IPv6 GEÇİŞ YÖNTEMLERİNİN BAŞARIM DEĞERLENDİRMESİ

Arsan Adnan Hameed HAMEED

YÜKSEK LİSANS TEZİ

BİLGİSAYAR BİLİMLERİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

ARALIK 2013

ANKARA

Arsan Adnan Hameed HAMEED tarafından hazırlanan IPv6 GEÇİŞ YÖNTEMLERİNİN BAŞARIM DEĞERLENDİRMESİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Prof. Dr. O. Ayhan ERDEM
Tez Yöneticisi

Bu çalışma, jürimiz tarafından oy birliği ile Bilgisayar Bilimleri Anabilim Dalında Yüksek lisans tezi olarak kabul edilmiştir.

Başkan: : Doç. Dr. Suat ÖZDEMİR

Üye : Prof. Dr. O. Ayhan ERDEM

Üye : Yrd. Doç. Dr. Hüseyin POLAT

Tarih : 23/12/2013

Bu tez, Gazi Üniversitesi Bilişim Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Arsan Adnan Hameed HAMEED

IPv6 GEÇİŞ YÖNTEMLERİNİN BAŞARIM DEĞERLENDİRMESİ
(Yüksek Lisans Tezi)

Arsan Adnan Hameed HAMEED

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

Aralık 2013

ÖZET

IPv4'ten IPv6'ya geçiş beklenen zaman içerisinde gerçekleşmesede, IPv4 adres alanının tükenmesi ve giderek artan internet kullanıcısı sayısı nedeniyle IPv6'ya geçiş kaçınılmazdır. Bu çalışmanın amacı IPv6'ya geçiş için geliştirilen otomatik tünelleme yöntemlerinin, ağ performansını nasıl etkileyeceğidir. Bu tez çalışmasında IPv4, IPv6 ve otomatik tünelleme yöntemlerinden oluşan 6to4 ve ISATAP'ın performans ve kalite açısından karşılaştırılması yapılmıştır. Karşılaştırma benzetim programları kullanılarak sanal ortamda geliştirilmiştir. Ağ verimliliği, jitter ve kayıp paket oranı metrikleri, Jperf programı kullanılarak hesaplanmıştır.

Bilim Kodu : 902.1063
Anahtar Kelimeler : Bilgisayar ağları, internet, internet protokol sürüm 6-4, tünelleme, 6to4, ISATAP
Sayfa Adedi : 123
Tez Yöneticisi : Prof. Dr. O. Ayhan ERDEM

IPv6 TRANSITION MECHANISMS PERFORMANCE EVALUATION

(M.Sc. Thesis)

Arsan Adnan Hameed HAMEED

GAZİ UNIVERSITY
INFORMATICS INSTITUTE
December 2013

ABSTRACT

Transition from IPv4 to IPv6 has not realized as expected, but because of the ever growing demands of internet and depletion of IPv4 address space the transition must be occur. This thesis was aimed at understanding how the transition mechanisms (Automatic Tunneling) will effect to network performance. Tunneling mechanisms will compared in terms of performance with IPv4 and IPv6 in virtual environment by using simulation programs. Parameters such as throughput, jitter and packet loss were evaluated in a lab environment using Jperf

Science Code : **902.1063**
Key Words : **Computer networks, internet, internet protocol version 6-4, tunneling, 6to4, ISATAP**
Page Number : **123**
Adviser : **Prof. Dr. O. Ayhan ERDEM**

TEŞEKKÜR

Bu araştırmanın konusu, deneysel çalışmaların yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu büyük katkılarından dolayı tez danışmanım Sayın Prof. Dr. Ayhan ERDEM'e, her konuda öneri ve eleştirileriyle yardımlarını gördüğüm hocalarıma ve arkadaşlarıma teşekkür ederim.

Bu araştırma boyunca maddi ve manevi desteklerinden dolayı aileme teşekkür ederim.

İÇİNDEKİLER **SAYFA**

İÇİNDEKİLER (Devam) **SAYFA**

İÇİNDEKİLER (Devam) **SAYFA**

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil (Devam) **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur**.**

Kısaltmalar	**Açıklama**
IP	Internet Protocol - İnternet Protokolü
IPv4	Internet Protocol version 4 (İnternet Protokol Sürüm 4)
IPv6	Internet Protocol version 5 (İnternet Protokol Sürüm 6)
IETF	Internet Engineering Task Force (Internet Mühendisliği Görev Gücü)
ARIN	American Registry for Internet Numbers (Amerikan İnternet Numaralar Tescil Kurumu)
TCP	Transmission Control Protocol (Veri İletim Protokolü)
UDP	User Datagram Protocol (Veri İletim Protokolü)
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol (Site İçi Otomatik Tünel Adresleme Protokolü)
DSTM	Dual Stack Transition Mechanism (İkili Yığın Geçiş Yöntemi)
MTU	Maximum Transmission unit (Maksimum Transfer Birimi)
MAC	Media Access Control (Ortama Erişim Kontrolü)
SIIT	Stateless IP/ICMP Translation Algorithm (Durumsuz IP/ICMP Geçiş Yöntemi)
FP	Format Prefix (Önek Biçimi)

Kısaltmalar	Açıklama
NAT	Network Address Translator (Ağ Adresi Dönüştürücüsü)
TRT	Transport Relay Translator (Çevri Geçiş Yöntemi)
RFC	Request for Comments (Protokol Açıklama Dokümanları)
MCT	Manually Configured Tunnel (Elle Yapılandırılmış Tünelleme Yöntemi)
GRE	Generic Routing Encapsulation (Genel Yönlendirici Kapsüllemesi)
IANA	Internet Assigned Numbers Authority (İnternet Atanmış Numaralar Yöneticisi)

1. GİRİŞ

İnternet, dünyanın her yerinde birbirleriyle bağlantılı çok sayıda cihazlardan oluşan geniş bir ağdan ibarettir. İnternet ağına bağlı olan bu cihazların adreslemesini ve birbirleri ile iletişim kurmasını internet protokolü (IP) olanak sağlar. İnternet protokolün dördüncü sürümü (IP version 4 – IPv4) günümüzde yaygın olarak kullanılmaktadır; ancak internetin hızla gelişmesi karşısında gerek adres sayısı, gerekse veri ve güvenlik açısından yetersiz kalmıştır. Ortaya çıkan bu sorunlar karşısında yeni bir internet protokol sürümüne ihtiyaç duyulmuştur. Bu sıkıntıların giderilmesi için yeni nesil IP sürüm 6 (IP version 6 – IPv6) geliştirilmiştir. IPv6'yı devreye sokmak için üç ayrı geçiş yöntemi geliştirilmiştir: ikili yığın (dual stack), tünelleme (tunelling) ve çeviriciler (translation) geçişleridir.

