

Teredo; Güvenlik ve Performans Analizi

Beyhan Çalışkan

Özet—Günümüzde yaygın olarak kullanılan IPv4 (IP versiyon 4), internetin hızlı gelişimi ile birlikte adres uzayını hızla tüketmektedir. IETF bu sorunu çözmek ve protokole yeni fonksiyonlar kazandırmak için 1990'ların başında çalışmalarına başlamış ve 1998 yılında RFC 2460 ile IPv6 standartlarını tanımlamıştır. Yeni protokole geçiş bir akşamda gerçekleşebilecek bir süreç değildir. Bu nedenle farklı iki protokolün uzun süre birlikte çalışması kaçınılmazdır. Protokoller arasındaki geçiş sürecinin başarısı ise, IPv4 düğümlerinin IPv6 düğümleri ile sorunsuz iletişimine bağlıdır. Bu amaçla birçok IPv6 geçiş yöntemi geliştirilmiştir. Bu çalışmada, IPv6 geçiş yöntemlerinden biri olan Teredo yönteminin güvenlik ve performans analizi yapılmıştır.

Anahtar Kelimeler—IPv6, geçiş yöntemi, güvenlik, performans, Teredo

I. GİRİŞ

IP (İnternet Protokolü), paket anahtarlama bilgisayar ağları arasındaki iletişim için tasarlanmıştır. Küresel ağ Internet'in genel dili olan bu protokol, 1981 yılında RFC 791 ile tanımlanmış ve standartlaşmıştır. Günümüzde yaygın olarak kullanılan IPv4 (IP versiyon 4), internetin hızlı gelişimi ile birlikte adres uzayını hızla tüketmektedir. IETF tarafından oluşturulan Address Lifetime Expectation çalışma grubuna göre, 2011 yılına kadar IPv4 adreslerinin tükeneceği öngörülmüştür. IETF bu sorunu çözmek ve protokole yeni fonksiyonlar kazandırmak için 1990'ların başında çalışmalarına başlamış ve 1998 yılında RFC 2460 ile IPv6 standartlarını tanımlamıştır [1].

IPv4 adreslerinin dağıtıldığı ilk zamanlarda etkili bir dağıtım yöntemi gözlemlenmemiştir. Var olan IPv4 adreslerinin yüzde altmış Amerika Birleşik Devletleri tarafından kullanılırken yüzde kırklık kısım Dünya'nın geri kalanı tarafından paylaşılmaktadır. Yani IPv4 adreslerinin %60'ı, Dünya nüfusunun %5'ine tahsis edilmiştir [2]. Diğer yandan, Çin ve Hindistan gibi nüfusu çok fazla olan ülkelerde IP adresi ihtiyacı hızla artmaktadır. Ayrıca, mobil cihazlara, oyun konsollarına hatta arabalara bile IP adresi verilmesi bir diğer önemli etken olmuştur. 1993 yılında bu sorunu çözmek için IETF tarafından IPng (IP next generation) çalışmaları

başlatılmıştır. Yapılan çalışmalar sonucunda, sorunun çözümü için iki yöntem belirlenmiştir:

1. Mevcut protokolü değiştirmeden, adres uzunluğunu arttırmak.
2. Tamamen yeni bir protokol geliştirmek.

Çok acil bir çözüm gerektiği için, yeni nesil protokolün geliştirilmesine başlanmıştır. İlk adı IPng olan bu protokol, sonradan IPv6 adını almıştır.

Yeni protokole geçiş bir akşamda gerçekleşebilecek bir süreç değildir. Bu nedenle farklı iki protokolün uzun süre birlikte çalışması kaçınılmazdır. Protokoller arasındaki geçiş sürecinin başarısı ise, IPv4 düğümlerinin IPv6 düğümleri ile sorunsuz iletişimine bağlıdır. Bu amaçla NGtrans çalışma grubu tarafından, IPv6 geçiş yöntemleri hakkında araştırmalar yapılmış ve çeşitli yöntemler önerilmiştir [3].

Bu çalışmada, IPv6 geçiş yöntemlerinden Teredo'nun performansı ve güvenlik analizi yapılmıştır. Çalışmanın ilk bölümünde Teredo yöntemi hakkında bilgi verilmiş, ikinci bölümünde ise Teredo yöntemine ilişkin güvenlik konuları araştırılmıştır. Sonraki bölümde gerçek ağ üzerinden yapılan performans testlerinin sonuçları tartışılmış ve son bölümde çalışmanın değerlendirilmesi yapılmıştır.

