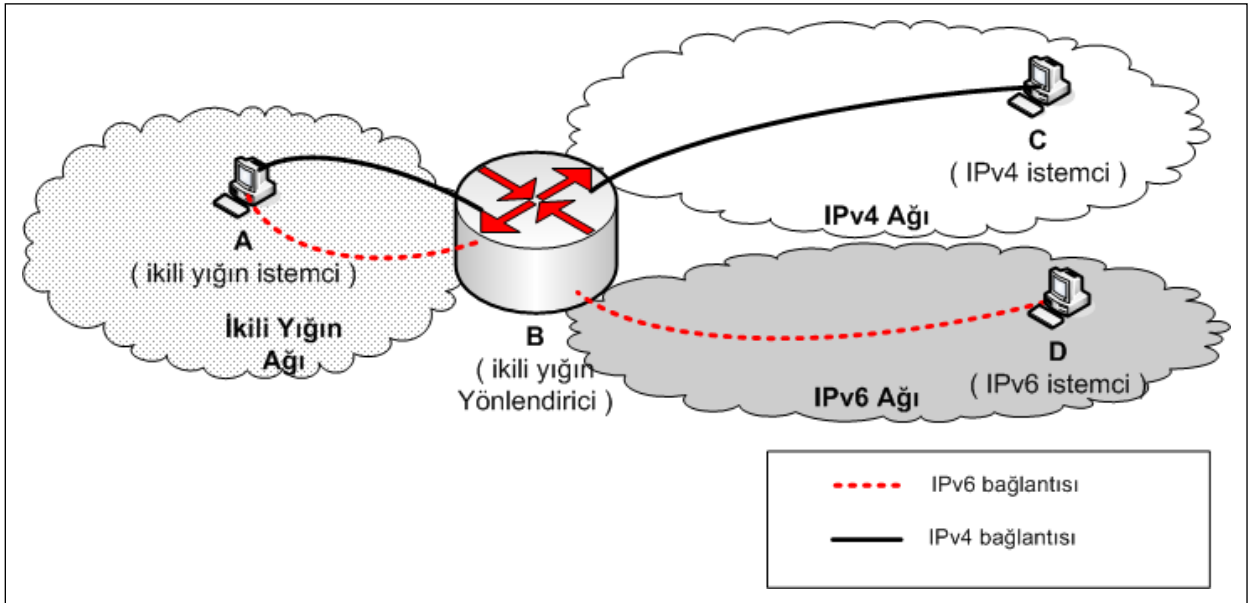
İkili yığın geçiş yöntemi kullanılan ağlarda istemciler, sunucular ve ağ cihazları her iki protokolü de desteklemektedir. Ağdaki her cihazın IPv4 ve IPv6 adresleri vardır.

Şekil 7' de 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 7: İkili Yığın Ağların Haberleşmesi

Şekilde 8'de 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 8: 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 ara yüzü 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 ara yüzü 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 ara yüz 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.

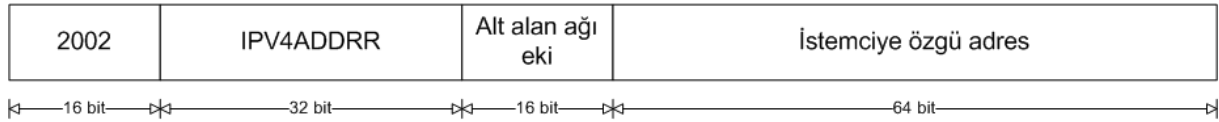
```
netsh interface ip set address "Local Area Connection" static 192.168.0.2 255.255.255.0
192.168.0.1
netsh interface ipv6 set address "Local Area Connection" 2001:db8:1:dede::23
netsh interface ipv6 add route ::/ "Local Area Connection"
```

6to4 Geçiş Yöntemi

6to4 geçiş yöntemi, yönlendirici – yönlendirici veya yönlendirici - istemci arasında kurulan tünel ile ağa IPv6 bağlantısı sağlamaktadır. Bu yöntem kullanılarak IPv6 desteği olan ancak yalnız 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 geiş yönteminde kullanılan adres yapısı Şekil 9’da 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 (IPV4ADDR) yer almaktadır.



Şekil 9: 6to4 Adres Yapısı

6to4 geiş 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 ağına 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 ara yüzüne küresel (yönlendirilebilir) bir IPv4 adresi (IPV4ADDR) atanmalıdır. Bu adres 6to4 ağına duyurulacak IPv6 adresinin oluşturulmasında kullanılmaktadır.