Bu çalışmada, yalın IPv4 ağı, yalın IPv6 ağı ve IPv6'ya geçiş yöntemlerinden otomatik tünelleme yöntemleri (6to4 ve ISATAP) ağlarının başarım değerlendirmesi yapılmıştır. Denemelerden çıkan sonuçlar doğrultusunda ağlar arası karşılaştırma yapılmıştır. Denemeler tamamen sanal ortamda benzetim programları kullanılarak yapılmıştır. Karşılaştırmada ağ verimliliği, gecikme zamanı değişimi (jitter) ve kayıp paket oranı metrikleri hesaplanmıştır. Denemelerde veri iletim protokolleri TCP ve UDP kullanılmıştır.

Bu tez çalışması beş bölümden oluşmuştur. Çalışmanın ikinci bölümünde, literatürdeki ve konuyla ilgili diğer çalışmalar araştırılmıştır. Tezin üçüncü bölümünde, IPv4, IPv6 ve IPv6'ya geçiş teknikleriyle ilgili temel bilgiler sunulmuştur. Dördüncü bölümünde, mevcut çalışmaların eksik yönlerini göz önünde bulundurarak yalın IPv4, yalın IPv6, 6to4 ve ISATAP ağları geliştirilmiştir. Geliştirilen ağlar başarım açısından değerlendirilmiş ve çıkan sonuçlar doğrultusunda ağlar arası karşılaştırma yapılmıştır. Beşinci bölüm ise elde edilen sonuçların verildiği sonuç ve öneriler kısmıdır.

2. KONUYLA İLGİLİ YAPILAN ÇALIŞMALAR

IPv4 adres havuzu çağımızda yaşanan teknoloji evrimi karşısında yetersiz kalmıştır[1]. IPv6, IPv4'ün sıkıntılarını gidermek için geliştirilmiştir. IPv6 çok büyük adres havuzuna sahiptir dolayısıyla gelecekte adres sıkıntısı yaşanmayacaktır[2]. IPv6'ya geçiş yapmak için 3 ayrı yöntem bulunmaktadır. Bu yöntemleri kullanarak IPv6'ya sıkıntısız bir şekilde geçiş yapılabilir ancak geçiş sürecinde ağların performansı düşebilmektedir[3]. Bu konuyla ilgili mevcut çalışmalar ve yayınlanmış makaleler gösterilmektedir.

Hiromi, R. ve Yoshifuji, H. (2006) IPv4-IPv4 (ikili yığın) yönteminden kaynaklanabilecek sorunlar ele alınmıştır ve çözüm yolları önerilmiştir [4].

Govil, J. ve arkadaşları (2008) " An examination of IPv4 and IPv6: constraints and varios transition mechanisms " adlı çalışmada geçiş mekanizmaları ve bütün geçiş yöntemlerden kısaca bahsedilmiş ve her geçiş yönteminin olabilecek bağlantı hatalar ele alınmıştır, ancak çalışma sadece sözel olarak gerçekleştirilmiştir [5].

Lee, J. ve arkadaşları (2004) "An IPv4-to-IPv6 dual stack transition mechanism supporting transparent connections between IPv6 nodes and IPv4 nodes in integrated IPv6/IPv4 network". Bu çalışmada ikili yığın geçiş yöntemi DSTM (Dual Stack Transition Mechanism) çalışmanın baş konusu olmuştur. çalışma benzetim ikili yığın ağı kurarak DNS trafiğinin gecikme ve yanıt zamanı hesaplanmıştır. Çalışmada yazar IPv6, IPv4 ve ikili yığın yöntemi arasında belirtilen metrikleri hesaplayarak karşılaştırma yapmıştır [6].

Tahir, H. ve arkadaşları (2006) " Implementation of IPv4 Over IPv6 using (DSTM) on 6iNet " adlı çalışmada DSTM yöntemini sadece TCP protokolü kullanılarak test edilmiştir [7].

Kobayashi, K. ve arkadaşları (2003) IPv6'yı Gigabit ağ altyapısında uygulamış ve sonuçları tartışılmıştır [8].

Xiaorui, K. ve arkadaşları (2005) " Discovering IPv6 Network Topology " adlı çalışmada IPv6'nın yeni özelliği olan network discovery "Komşu Ağ" konusu ile

ilgili benzetim ağ kurarak söz konusu komşu ağ özelliğini çalıştırmış ve test edilmiştir [9].

Aua'afrah, R. ve arkadaşları (2010) BDMS (Bi-directional MapPing System) ve DSTM benzetim ağları kurarak performans karşılaştırması yapmıştır [10].

Hong, Y. ve arkadaşları (2003) "Application translation for IPv6 at NAT-PT" adlı çalışmada IPv6 Uygulama Katmanı Ağ Geçidi (ALG) konusu ile ilgili başarım değerlendirme çalışması yapılmıştır [11].

AL-tamimi, B. ve arkadaşları (2008) bu çalışmada Benzetim programları kullanarak otomatik tünelleme yöntemi Teredo (Tunneling IPv6 over UDP through NATs) ağı geliştirmiş ve uygulamıştır [12].

Shin, M. ve arkadaşları (2006) " An Empirical Analiyses of IPv6 Transition Mechanisms " bu çalışmada yalın IPv6 ağı, çeviriciler yöntemi ağları ile karşılaştırılmıştır ve sonuç olarak performansı düşük olan ağ tespit edilmiştir [13].