II. TEREDO

Teredo yöntemi, ikili yığın çalışan ve NAT arkasında bulunan düğümlerin, IPv6 bağlantısını sağlamak için geliştirilmiştir. Bu yöntem düğümden-düğüme otomatik tünelleme sayesinde bir veya birçok NAT arkasında bulunan istemcilerin IPv6 bağlantısını sağlamaktadır. Bu işlem IPv6 paketlerinin IPv4 UDP (User Datagram Protocol) mesajları içine paketlenmesi ile gerçekleşir [4].

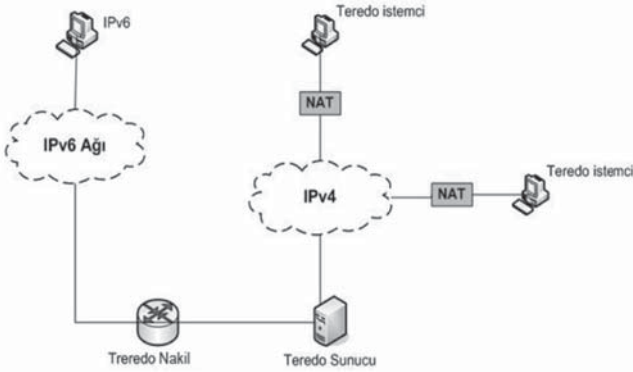
Birçok İnternet kullanıcısı bağlantısını NAT arkasından gerçekleştirmektedir. IPv6 protokolünde çok sayıda adres olduğu için NAT gibi bir mekanizma yoktur. Fakat geçiş sürecinde bu konuya çözüm gerekmektedir. NAT yapan cihazların IPv4 yararlı veri yükü alanında filtreleme uygulaması problem oluşturmaktadır. Bunun nedeni, IPv6 paketlerinin tünel içerisinde IPv4 yararlı veri yükü olarak taşınması ile açıklanabilir. Bir diğer sorun NAT arkasındaki adreslerin global olmayışıdır. 6to4 gibi mekanizmalar global

Beyhan Çalışkan, TÜBİTAK Ulusal Akademik Ağ ve Bilgi Merkezinde sistem yöneticisi olarak çalışmaktadır. Telefon: 312-2989376; faks 312-2989393; Eposta: beyhan@ulakbim.gov.tr

IPv4 adresine ihtiyaç duyduğundan bu ortamlarda kullanılması zordur. Ancak NAT yapan cihazın 6to4 yönlendiricisi olması durumunda işleyiş sağlanabilir.

Teredo mimarisi Şekil 1'de gösterilmiştir. Bu yönteme ait terimler aşağıda kısaca açıklanmıştır [4]:

- **Teredo Servisi:** IPv6 paketlerinin UDP üzerinden taşınması.
- **Teredo İstemcisi:** IPv6 bağlantısı talep eden düğüm.
- **Teredo Sunucu:** Teredo istemcilere IPv6 bağlantısını sağlayan düğüm.



Şekil 1. Teredo mimarisi

- **Teredo Nakil (relay):** Teredo istemcilere gelen trafiği, Teredo servisini kullanarak yönlendiren IPv6 yönlendirici.
- **Teredo IPv6 Servis Takısı:** IANA tarafından atanan, Teredo istemcilerine ait IPv6 adres bloğudur (2001:0000::/32).
- **Teredo UDP Portu:** Teredo sunucuların dinlediği UDP 3544 portudur.
- **Teredo Balon (Bubble):** Yararlı veri taşımayan, asgari uzunluktaki IPv6 paketi. Teredo nakil ve istemcileri bu paket sayesinde NAT içerisinde eşleştirme yapar.
- **Teredo Servis Portu:** Teredo paketlerinin gönderildiği port olarak tanımlanır. Bu port Teredo istemcinin IPv4 adresini kullanarak işlem yapar.
- **Teredo Sunucu Adresi:** Teredo sunucusuna ait IPv4 adresidir.
- **Teredo –eşleme Adresi ve Teredo-eşleme Portu:** NAT sonucu çevrilen global IPv4 adresi ve UDP portu ve Teredo istemciye ait Teredo servis portu bilgileri.

İstemci bu bilgileri Teredo protokolü sayesinde elde eder.