6to4 yönlendiricinin 6to4 ağına bağlı ara yüzüne 2002::/16 öneğine sahip 6to4 adresi atanmalıdır. Bu adres 2002:IPV4ADDR::/48 öneğini içermektedir. Bu ara yüz ile 6to4 istemcilerin IPv6 adresi alırken kullanacakları önek 6to4 ağına duyurulmaktadır.

Örneğin; 6to4 yönlendiricinin IPv4 ara yüzünde “172.16.30.193” adresi kullanılmakta ise bu adresin onaltılık düzende gösterimi “ac10:1ec1” şeklindedir. Alt alan ağı ekinin “baba” olduğu durumda 6to4 ara yüzünden 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:IPV4ADDR::SUBNETID::/64 öneğine 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 ara yüzü ve bir adet IPv6 adresine sahip ara yüzü 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.

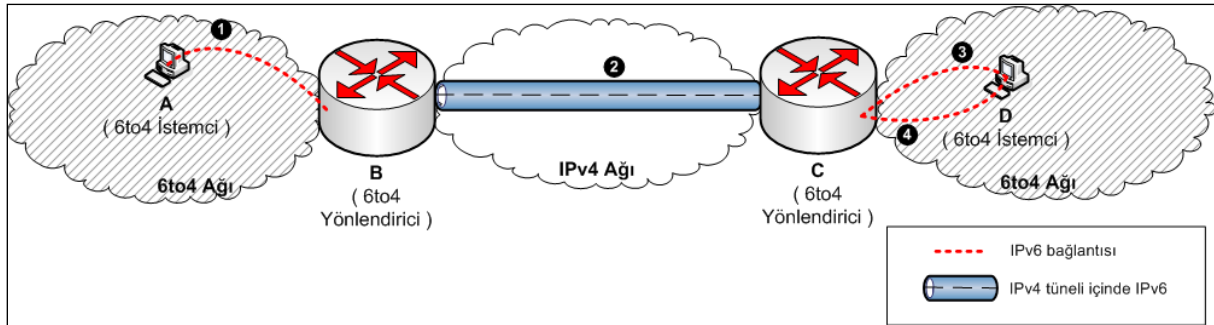
```

[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

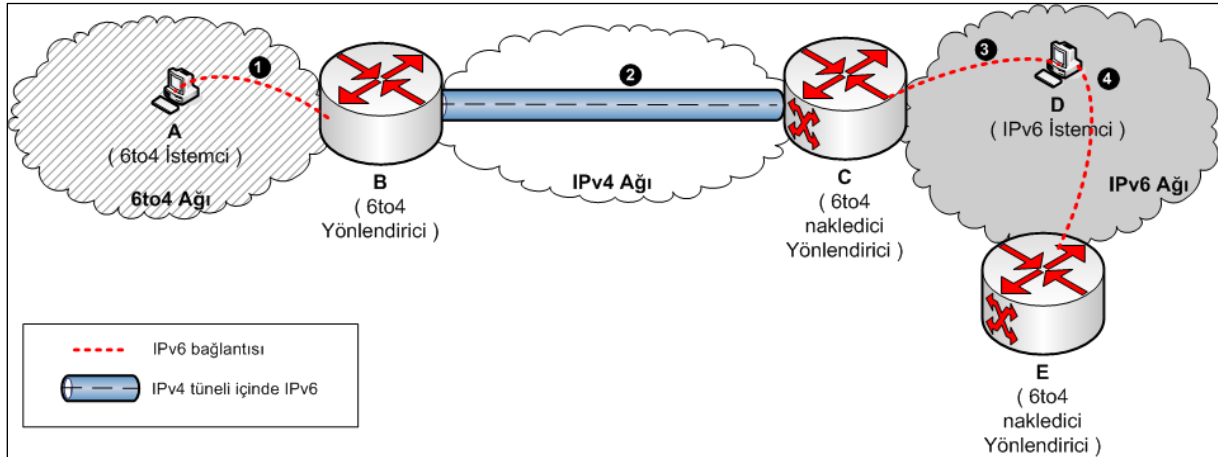


Şekil 10: İki 6to4 Ağının Haberleşmesi

Şekil 10'da 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 ara yüzünden gönderdiği yönlendirici ilanı ile 2002::/16 önekinde sahip IPv6 adresi ve **B**'nin 6to4 adresini alır.
- A, oluşturduğu IPv6 paketini **B**'ye iletir.
- 6to4 ara yüzünden IPv6 paketini alan **B**, IPv6 varış adresinden, IPv4 varış adresini çıkarır. IPv6 paketini IPv4 paketine sarmalar ve sarmalanmış paketi IPv4 ara yüzünü kullanarak IPv4 ağına gönderir.
- Sarmalanmış paketi alan **C** paketi açar. IPv6 paketini, 6to4 ara yüzünden 6to4 ağına gönderir.
- **D** aldığı IPv6 paketini işler ve aynı yolu kullanarak pakete cevap verir.

6to4 ağının IPv6 ağı ile haberleşmesi



Şekil 11: 6to4 Ağının IPv6 Ağı ile Haberleşmesi

Şekil 11’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. Haberleşme esnasında gerçekleşen adımlar aşağıda detaylı olarak açıklanmıştır.

- A , B’nin 6to4 ara yüzünden gönderdiği yönlendirici ilanı ile 2002::/16 önekinde sahip IPv6 adresi ve B’nin 6to4 adresini alır.
- Oluşturduğu IPv6 paketini B’ye iletir.
- 6to4 ara yüzünden 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 ara yüzünden sarmalanmış paketi alan C, paketin sarmalamasını açar. IPv6 paketini, IPv6 ara yüzünü 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 ara yüzü 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 sistemine 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 ara yüzü tanımlamak gerekmektedir. Tünel ara yüzü 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 ara yüzüne 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” ara yüzü 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 ara yüzünün 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 ara yüzünü 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
```