Karuppiah j. ve arkadaşları (2000) " IPv6 Dual Stack transition technique performance analysis: KAME on FreeBSD as the case " bu çalışmada, IPv6 ve IPv4 birbirileri ile kurduğu benzetim ikili yığın ağ üzerinden karşılaştırmıştır bu denemede FreeBSD işletim sistemi kullanılmıştır. Bu karşılaştırmada sadece gecikme süresi ve ağ verimliliği hesaplanmıştır [14].

3. İNTERNET PROTOKOLLERİ

Bilgisayara ve İnternet'e olan ihtiyaçlar gün gittikçe daha da artıyor. İhtiyaçların artması ile birlikte IETF (Internet Engineering Task Force) yeni İnternet protokolünü hazırlaması çalışmalarını yıllar önce başlattı. IPv4 ilk tasarlandığı zaman bu kadar başarılı olacağı düşünülmemişti. Bunun yanı sıra İnternet ağının bu kadar hızla büyümesi hiç tahmin edilmemişti. Bu yüzden yeni IPv6 biran önce devreye geçmesi lazım bu geçiş süreci de üç tane geçiş yöntemi kullanılarak gerçekleştirilebilir. Bunlar: İkili Yığın, Dönüştürücü ve Tünelleme. Bu bölümde İnternet protokolleri sürüm 4 ve sürüm 6, 6to4, ISATAP ve bunlara bağlı detaylar incelenecektir [2].

3.1. IPv4

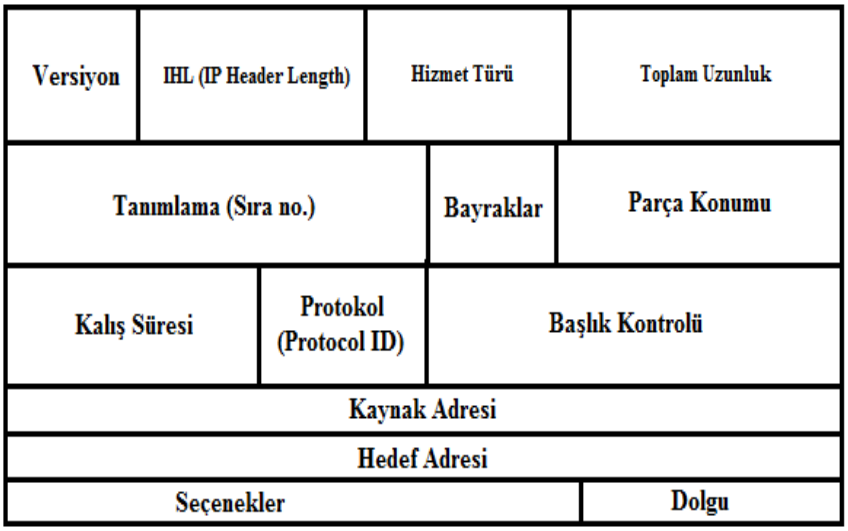
IPv4 protokolü 1981 yılında RFC (Request for Comment) 791 ile yayımlandıktan sonra yaygın bir şekilde kullanılmaktadır. Günümüze kadar IPv4 internet trafiğini başarılı bir şekilde taşımıştır. İnternet protokolü sürüm 4, o günlerin koşullarına göre tasarlanmıştır ve günümüzde bu kadar teknolojinin hâkim olduğu bir dönemde yetersiz kalmıştır [15]. Günümüzde IPv4 adres havuzunda önemli sıkıntılar yaşanılmaktadır ve bu sıkıntılar önümüzdeki yıllarda daha da artacağı öngörülmüştür. Örneğin dünyada hızla gelişen ülkelerden olan Çin'de IPv4 adres almaya çalışan kişi ve kurumlar sayısı ciddi sıkıntılar yaşamaktadır. IPv4 adresinin dağıtımında etkili yöntemlerin olmasından dolayı adres havuzu hızla tükenmektedir. IPv4 adresi 32 bitten oluşmaktadır ve bu sayı bizlere 4,294,967,296 farklı adres üretmektedir. Adreslerin bir kısmı yerel ağlar için ayırılmış bir kısmı araştırmalar için ayırılmıştır. Günümüzde teknolojilerin arttığı ve çevrimiçi uygulamaların bulunduğu bir dönemde IP adreslerine çok ihtiyaç duyulmuştur. Bu ihtiyaçlara karşı yapılan bazı çözümlerden alt ağ maskesi ve ağ adres çevrimi NAT (Network Address Translation) gibi geçici çözümler üretildi ancak bu çözümler ile birlikte ortaya yeni sorunlar çıkmıştır dolayısıyla bu problemleri kökten kaldıracak daha etkin çözümler aranmaya başlanmıştır [15].

IPv4 adreslerinin dünyaya adil bir şekilde dağıtılmamasından dolayı nüfusu çok olan ülkelerde ve bunun yanında hızla gelişmekte olan ülkelerde adres sıkıntıları erken hissedilmeye başlanmıştır. Örnek olarak Japonya, Çin, Güney Kore ve Hindistan gibi ülkeler adres sıkıntısı yaşayan ülkelerdir. IPv4 ABD tarafından ilk tasarlandığında %55'ne hâkim durumdaydı, bu oran daha sonra IPv4'ün dünya çapında kullanılmasıyla %37 düştü ancak bu oran da çok yüksek orandadır. Diğer ülkeler ile mukayese edildiğinde örneğin Türkiye IP adreslerinin % 0.41'ine sahiptir. Dünyanın neredeyse her yerinde internet ve teknolojik cihazların bulunduğu bir dünyadayız. Bu adres sıkıntısını bir an önce çözüme kavuşturmak gerekmektedir. IPv6 bu sıkıntıları kökten çözecek bir şekilde tasarlandı ve adres dağılımı IPv4'te yaşanan hataların tekrarlanmaması için sistematik bir şekilde dağıtılacaktır [15].

3.1.1. IPv4 başlık biçimi

IPv4 adresleri 32 bit uzunluğunda, ikili sayılardan 0'lar ve 1'lerden oluşmaktadır. IPv4 adreslerinin okunurluğunu kolaylaştırmak için onluk sayılar şeklinde yazılmaktadır. 192.168.45.1 bu IPv4 adresi onluk şeklinde yazılmıştır ancak bu adres bilgisayar tarafından ikili sayılar şeklinde okunmaktadır[15,16,17].