- **Teredo IPv6 İstemci Takısı:** Teredo IPv6 servis takısı ve Teredo sunucu adresinden oluşturulan global IPv6 adres takısıdır.
- **Teredo Düğüm Tanımlayıcı (Node Identifier):** Teredo servisi ile erişilebilir bir istemciye ait, 64 bit uzunluğundaki IPv4 adresi ve UDP port bilgilerini taşıyan alandır.
- **Teredo IPv6 Adresi:** Teredo IPv6 istemci takısı ve Teredo düğüm tanımlayıcısı tarafından oluşturulan adrestir.
- **Teredo Yenileme Süresi (Refresh Interval):** Bir Teredo IPv6 adresinin yenilenen trafikte geçerlilik süresini belirtir. Varsayılan değer 30 saniyedir.
- **Teredo İkincil Port:** Teredo yenileme süresi bilgisinin gönderildiği ve alındığı bir UDP portunu ifade eder. Bu port üzerinden Teredo trafiği geçmez.
- **Teredo IPv6 Keşif Adresi:** “224.0.0.253” olarak tanımlanmış, ağdaki diğer Teredo istemcilerini bulmak için kullanılan IPv4 adresidir.

Teredo işleyişine geçmeden, Şekil 2’de gösterilen Teredo adres yapısını anlamak önemlidir.

32 bit	32 bit	16 bit	16 bit	32 bit
Teredo takısı	Teredo Sunucu IPv4 Adresi	Bayrak	Port	İstemci IPv4 Adresi

Şekil 2. Teredo adres yapısı

Teredo IPv6 adres yapısında, 32 bit uzunluğundaki Teredo servis takısı 2001:0000::/32 olarak rezerve edilmiştir. Sonraki 32 bit’lik alanda, Teredo sunucuya ait IPv4 adresinin bilgisi taşınmaktadır. Takip eden bayrak alanında NAT tipine ait bilgi vardır. Sonraki 16 bit, NAT cihazı tarafından kullanılan global UDP portunu hexadecimal olarak ve gizleyerek (bit flipping) gösterir. Son 32 bit ise Teredo sunucu tarafından tespit edilen NAT cihazına ait global IPv4 adresinin hexadecimal ve gizlenmiş halidir.

Teredo istemcilerin bu yöntemi kullanabilmesi için önceden yapılandırma gereklidir. İlk adım Teredo istemciye Teredo sunucusuna ait IPv4 adresinin tanıtılmasıdır. İstemci, link-local IPv6 adresinden ağdaki yönlendiricilere yönlendirici isteği (Router Solicitation) [5] mesajı göndererek Teredo sunucuya ait IPv4 adresini öğrenir. Ayrıca, yönlendirici tavsiyesi mesajından da Teredo IPv6 servis takısına ait bilgi elde edilir. Bir sonraki adımda istemci, rezerve edilmiş adres ve port bilgilerinden yararlanarak Teredo IPv6 adresini oluşturur.

Teredo sunucusu, Teredo istemcisinden gelen IPv6 paketlerini UDP içine paketler. Bu işlem sırasında paketin varış düğümüne ait IPv4 adresi ve UDP port numarası IPv6 varış adresinden türetilir. Giden pakette kaynak adresi olarak kendi IPv4 adresini ve kaynak port olarak Teredo UDP portunu (3544) gönderir. Teredo nakil ise Teredo servis takısını dış dünyaya anons eden bir IPv6 yönlendiricidir.

III. TEREDO YÖNTEMİNDE GÜVENLİK

Günümüzde bilgisayar ve ağ güvenliği hayati öneme sahiptir. E-devlet, sağlık, finans ve eğitim gibi birçok hizmetin Internet üzerinden verilmesi konun önemini arttırmaktadır. Bu bakış açısıyla, yeni bir protokole geçişte mevcut güvenlik politikalarının işlevselliği ve uygulanabilirliği ayrıntılı olarak araştırılmalıdır. Çalışmanın bu bölümünde IPv6 geçiş yöntemlerinden Teredo'ya ait güvenlik konuları araştırılmış ve çeşitli güvenlik çözümleri önerilmiştir. IPv6 ile ilgili genel güvenlik konuları RFC 4942'de tartışılmıştır ve bu çalışmanın kapsamı dışındadır.

