

IPv6 Tünelleme Teknikleri (*)

Gökhan Akın, Asım Güneş

İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı
gokhan.akin@itu.edu.tr, asim.gunes@itu.edu.tr

Özet: IPv6 geçiş döneminde kullanılmak üzere geliştirilmiş ISATAP, 6to4 ve Teredo tünelleme teknikleri üzerine yapılan inceleme anlatılmaktadır.

Abstract: ISATAP, 6to4 and Teredo tunneling techniques which are developed for IPv6 migration was studied in this research.

Anahtar Kelimeler: IPv6, ISATAP, 6to4, Teredo.

1. Giriş

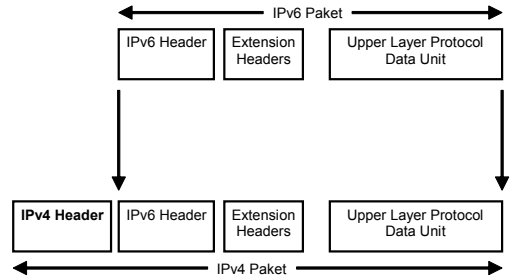
IPv6'ya geçiş döneminde IPv6 desteklemeyen sadece IPv4 çalışan altyapılar üzerinde IPv6 haberleşmesi yapılabilmesi için tünelleme tekniklerinin kullanılması gerekmektedir. Daha önceleri IPv4 üzerinde IPX, AppleTalk gibi diğer üçüncü katman protokollerini taşımak amacı ile GRE gibi tünelleme teknikleri geliştirilmiştir.

Ancak bu gibi teknikler ağların çıkış yönlendiricilerinde bir ağ ile diğer ağ arasında statik olarak yapılabilir. İhtiyaç duyulan yapı ise bütün istemcilerin, dünyadaki herhangi bir istemci ile yönlendirici cihazlarda hiç bir konfigürasyon yapmadan erişebilmesidir.

Bu amaçla otomatik tünelleme teknikleri olan IPv6 Otomatik Tünelleme, 6over4, ISATAP, 6to4 ve Teredo protokolleri geliştirilmiştir.

Bu tekniklerin çalışabilmesi için Dual Stack veya Dual IP olarak adlandırılan ve aynı işletim sisteminde hem IPv4 hem de IPv6 destekleyen bir işletim sisteminin kullanılması gerekmektedir. Bunu yanı sıra DNS sunucularında "AAAA" kaydı ile gerçekleştirilen IPv6 desteği de gereklidir.

2. Genel IP4-IPv6 Tünelleme Sistemi



Şekil 1. IPv4 ile Kılıflanmış IPv6 Paketi

Bütün tünelleme tekniklerinde IPv6 paketinin kılıflanması (encapsulation) için aynı format kullanır. Bunun için IPv6 paketinin MTU boyutu 20byte IPv4 başlığı düşünülerek belirlenir ve IPv4 başlığındaki protokol numarası kısmı 41 olarak atanır.

3. IPv6 Otomatik Tünelleme ve 6over4

IPv6 otomatik tünelleme (RFC 2893) sadece dual stack çalışan iki pc arasında haberleşmeyi sağlamaktadır. Günümüzde yerini ISATAP'e devretmiştir.

* Bu bildiri, inet-tr'07 (XII. "Türkiye'de İnternet" Konferansı) 'nda sunulmuştur. Bir yanlışlık nedeniyle ilgili bildirilerle birlikte basılamadığından burada yer almıştır.

6over4 (RFC 2529) tünelleme tekniğinin en büyük özelliği ise diğer tekniklerde olmayan IPV6 multicast trafiği desteğidir. Ancak bu desteğin paralelinde protokol IPV4 multicast desteğinde ihtiyaç duyduğu için çok popüler değildir. Bunu yerine de ISATAP tercih edilmektedir.

4. ISATAP (RFC 4214)

Aynı kurum içersinde dual stack mimarisine sahip istemcilerin otomatik olarak IPV4 ağ alt-yapısı üzerinden IPV6 istemcilere ulaşmasını sağlayan protokoldür.

Adres yapısı olarak “[64-bit ön adres]:0:5EFE:a.b.c.d” kullanılmaktadır. Ön adres Global IPV6 adresi olabileceği gibi FE80 şeklinde Site-Local adreste olabilir. fe80::5EFE:160.75.8.128

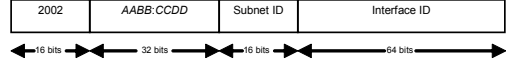
veya 2001:a98:8000:1::160.75.8.128 ISATAP adreslere örnek olabilir.

İki Dual-Stack istemci, 2.bölümdeki paket yapısını kullanarak birbirleri arasında otomatik ISATAP tüneli oluştururlar. Aynı firma içindeki Native IPV6 istemciler ile haberleşebilmeleri için ise ISATAP yönlendirici gerekir. ISATAP yönlendiricinin istemci tarafında öğrenilmesi, işletim sistemi tarafından otomatik olarak “isatap.domainadi” şeklinde DNS sunucusuna sorulması şeklinde olabileceği gibi, yönlendirici adresinin istemciye statik olarak tanımlanması şeklinde de olabilir. Ancak statik tanımlama bu şekilde otomatik tünelleme tekniği için bütün istemcilere elle müdahaleyi gerektiren bir durum olduğu için DNS sistemini kullanmak daha kolay olacaktır.

5. 6to4 (RFC 3056)

Dual stack mimarisine sahip istemcilerin otomatik olarak IPV4 ağ altyapısı üzerinden IPV6 istemcilere ulaşmasını sağlayan protokoldür. 6to4 ile haberleşecek istemcilerin aynı firmada

olmalarına gerek yoktur. Herhangi iki istemci Internet üzerinden haberleşebilir.