192.168.45.1 = 11000000.10101000.00101101.00000001.



Şekil 3.1. IPv4 yapısı.

IPv4 başlığı Şekil 3.1'de gösterilmiştir. Başlıkta bulunan bütün bölümler aşağıda sırasıyla anlatılmıştır.

Versiyon: İnternet protokolünün sürümünü belirten bölümdür ve 4 bitten oluşmaktadır[18].

IHL: İnternet protokolünün başlık uzunluğunu beliren bölümdür. İnternet protokolünde en küçük Başlık 20 Byte'ten oluşmaktadır en büyük başlık ise 60 Byte' ten oluşur[18].

Hizmet Türü: Özel uygulamalar tarafından kullanılan bir alandır boyutu 8 bittir. [18].

Toplam Uzunluk: Ağ üzerinden gönderilen paketlerin toplam uzunluğunu belirten bölümdür, boyutu 16 bittir [18].

Tanımlama: Paketlerin ilişkilendirmesini sağlayan rastgele bir sayıdır. Boyutu 16 bittir [18].

Bayrak: paketlerin parçalar şekline bölündüğünde bu parçaların hedefine ulaşması için denetimi sağlayan bölümdür. Boyutu 3 bittir[18].

Parça Konumu: IPv4 paketlerinin hangi sırada birleşerek datayı oluşturacağını gösteren kısımdır. Boyutu 13 bittir[18].

Kalış Süresi: veri paketinin düğümler arasındaki hop sayısını belirtir. Boyutu 8 bittir [18].

Protokol: İnternet paketinin içine entegre edilmiş üst seviyedeki protokolü belirtmektedir. Boyutu 8 bittir[18].

Başlık Kontrolü: Veri paketinin aktarım sırasında bozulmaya uğrayıp uğramadığını test etmek için tutulan bölümdür. Boyutu 8 bittir[18].

Kaynak Adresi: Kaynak düğümün IP adresini belirten 32 bitlik bir alandır [18].

Hedef Adresi: Hedef düğümün IP adresini belirten 32 bitlik bir alandır [18].

Seçenekler: İnternet protokol başlığında bulunan özellikleri taşıyan alandır. Bu alanda bulunan bütün özellikler etkinleştirene kadar değerleri 0'dır. Etkinleştirmek istenilen özelik değeri 1'e dönüştürülür. Bu alanın boyutu bütün özellikler etkinleştirilirse 40 Bit'e kadar çıkmaktadır [18].

Dolgu: IP paket başlığının 32 bitin katları şeklinde olmasını sağlayan alandır. Boyutu kullanılan başlığa göre değişmektedir[18].

IPv4'te küresel IP adresleri ve özel IP adresleri mevcuttur. Küresel IP adresleri, dünyada eşi benzeri olmayan bir IP adrestir. Küresel IP'yi dışarıya yönlendirme yapabilmektedir. Özel IP adresi ise bir site içerisinde ya da bir iş yerinde ya da ev içinde yani yerel ağlarda kullanılmaktadır ancak bu adresler dışarıya veya internet üzerinden yönlendirme yapamamaktadır. İki düğümün birbirleri ile internet üzerinden iletişim kurmaları için mutlaka 2 küresel IP adresleri olması gerekmektedir. IPv4 adres sıkıntısından dolayı bir çözüm olarak ortaya çıkan NAT sayesinde bir yerel ağ içerisinde birden fazla kullanıcıyı tek küresel IP adres üzerinden internete bağlanabilir[15,16].

3.1.2. IPv4 adres atama

Şuana kadar iki çeşit internet adresi bulunmaktadır. Birisi günümüzde kullanılan IPv4 (32bit) diğer ise yeni IPv6 (128bit). IPv4 çok yaygın bir şekilde kullanmasından dolayı adres havuzu tükenmek üzeredir dolayısıyla yeni IPv6 yaygınlaşması ciddi derecede hız kazanmaktadır. IPv6, sunduğu kolaylıklar ve birçok özellikler yaygınlaşmasını kolaylaştırmaktadır. IPv4 adresinin kolay okunması için 8 bitten oluşan dört oktet halinde ifade edilmektedir. Toplam IPv4 adres sayısı 4 milyar 294 milyon 967 bin 196 adet adrestir. IPv4 adresi noktalı yazım sistemiyle yazılır (Dotted Decimal Notation). IPv4 adresinde bulunan dört oktetin her birinde 0 ile 255 arasında değişen sayılardan oluşur. IPv4 adresleri iki bölümden oluşur: Ağ numarası ve düğüm numarası. Ağ numarası, bilgisayarın hangi ağa ait olduğunu gösterir, düğüm numarası ise bilgisayarın bulunduğu ağda diğer bilgisayarlardan ayırması için kullanılan bir numaradır[17].

IPv4 günümüzde halen kullanılmakta olan internet protokolüdür. IPv4, beş sınıftan oluşmaktadır bu sınıfların detayları ve özellikleri Çizelge 3.1'de gösterilmiştir.

Çizelge 3.1. IPv4 sınıfları.