Teredo düğümleri IPsec mekanizmalarından herhangi bir kısıtlama olmaksızın faydalanabilir. Bu durum şüphesiz ağı daha güvenli hale getirmektedir. Fakat Teredo yöntemi ile ortaya çıkabilecek güvenlik sorunları göz ardı edilmemelidir. Bu sorunlar dört grup altında toplanabilir [4]:

1. NAT üzerinden sızmak:

Teredo servisini kullanan düğümler, bir veya birden çok NAT katmanının arkasından IPv6 erişimi sağlayabilmektedir. Bu erişimin sağlanabilmesi için NAT cihazı üzerinde bulunan ateş duvarının Teredo servislerine izin vermesi gerekmektedir. Yani Teredo istemciler IPv6 üzerinden gelen bütün trafiğe açıktır ve olası saldırıların hedefi olabilmektedirler. Bu soruna çözüm olarak, bütün Teredo istemcilerin kendi üzerinde kişisel ateş duvarı bulundurulması önerilmektedir. Modern işletim sistemlerinin çoğunda yerleşik ateş duvarı yazılımı mevcuttur ve bu çözüm kolayca uygulanabilir.

Diğer bir güvenlik önlemi, Teredo üzerindeki link-local adreslere ait trafiğin engellenmesidir. Çünkü Teredo servisleri tarafından link-local adresleri kullanılmamaktadır.

Son olarak IPsec servislerinin kullanılması önerilmektedir. Bu sayede istemciler ile Teredo servisini sağlayan sunucular veya yönlendiriciler arasında bir koruma sağlanabilir.

2. Teredo servisini arada adam saldırısı (man-in-the-middle) için kullanmak:

Saldırgan Teredo istemcilerinden gelen yönlendirici isteklerini engelleyerek, istemciye farklı bir yönlendirici tavsiyesi mesajı gönderebilir. Bu durumda Teredo istemcisi istenenden farklı bir IP adresi alabilir. Bu tip bir saldırı,

istemciye erişim imkanı olmayan bir IP adres atayarak servis almasını engellemek veya istemcilere kendi IP adresini ağ geçidi olarak anons edip, üzerinden geçen trafiği dinlemek için kullanılabilir. Böyle bir saldırının gerçekleşebilmesi için, saldırının yönlendirici isteğini engelleyebilecek seviyede DoS yapılabilmesi gerekmektedir. Ayrıca, Teredo sunucu adresinin değiştirilebilmesi için kimlik doğrulama mekanizmasının aşılması gereklidir. SSL gibi şifreli kanallar yardımıyla yapılan kimlik doğrulama işlemleri saldırının işini daha da zorlaştıracaktır.

IPsec kullanımı adres değiştirme ve trafik dinleme saldırılarını etkili bir şekilde engelleyebilmektedir ve ortadaki adam saldırılarına karşı önlem olarak önerilmektedir.

3. Teredo servisine yönelik DoS:

Teredo servisine yönelik beş çeşit DoS saldırısı yapmak mümkündür.

- Saldırgan ağın IPv6 kısmında bir Teredo yönlendiricisi gibi davranıp Terdeo IPv6 takısına yönelik yönlendirme yapabilir. Bu saldırı IPv6 yönlendirmesine yöneliktir.
- Ortadaki adam saldırısında anlatıldığı gibi yönlendirme tavsiyesi mesajları değiştirilirse, istemci IPv4 paketlerini var olmayan bir adrese veya istenmeyen başka bir IPv4 adresine gönderebilir.
- Teredo istemcileri iletişime geçtikleri en son düğümleri önbellekte (cache) tutar. Saldırgan istemciye çok sayıda Terdeo istemcisinden bağlantı geliyormuş gibi paket gönderdiğinde önbellek doldurulabilir. Bu durumda Teredo istemcileri arasındaki doğrudan bağlantı engellenebilir.
- Saldırgan, yerel eş keşfi işlemi (local discovery procedure) [4] balonunda değişiklik yaparak istemciye gönderebilirse bu işleme yönelik DoS saldırısı gerçekleşebilir.
- Teredo sunucu ve yönlendiricilerine çok sayıda paket göndererek sistem kaynakları tüketilebilir. Teredo sunucular hata korumalı (failover) çalışabildiğinden bir sunucudaki kaynaklar tükendiğinde servisi diğer bir Teredo sunucusu devralabilir. Teredo yönlendiriciler üzerinde istemci başına açılacak oturum sayısı kısıtlanarak önlem almak mümkündür.