Şekil 2. 6to4 Adres Yapısı

Bütün 2002::/16 aralığı, 6to4 adreslemesi için rezerve edilmiştir. “AABB:CCDD” ise IPV4 adresinin onaltılık sistemde gösterilmiş halidir. Bu şekilde global bir IPV4 adresine sahip herkes aynı zamanda global olarak ona ayrılmış bir IPV6 adresine de sahiptir. Bu sayede firmalardan bağımsız bir yapı elde edilmiştir.

Global Native IPV6 istemciler ile haberleşme olabilmesi için 6to4 Relay gerekir. 6to4 Relayin istemcilere atanması RFC 3068 ile tarif edilmiş anycast ile Relay bulunması tekniği ile olabileceği gibi, işletim sisteminde tarif edilecek bir DNS adının sorgulanması veya elle girilmesi şeklinde de olabilmektedir. Örnek olarak MS işletim sistemlerinde değiştirilmemesi durumunda 6to4.ipv4.microsoft.com adresi sorgulamaktadırlar.

6to4 da Relay farklı firmaların NativeIPV6 geçişi için kullanıldığı için büyük servis sağlayıcıların sağlaması gereken bir hizmettir. Günümüzde test amaçlı 6to4 Relay sunucuları bulunmaktadır.

6. Teredo (RFC 4380)

Protokol, diğer adı shipworm olarak da geçen canlıdan ismini almıştır. 6to4 tekniğinde iki istemcinde NAT arkasında olma durumunda, NAT tercüme tablosunda kayıt olmadığı için veya bazı NAT cihazının sadece TCP ve UDP protokollerini geçirebildiği, protokol 41’i geçiremediği için erişim sorunu yaşanır. Teredo NAT arkasındaki istemcilerin de IPV6 ile haberleşmelerinin sağlanması için geliştirilmiştir. Teredo son çare (last resort) çözümdür. Native IPV6, ISATAP veya 6to4 ile haberleşme gerçekleştirilemiyorsa kullanılır.



Şekil 3. Teredo Adres yapısı

Teredo için 2001:0000::/32 aralığı rezerve edilmiştir. Teredo Server IPV4 adres kısmı, adresin onaltılık olarak yazılmasından oluşur. Flags kısmının ilk biti “Cone” tipi NAT arkasında ise 1 yoksa sıfır değerini alır. Diğer kısımlar rezerveridir. Obscured External Port değeri kullanılan UDP port numarasını onaltılık şeklinde 0xFFFF ile XOR’lanmış hali, Obscured External Address değeri ise IPV4 adresinin onaltılık şekilde 0xFFFFFFFF ile XOR’lanmış halidir. Gerçek IP adresi 160.75.126.38, kullandığı port numarası UDP 2500 ve Teredo sunucu IP adresi 160.75.100.1 olan bir istemcinin Teredo adresi “2001:0000:A04B:6401:0:F63B:5FB4:81D9” şeklinde olur.

NAT arkasındaki istemci-1 diğer bir NAT arkasında istemci-2 ile haberleşmek için önce direk erişmeyi dener. Hedef NAT arkasında olduğu için ve daha önce istemci-1’e hiç bağlantı kurmadığı için aralarında haberleşme başlamaz. Bu durumda istemci-1, istemci-2’nin Teredo sunucusu ile haberleşir. Bütün istemciler Teredo sunucuları ile sürekli bağlantıda olduğu için Teredo sunucu istemci-2’ye NAT arkasında olmasına rağmen ulaşabilir ve istemci-1’e erişmesi gerektiği bildirerek aralarındaki haberleşmenin başlamasını sağlar.

Bu teknik NAT arkasındaki istemcilerin birbirlerine doğrudan erişmelerine olanak sağladığı için güvenlik sorunlarına da yol açmaktadır. Bunun yanı sıra P2P yazılımları tarafından da kullanılmaktadır.

7. Sonuç

IPV6 geçiş süreci mobil istemcilerin artması ve mobil istemcilere daha geniş bant genişlikleri sağlanmasının paralelinde hızlanacaktır.

Bunun yanı sıra Native IPV6 olarak hizmet verecek sunucuların artması ile bu geçiş döneminde kurumlar arası hizmet verebilecek 6to4 ve Teredo teknikleri için Relay sunucuların kamuya hizmet verilebilecek şekilde devreye girmesi gerekmektedir.

Özellikle Teredo tekniği sayesinde bütün NAT arkasındaki istemciler kendilerine ait bir global IPV6 adresine de sahiplerdir. Buda Dünya’daki İnternet’e erişen istemcilerin çok büyük bir kısmının yönlendiricilerinde hiç bir değişiklik yapmadan artık doğrudan birbirlerine ve Native IPV6 adresine sahip diğer istemcilere erişebilir duruma gelmelerini sağlamaktadır.

Kaynaklar

- [1] RFC4214, ‘Intra-Site Automatic Tunnel Addressing Protocol’
- [2] RFC 3056, ‘Connection of IPv6 Domains via IPv4 Clouds’
- [3] RFC 4380, ‘Tunneling IPv6 over UDP through NATs’
- [4] Karlsson B. ‘Implementing IPv6 Networks’ Cisco Press, 2003
- [5] İnternet Protokol V6 , www.microsoft.com/ipv6 , Microsoft Corp.
- [6] IPV6 , www.cisco.com/go/ipv6 , Cisco Corp.
- [7] The Teredo Protocol, www.symantec.com/avcenter/reference/Teredo_Security.pdf, Symantec Corp.