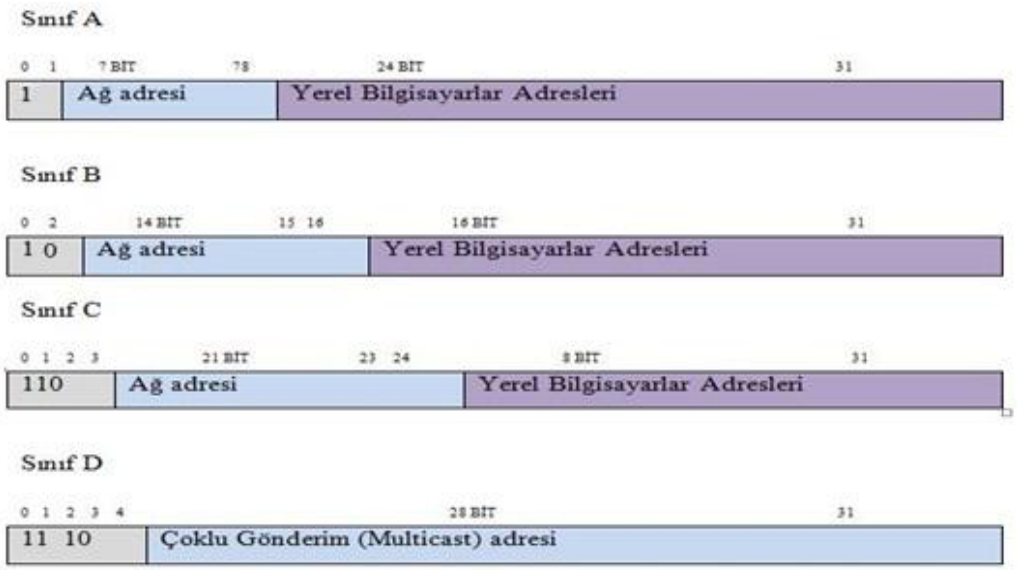
Adres sınıfı	Kurulabilir ağ sayısı	Kullanıcı adres Sayısı
A	126	16 Milyon
B	16382	65534
C	2 Milyon	256
D	Çoklu-Yayın kullanım için ayrılmıştır	
E	Gelecekte kullanım için ayrılmıştır	

3.1.3. Ağ'da adresleme

IP; İnternet üzerindeki cihazların adreslemesini ve birbirleriyle iletişiminin gerçekleştirilmesine olanak sağlamaktadır. Ağa bağlı olan her donanım için 32 bitten oluşan bir IP adresi olması gerekmektedir. IP adresi atanması için dikkat edilmesi gereken birçok husus vardır. Bunlardan en önemlisi bir adres atanırken belli bir cihaza diğer cihazlara atanmış olan adresin başka bir cihaza atanmamış olması gerekmektedir. Bunun yanında da atanan bir IP adresinin ağ numarası aynı ağ içerisinde bulunan bütün cihazlarda aynı olması gerekmektedir[15].

3.1.4. IPv4 adres sınıfları

İnternet protokolü sürüm 4, Beş temel sınıfa ayrılmıştır. Bunlar; A,B,C,D ve E sınıfları olarak ayrılmıştır. Ağ kurulumu sırasında sınıf seçimi kurulan ağın büyüklüğüne bağlıdır. IP adresleri iki kısma ayrılır; ağ adresi ve donanım adresi. Ağ adresi aynı olan cihazların aynı ağda olduğunu göstermektedir. Ağ adresleri yönlendiriciler için çok önemlidir, bütün yönlendirmeler ağ adresine bakılarak yapılmaktadır. İnternet protokolünde ağ adresi ile donanım adresinin ayrılması için ağ maskesi kullanılır. IPv4 adres sınıflarına göre bit dağılımı Şekil 3.2'de gösterilmektedir[15].



Şekil 3.2. IPv4 adres bit dağılımı

Yukarıdaki Çizelge 3.2'de her sınıf için atanabilecek maksimum düğüm sayısı belirtilmiştir.

IPv4 Sınıf A

IPv4 sınıflarının ilk sınıfı olan A sınıfı büyük ağlarda kullanılan adres sınıfıdır. A sınıfının sadece ilk okteti ağ adresini temsil etmektedir, geride kalan üç oktet ise düğüm adresleri için ayırılmıştır. A sınıfı 16 milyon düğüm adresi barındırmaktadır. Bu tür sınıf büyük şirketlerde kullanılır örneğin Microsoft şirketi Çizelge (Bkz. Çizelge 3.1) [15].

IPv4 Sınıf B

IPv4, B sınıfı orta büyüklükte olan ağlarda kullanılmaktadır. Bu sınıfta ilk iki oktet ağ adresini temsil ederken diğer iki oktet ise düğüm adresleri için ayırılmıştır. B sınıfı kullanarak 16382 alt ağ oluşturabiliriz ve her alt ağda 65534 düğüm adreslenebilir. B sınıfı çoğunlukla orta boy ağlarda kullanılmaktadır örneğin üniversiteler ve şirketler ağları (Bkz.Çizelge 3.1) [15].

IPv4 Sınıf C

Küçük ağlarda kullanılan IPv4 C sınıfı 3 oktetini ağ adresi için ayırırken geride kalan bir oktet ise düğüm adres için ayırmıştır. C sınıfını kullanıldığında yaklaşık iki milyon alt ağ oluşturulabilir ve her alt ağda 254 düğüm adreslenebilir. (Bkz. Çizelge 3.1) [15].

IPv4 Sınıf D,E

IPv4, D ve E sınıfları düğümler adreslemesi için kullanılamaz. D sınıfı çoklu gönderim için kullanılmaktadır. E sınıfı gelecek için ayırılmıştır (Bkz. Çizelge 3.1) [15].

Özel IP Adresleri

IPv4'te düğüm okteti 0 olan adreslerin hiçbir bilgisayara ait olmaması anlamına gelmektedir. Bu tür adresler yönlendiriciler tarafından yönlendirme tablosu oluşturması için kullanılmaktadır örneğin 192.168.121.0.

255 ile biten IPv4 adresleri genel yayın adresleri olarak bilinir. Belli bir mesajı ilgili ağda bulunan her bilgisayara duyurulmasını sağlayan adreslerdir.

Her dört okteti 255 olan IPv4 küresel yayın adresidir. Tüm ağlara ve bilgisayara aynı anda belli bir mesajı iletir. Bu tür IP adresler bütün ağları ve bilgisayarları aynı anda adresler.

127.0.0.1 adresi IPv4 özel adreslerindendir. Bu adres bilgisayarın TCP/IP protokolünü test etmek için kullanılır. (Bkz. Çizelge 3.1) (Bkz. Şekil 3.2) [15].

3.1.5. Alt ağlar

Alt ağlar veya (subnetting) IPv4 adreslemenin en önemli adresleme yollarındandır. Büyük ağlarda, adreslerin daha sistematik bir şekilde ve daha küçük parçalara ayrılarak alt ağlar oluşturur.