4. Teredo istemcisi olmayan düğümlere DoS:

Teredo yönteminde beklenmedik noktalara paket enjeksiyonu yaparak DoS saldırısı yapmak mümkün olabilir. Bu tip saldırılar üç grup altında toplanabilir:

- Teredo sunucusu yansımala saldırısı için kullanılabilir.

- IPv6 düğümlerine yönelik DoS saldırılarının Teredo sunucusu üzerinden taşınması.
- IPv4 düğümlerine yönelik DoS saldırılarının Teredo yönlendiricisi üzerinden taşınması.

Bu saldırılara karşı genel önlem, Teredo trafiğinin kendine özgü trafik paterninden yararlanmaktır. Teredo trafiği Teredo UDP portu ve IPv6 adres takısı gibi spesifik paternlere sahiptir. Trafığe ait bu özellikler saldırı durumunda filtreler yazılmasını sağlayabilir.

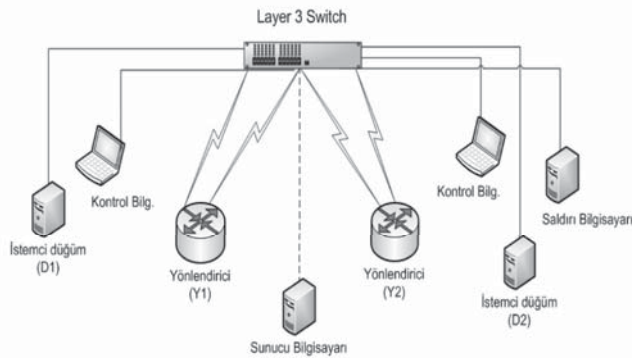
IV. TEREDO YÖNETİMİNDE PERFORMANS

Ağ üzerinden verilen birçok hizmet ve uygulama ağ performansına doğrudan bağlıdır. Bu bakımdan, hem akademik ağlarda hem de ticari ağlarda performans oldukça önemli bir konudur. Çalışmanın bu bölümünde Teredo yönteminin performansı gerçek ağ üzerinde yapılan testlerle araştırılmıştır. Hazırlanan test düzeneği, throughput ve gecikme süresi değerlerini ölçmeye yöneliktir.

A. Test Ortamı

Teredo geçiş yöntemine ilişkin bütün performans testleri gerçek ağ ortamında yapılmıştır. Şekil 3'te gösterilen test ortamında iki adet Cisco 2600 serisi yönlendirici, iki adet eş özelliklere sahip istemci bilgisayar, iki adet kontrol bilgisayar, bir adet sunucu bilgisayar ve Cisco 3560 serisi anahtarlama cihazı bulunmaktadır.

İstemci ve sunucu bilgisayarları eş donanımlara sahiptir. Her birinde Intel Pentium 4 2.66 GHz işlemci, 1024Mb ram bellek, 80GB sata sabit disk ve 1Gbit SkyConnect ethernet kartı donanımları mevcuttur. Cisco yönlendiricilerde 2611XM (MPC860P) işlemci, 256Mb ram bellek ve iki adet 100Mbit ethernet arayüzü bulunmaktadır. Tüm cihazlar, Cisco 3560 Gigabit switch üzerine CAT5e kablolar ile bağlanmıştır. Test senaryolarında kullanılan farklı ağlar, Cisco 3560 switch üzerinde oluşturulan VLAN'lar yardımıyla sağlanmıştır.



Şekil 3. Test ortamı

B. İşletim Sistemleri

Sunucu bilgisayarında FreeBSD 7.2 i386, istemci bilgisayarlarında FreeBSD 8.0 i386 işletim sistemleri kullanılmıştır. Sunucu ve istemci bilgisayarlar üzerinde yapılan ince ayarlar aşağıda verilmiştir:

- kern.ipc.somaxconn=5000
- kern.ipc.nmbclusters="32768"