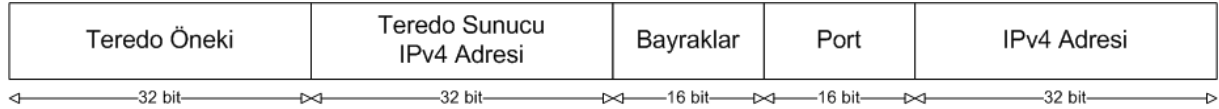
Teredo Geçiş Yöntemi

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 kullanılmadığı 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 12’de yer alan adres yapısı kullanılmaktadır.



Şekil 12: 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

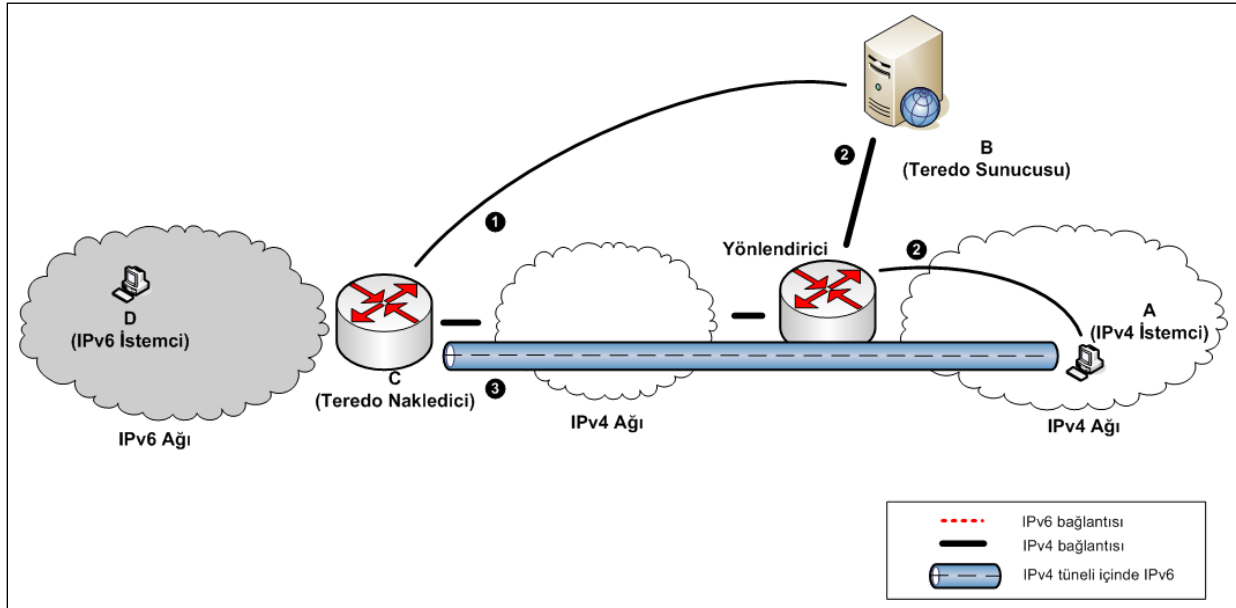
Teredo istemci, küresel IPv4 adresi bulunmayıp NAT ve/veya güvenlik duvarı arkasında yer alan bir cihazdır. Teredo istemcinin IPv6 ağına bağlanırken kullanacağı Teredo sunucu ayarlanmalıdır (NAT arkasındaki güncel Windows işletim sistemine sahip istemciler otomatik olarak teredo.ipv6.microsoft.com adresinde 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 13'te gösterilmiştir. Şekil 13'te yer alan 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.