Alt ağlarına örnek olarak bir üniversite ağı B sınıfı IPv4 adresi ile adreslenecektir, adresleme işleminde üniversitede bulunan her cihaza tek parça şeklinde adres vererek

adresleme işlemi karışık bir hale gelecektir. Onun yerine alt ağları kullanarak ve üniversite ağını küçük alanlara bölerek daha sistematik ve kullanışlı olacaktır. Böylece hem adres atama ve hata ayıklaması ve düzeltmesi daha kolay olur. Bu hiyerarşik yapı sayesinde problemi yakalamak daha hızlı olacaktır çünkü hata veren bir bilgisayarın hangi alt ağa ait olduğu IP adresine bakılarak bulunur ve bütün ağı taramaksızın sadece ilgili alt ağda hatayı ayıklayarak hatayı hızlıca giderebiliriz. Ağların alt ağlara ayrılmasının faydaları ise mevcut internet protokolünü adreslerinin sınırlı olmasından dolayıdır, bu işlem sayesinde boşa harcanmış IP adreslerini en az seviyeye düşürülür. Ağların alt ağlara parçalanması yoğun çoklu gönderim yayın mesajlarını azaltır ve dolayısıyla ağ sistemi yoğun trafiğe maruz kalmamış olacaktır, bu da ağ performansını artırır[15].

3.1.6. Ağ maskesi

Alt ağları yönetmenin en önemli öğelerinden olan ağ maskesi (Subnet mask) alt ağların ölçümünü belirlemesini sağlamaktadır. IP adresinin hangi kısmı ağ adresi ve hangisi düğüm adresi olduğu ağ maskesine bakılarak öğrenilir. Ağ maskesi alt ağların kullanıcı sayısına göre ayarlanmalıdır. Bir alt ağda bulunan bilgisayarın iletişime geçmek istediği bir bilgisayar ile aynı ağda değilse doğrudan iletişime geçemez ancak ayna ağda bulunan iki bilgisayar doğrudan birbirleri ile iletişime geçebilirler. Alt ağda bulunan bir bilgisayarın hangi alt ağa ait olduğunu IP adresinde bulunan ağ kısmına bakılarak öğrenilebilir. IP adresi iki kısımdan oluşur; ağ kısmı ve düğüm kısmı. Bir IP adresinde ağ kısmının ile düğüm kısmını ayırt etmek için ağ maskesine bakılır.

Şekil 3.3. Ipv4 alt ağ maskesi

Örnek olarak Şekil 3.3'te iki adet bilgisayar bulunmaktadır. Bu iki bilgisayar birbirleri ile Ethernet kablosu ile doğrudan bağlanmıştır. Sol taraftaki bilgisayar C sınıfı 192.168.67.150 IPv4 adresi ile adreslenmiştir ve bu bilgisayarın ağ maskesi 255.255.255.0'dır bu bilgisayarın sağ tarafta bulunan bilgisayarla iletişime geçmesi için her iki bilgisayarın aynı ağda bulunması şarttır. Sağdaki bilgisayar C sınıfı 192.168.67.200 IPv4 adresi ile adreslenmiştir ve ağ maskesi de 255.255.255.0'dır. ağ maskesine bakılarak her iki bilgisayarın aynı ağ adresi aralığında olduklarını öğrenebiliriz. Her iki bilgisayarın ağ adresi 192.168.67.0 dolayısıyla Bu bilgisayarlar doğrudan birbirleri ile iletişime geçebilmektedir [15].

3.2. IPv6

İnternet protokolleri muazzam örümcek ağı adı verilen internet'in temelini oluşturmaktadır. Şu anda yaygın olarak kullanılan IPv4 1981 yılında RFC 791 tarafından tanımlanmıştır. IPv4 32 bitlik uzunluğa sahiptir ve bu uzunlukta yaklaşık 4 milyar adres yapmaktadır.[16]. IPv4 adresleri yapılan çalışmalara göre yakın tarihte tükenecektir. Bu adres aralığı sıkıntısı aslında IPv4 adres aralığının tümü adreslerin kullanılmasından kaynaklanmamaktadır. Bu adreslerin bilgisayarlara tek tek verilmeyip aslında birer ağ dâhilinde dağıtılması, adreslerin verimli kullanımını engellemektedir. Adres dağıtımı yapılan ağlar üç sınıfa ayrılmıştır[31].

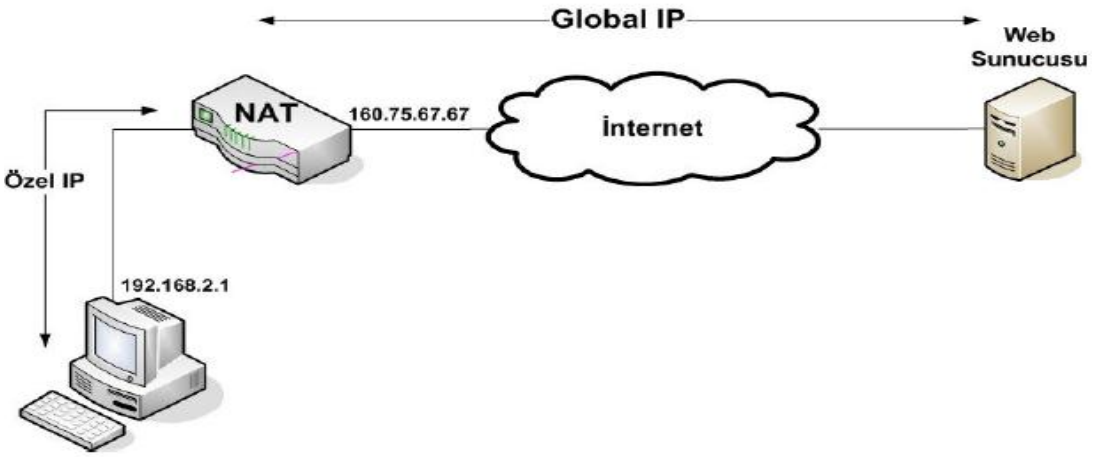
- Sınıf A'da 128 adet ağ ve her bir ağa 16 milyon adres düşmektedir.
- Sınıf B'de 16.000 adet ağ ve her ağda 65.000 adet adres bulunmaktadır.
- Sınıf C'de 2 milyon ağ ve her ağda 254 kullanılabilir adres bulunmaktadır.