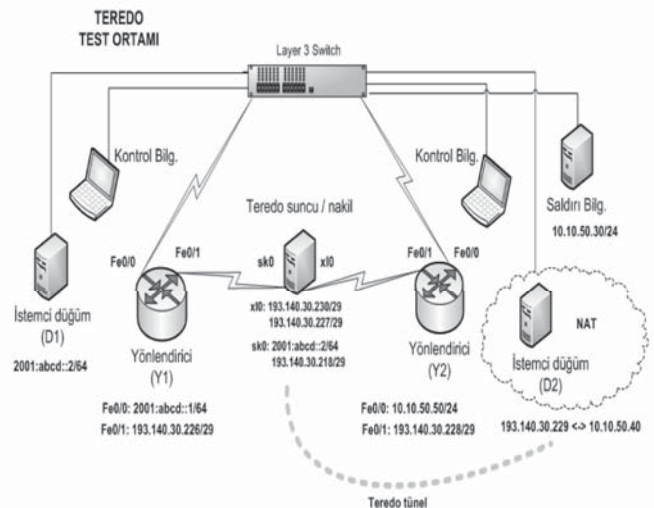
C. Ölçüm Araçları

Teredo geçiş yönteminin ağ performansını ölçmek için Netperf [6] uygulaması kullanılmıştır. Bu uygulama, istemci ve sunucu olarak iki farklı yapıda çalışmaktadır. D1 istemcisi üzerinde "netserv -6" parametresi ile sunucu olarak çalıştırılmış, D2 istemcisi üzerinde ise "netperf -P0 -fm -6 -H D1 -tTCP_STREAM -l120 -- -m [74-128]" parametreleri ile istemci modunda çalıştırılmıştır. Netperf çıktıları throughput değerlerinin belirlenmesinde kullanılmıştır. Gecikme süresi değerleri ICMPv6 kullanılarak elde edilmiştir.

Yapılan testler, IPv6 performans metodolojine [7] uygun olarak 64, 128, 256, 512, 1024, 1280, 1518 ve 8192 byte büyüklüğündeki TCP ve UDP paketleri ile gerçekleştirilmiştir. Her bir test, 120 saniye süresince çalıştırılmıştır.

D. Teredo Test Senaryosu

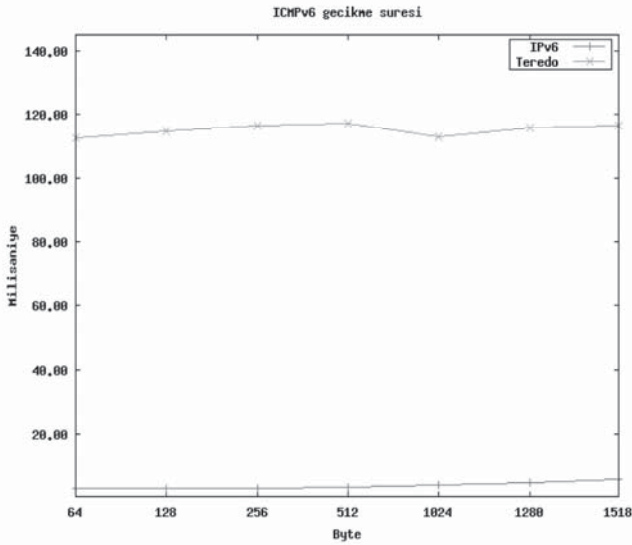
Test senaryosunda, IPv4 ağında ve NAT arkasında bulunan D2 düğümü, sadece IPv6 adresine sahip D1 düğümü ile iletişim kurmuştur. NAT işlemi Y2 yönlendiricisi tarafından gerçekleştirilmiştir. Teredo sunucusu aynı zamanda Teredo nakil yönlendiricisi olarak çalıştırılmıştır. Teredo sunucu / nakil FreeBSD 7 işletim sistemine sahip ve Miredo [8] yazılımı çalıştıran bir bilgisayardır. Miredo yazılımı aynı zamanda D2 istemcisi tarafından Teredo istemci uygulaması olarak çalıştırılmıştır. Şekil 4'te Teredo test ortamı ayrıntılı olarak gösterilmiştir.