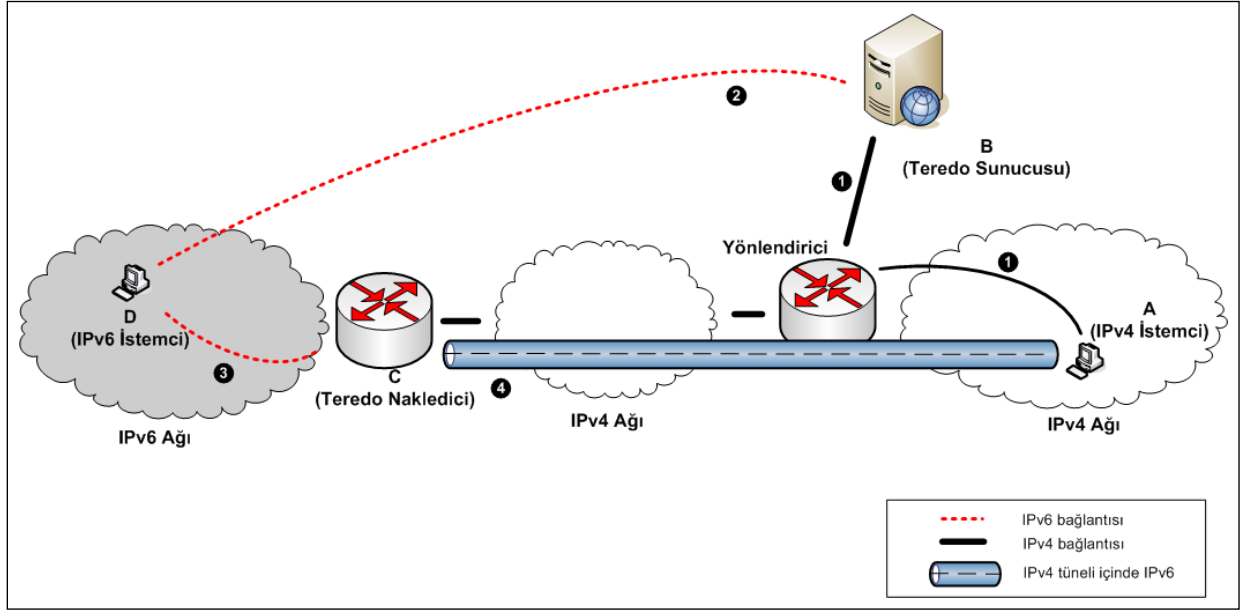
Şekil 13: Teredo nakledicinin/istemcinin Teredo istemciye IPv6 paketi göndermesi

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 naklediciler 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 14: 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 14’de verilen ağ yapısında A’nın D ile iletişimde 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. Ara yüzler arası paket iletimi açılmış olmalıdır. FreeBSD için ara yüzler 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 ara yüz üzerinde veya iki farklı ara yüz 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 ara yüzü ve Teredo sunucu yapılandırılması öncesinde 6to4 ara yüzü kullanım dışı bırakılmalıdır.

Windows Vista / Windows 7

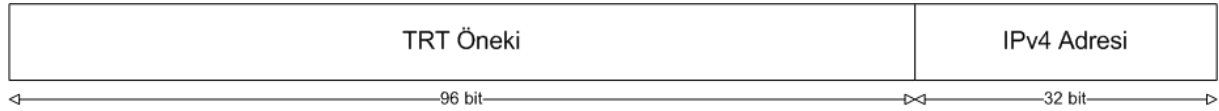
IPv6 bağlantısına sahip olmayan ve sanal IPv4 adresine sahip Windows Vista ve Windows 7 işletim sistemleri Teredo ara yüzünü otomatik olarak yapılandırmaktadır. Varsayılan Teredo sunucusu olarak `teredo.ipv6.microsoft.com` adresi ayarlanmaktadır. Bu sunucu ile ilişkilendirilmiş IPv6 adresi istemciye 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) Geçiř Yöntemi

TRT (Transport Relay Translator) geçiř yöntemi, OSI referans modeli taşıma (transport) katmanında çalışan bir çeviri yöntemidir. IPv6 desteęi verilememiř IPv4 cihazlara (örneęin IPv4 web sunucuları) IPv6 protokolünü kullanarak eriřmek için kullanılması planlanmıřtır.