Problemin kaynağını bu mimaride aramak gerekmektedir. Mesela B sınıfı bir adres aralığı alan bir firmanın 65.000 adet IP adresine ihtiyacı olmasa bile bu adresler kendisine atanmaktadır ve başka bir firma tarafından kullanılamamaktadır. Bu da çok ciddi adres israfına neden olmaktadır[31].

Bu anlatılan adres darlığının yakın bir süre içinde İnternet için bir problem haline geleceği gerçeği 1991 yılında anlaşılmış ve yeni nesil İnternet Protokolü konusunda çalışmalar başlatılmıştır. Yeni nesil IP çalışmalarına paralel olarak mevcut protokol

olan IPv4'ün ömrünün nasıl uzatılabileceği konusu üzerine de yoğun çalışmalar yapılmıştır. Bu çalışmalar sonucunda 1993 yılında İnternet'e yeni bir soluk getirmek amacıyla CIDR (Classless Inter-Domain Routing) haberleşme dünyasına tanıtılmıştır [31].

CIDR'da asıl amaç sınıfsal adres dağıtımını ortadan kaldırarak mevcut IPv4 adreslerini daha verimli kullanabilmektir. Bu konuda da başarılı olunmuştur. Ancak gerek şimdiye kadar dağıtılmış birçok adres nedeniyle gerekse İnternet'in çok hızlı gelişmesi ve İnternet'e bağlanan cihazların sayısının giderek artması nedeniyle CIDR da tam olarak bir çözüm olamamıştır. IPv4 adres sorununu çözmek için geliştirilen diğer bir yöntem ise NAT olarak adlandırılmış ve RFC 1597 ile RFC 1918'de tanımlanmıştır (Şekil 3.4). NAT'ın çalışma mantığına göre tüm ağların içindeki adresler aynı özel IP adresleri olabilmekte ve bu adresler ağ dışına yönlendirilememektedir. Ancak ağ içindeki cihazlar ağ dışına veya İnternet'e çıkarken küresel adres ile eşleşmektedirler. Bu şekilde sadece ağ dışına çıkan cihazlara küresel IPv4 adresi atanmakta ve adres tasarrufu sağlanabilmektedir.



Şekil 3.4. NAT örneği

Şekil 3.4'de özel IP adresi 192.168.2.1 olan bir makinenin internet 'teki bir web sunucusu ile haberleşmesi gösterilmektedir. Bu cihazın paketlerinin İnternet ortamında yönlendirilebilmesi için yerel ağ dışına çıkarken, NAT cihazı tarafından küresel bir IP ile eşleştirilmesi lazımdır. Örnekte eşleştirilen IP adresi

160.75.67.67'dir. Bu adres küresel bir IP adresidir ve tüm dünyada sadece bir makineye verilebilir. Ancak 192.168.2.1 adresi özel bir IP adresidir ve aynı yerel alan ağı içinde birden fazla kullanılmamak şartıyla değişik ağlarda sayısız bir şekilde tekrarlanabilmektedir[31].

Özel adresler internet adresi otoritesi olan IANA (Internet Assigned Numbers Authority) tarafından 3 blok olarak tanımlanmışlardır:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

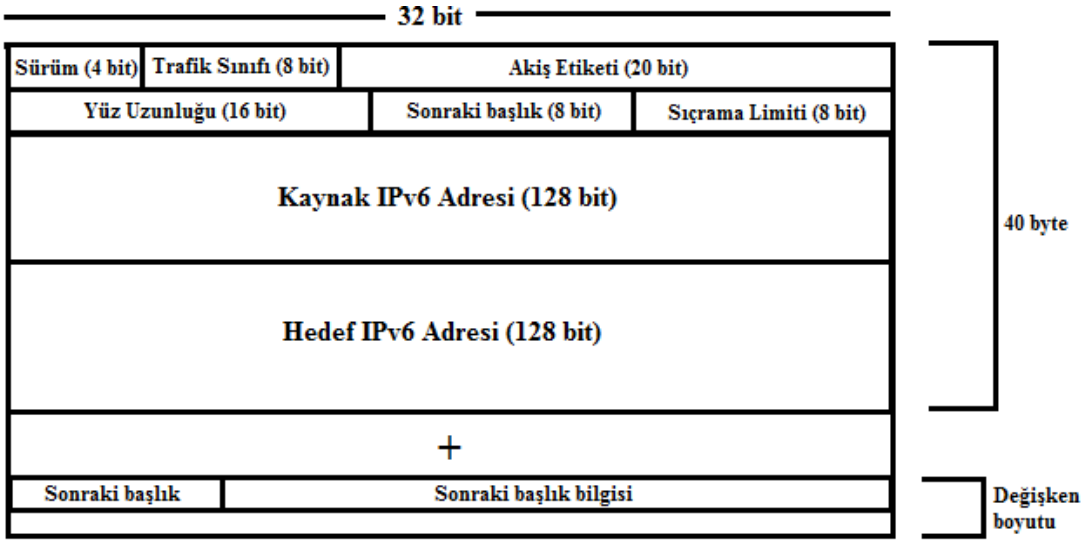
İlk blok 24 bitlik, ikinci blok 20 bitlik ve üçüncüsü 16 bitliktir. Bu adreslerden herhangi bir çeşidini kullanmak isteyen bir firma IANA'ya danışmaya gerek olmadan rahatça adres dağıtımı yapabilir. Çünkü özel IP adreslerinin yerel alan ağı dışında hiçbir geçerliliği yoktur ve başka bir firmanın özel IP adresiyle çakışma olasılığı yoktur. NAT yerel alan ağlarında geniş anlamda kullanım bulmuştur ve IP adres aralığındaki azalmayı yavaşlatmıştır. Ancak uçtan uca (peer-to-peer) bağlantıyı imkânsız kılması nedeniyle özellikle ses ve görüntü servisleri gibi servislerde kullanılamamış ve yeni nesil bir IP ihtiyacını gidememiştir. Bütün bu gelişmeler göz önüne alınarak IPv6 yapısı, ihtiyaçları en iyi şekilde karşılayabilecek şekilde geliştirilmeye çalışılmıştır. Bu araştırma geliştirme sırasında yeni nesil protokolün aşağıdaki özellikleri sağlaması gerektiğine karar verilmiştir:

- Sağlayacağı adres aralığının hiçbir zaman bitme derdinin olmaması
- IPv4'teki gibi sınıfsal adres dağıtımını kullanmak yerine CIDR kullanmak.
- Şuanda IPv4 ile çok kabarmış olan yönlendirici tablolarının boyutunu düşürmek ve yönlendirmeyi daha verimli hale getirmek.
- İnternet için küresel IP adresleri, yerel ağ için yerel IP adresleri kullanmak.