Şekil 4. Teredo test senaryosu

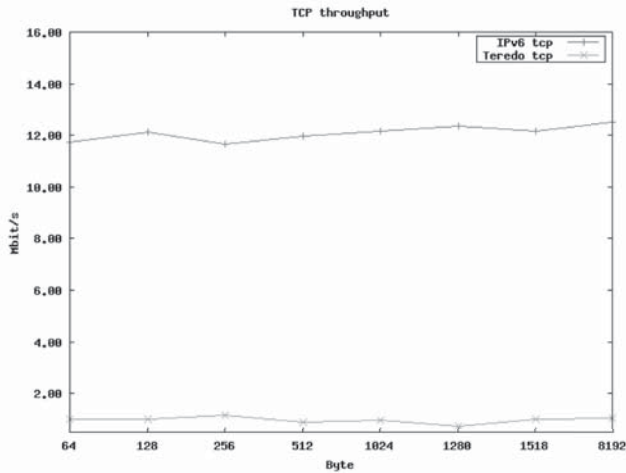
E. Test Sonuçları

Yalnız IPv6 ile Teredo yönteminin karşılaştırıldığı gecikme süresi testi, ICMPv6 kullanılarak gerçekleştirilmiştir. Boyutları 64 ile 1518 byte arasında değişen paketler kullanılarak yapılan testlere ilişkin sonuçlar, Şekil 5’te gösterilmiştir. Yalnız IPv6 kullanıldığında gecikme süresi 2ms ile 8ms değerleri arasındayken, Teredo yönteminde gecikme süresi 116ms değerine kadar artmıştır. Teredo yönteminde yaşanan bu kaybın nedeni, kullanıcı seviyesinde çalışan Miredo yazılımı olabilir.



Şekil 5. ICMPv6 gecikme süresi

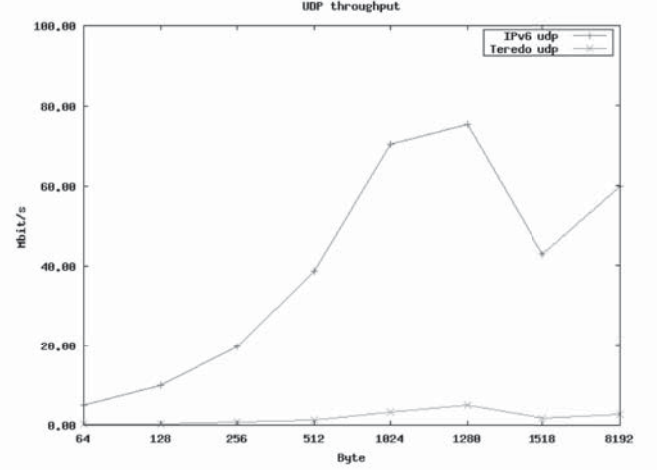
Throughput testleri, TCP ve UDP protokolleri kullanılarak farklı paket boyutları için tekrarlanmıştır. Şekil 6’da TCP throughput test sonuçları verilmiştir. Yalnız IPv6 kullanıldığında 12.65Mbit/s değerine ulaşan TCP throughput değeri, Teredo yönteminde 1Mbit civarında performans göstermiştir.



Şekil 6. TCP throughput performansı

UDP throughput test sonuçları Şekil 7’de gösterilmiştir. Yalnız

IPv6 kullanıldığında 80Mbit/s seviyesinde olan UDP throughput performansı Teredo yönteminde 1.9Mbit/s değerine düşmüştür.



Şekil 7. UDP throughput performansı

V. SONUÇ

Bu çalışmaya ait bulgular ışığında, Teredo ağ performansının yalnız IPv6 karşısında çok düşük olduğu gözlemlenmiştir.

REFERANSLAR

- [1] B. Çalışkan “IPv6 Geçiş Yöntemlerinin Güvenlik ve Performans Analizi,” Y.Lisans tezi, Yönetim Bilişim Sistemleri, Gazi Üniv., Ankara, Türkiye, 2010.
- [2] Internet World Stats “ Internet Usage Statistics” (2009), <http://www.internetworldstats.com/stats.htm>
- [3] 6bone, (2009) <http://go6.net/ipv6-6bone>
- [4] RFC 4380, Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)
- [5] RFC 4861, Neighbor Discovery for IP Version 6 (IPv6)
- [6] Netperf, (2009) <http://www.netperf.org/netperf/>
- [7] RFC 5180, IPv6 Benchmarking Methodology for Network Interconnect Devices
- [8] Miredo, (2009), <http://www.remlab.net/miredo/>

Beyhan ÇALIŞKAN 1981 yılında Bulgaristan’ın Şumen şehrinde doğdu. Lisans eğitimini Ankara’da bulunan Gazi Üniversitesi Eğitim Fakültesinde 2006 yılında tamamladıktan sonra aynı üniversitenin Bilişim Enstitüsünde 2010 yılında master eğitimini tamamladı. Özel sektörde Sistem Mühendisi ve İnternet Mühendisi olarak çalıştı. 2008 Mart ayında Ulusal Akademik Ağ ve Bilgi Merkezinde sistem yöneticisi olarak başladığı görevini sürdürmektedir.

Çalışkan, Unix sistemleri, ağ güvenliği, IPv6 konularında çalışmaktadır.