TRT yöntemini kullanan bir ağda 3 bileřen yer almaktadır. Bunlar IPv6 istemci, IPv4 istemci ve TRT yönlendiricidir. IPv6 ağından IPv4 aęına iletiřim saęlamak 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 eriřmek istedięi IPv4 istemcisinin adresini ekler. TRT yönlendirici, TRT önekine sahip paketleri bir istemciden alır, dięer istemciye yeni bir TCP/UDP baęlantısı açar ve çevrilecek protokolün bařlığını paket verisine ekleyerek gönderir. TRT geçiř yönteminde kullanılan adres yapısı Őekil 15'te gösterilmiřtir.



Őekil 15 TRT adres yapısı

TRT yönteminin avantaj ve dezavantajları ařaęıda belirtilmiřtir.

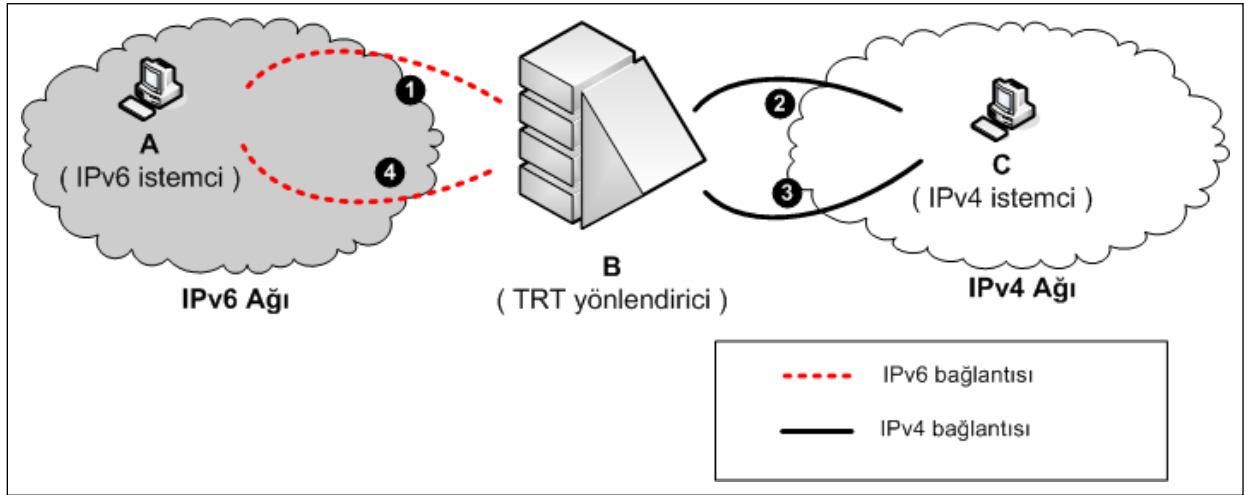
Avantajları

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

Dezavantajları

- TRT durum bilgisini tutan bir sistemdir. TRT yönlendirici üzerinde o an haberleřen uçların bilgisini tutmaktadır. İki ucun oturumu tek bir TRT yönlendiricisi üzerinden gerçekleřmektedir. Bu da TRT yönlendiricisini tek noktada arıza tehdidine karřı açık hale getirmektedir.
- Paket bařlığı deęiřtięi için IPsec ile uçtan uca güvenlik ve doęrulama yöntemleri TRT ile kullanılamamaktadır.

TRT Ağ Yapısı



Şekil 16: TRT ağ yapısı

Yalın IPv6 ve yalın IPv4 iki istemcinin TRT yönlendiricisi aracılığıyla haberleşmesi Şekil 16'daki 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 önekinin 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 ara yüzü kullanılmaktadır. *faith* ara yüzünün aktif olması için çekirdekte aşağıda belirtilen satır yer almalıdır.

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

Faithd uygulaması, *faith* ara yüzüne gelen TRT önekinin 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; ara yüzler arası IPv6 paketi iletimi açılmakta ve faith ara yüzü 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 ara yüzü 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 trafiginin çevirisi
/usr/sbin/faithd ftp /usr/libexec/ftpd ftpd -l # yönlendirilmemiş FTP trafiginin çevirisi
```

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
```

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.msp>
- 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, "Connectivity 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 Geçiş 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