IPv4'te eksikliği hissedilen yukarıdaki özellikler doğrultusunda geliştirilen IPv6; IPv6 adres yapısı, IPv6 başlığı ve eklentileri, IPv6 yönlendirme, IPv6 alan adı sistemi ve IPv6'ya geçiş teknikleri başlıkları altında aşağıda detaylı bir şekilde incelenecektir [31].

3.2.1. IPv6 temel başlık biçimi

IPv6'nın temel başlık biçimi Şekil 3.5'da gösterilmiştir. Bu başlık, standart boyutu 40 Byte olan IPv6 başlığı ve seçime bağlı ek başlıklardan oluşur. Bazı ek başlıklar temel başlıktan büyük bazıları ise küçüktür. Ek başlıklar seçime bağlı olarak sıfır ya da n tane olabilir. Üst katman verisi diğer tüm kısımlardan büyüktür[20].



Şekil 3.5. IPv6 başlık biçimi

IPv6 Paket Başlığında Sırası İle Aşağıdaki Alanlar Bulunmaktadır:

Sürüm: Bu alan IPv4'teki sürüm alanı ile aynı uzunlukta yani 4 bit uzunluğundadır ve İnternet protokolünün hangi sürüm olduğunu belirtmektedir. IPv6 için 6 değerini almaktadır[20].

Trafik sınıfı: 8 bitlik bir alandır. IPv4'teki hizmet tipi alanı yerine getirilmiştir. IPv6 paketleri arasındaki değişik sınıf ve öncelikleri belirtme görevini üstlenmektedir[20].

Akış etiketi: 20 bit uzunluğundaki akış etiketi bölümü değişik akış yönleri çizen paket dizilerini etiketlemek için kullanılmaktadır. Bu etiketleme genellikle servis çeşitlerine göre yapılmaktadır. Akış etiketini desteklemeyen bir düğüm eğer paketi yaratıyorsa bu alana sıfır değeri yerleştirir, paketi yönlendiriyorsa bu alanı hiç değiştirmeden paketi yönlendirir, eğer paketi alan tarafsa bu alandaki değeri hiç dikkate almaz[20].

Yük uzunluğu: IPv6 başlığını takip eden tüm paketin uzunluğunu 16 bitlik bir alanda ifade etmektedir. Eğer pakette bir veya birden fazla eklenti başlığı varsa onlarda bu uzunluğa dâhil edilir. IPv4 başlığındaki karşılığı toplam uzunluk alanıdır[20].

Sonraki başlık: 8 bitlik bu alanda IPv6 başlığından hemen sonra gelen başlık çeşidi belirtilmektedir. Bu herhangi bir eklenti başlığı olabilir veya TCP, UDP gibi daha üst seviyelerden bir protokol olabilir. IPv4'te protokol alanı adıyla geçmektedir[20].

Atlama limiti: 8 bitlik bir değerle ifade edilmektedir. Paket her bir düğümden geçtikçe atlama limiti sayısı bir eksiltilmektedir. Bu sayı sıfır olduğu zaman paket atılmaktadır. IPv4'teki karşılığı TTL alanıdır[20].

Kaynak adresi: 128 bitlik paketin kaynak adresini belirten alandır.

Hedef adresi: 128 bitlik paketin hedef adresini belirten alandır. Eğer yönlendirici başlığı varsa, hedef adres bu sefer en son alıcının adresi değildir[20].

3.2.2. IPv6 adres ön ekleri

IPv6 ön ekleri (prefix) gösterimi IPv4'de kullanılanla aynı şekilde CIDR gösterimine göre ifade edilmektedir. 24 bitlik alt ağ maskesine sahip olan bir IPv4 adresi 192.168.1.0/24 şeklinde gösterilirken, 48 bitlik bir ön eke sahip IPv6 adresi de 2001:0:2310::/48 şeklinde gösterilmektedir. Bu adres için aşağıdaki gösterimlerin tamamı doğrudur:

2001:0000:2310:0000:0000:0000:0000:0000/48

2001:0:2310:0:0:0:0:0/48

2001:0:2310:: /48

Ancak aşağıdaki gösterimler doğru değildir:

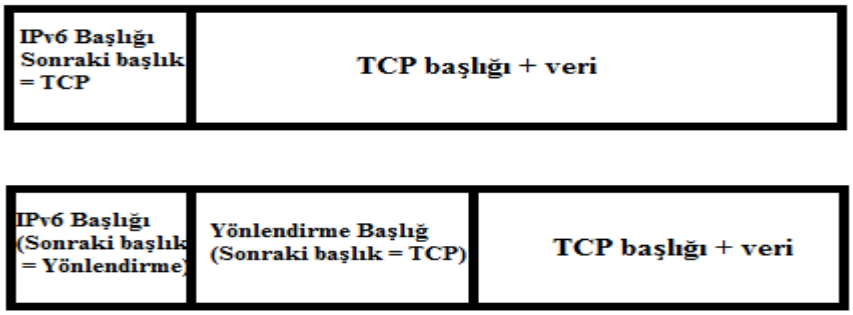
2001:0:231/48	Sağ taraftaki 0'lar ön eke göre gösterilmeyebilir ancak 16 bitlik bloğun içindeki sağda bulunan bir sayıyı takip eden 0'lar atılamaz. Yukarıdaki gösterim 2001:0:2310/48 şeklinde değil de 2001:0:0231/48 şeklinde anlaşılmaktadır.
2001::2310/48	Bu adres gösterimi de yukarıdaki adresi ifade etmemektedir. Bu adres 2001:0:0:0:0:0:0:2310 şeklinde bir adresi belirtmektedir.
2001::2310:: /48	Bu gösterim tamamen söz dizimi hatasıdır, "::" ifadesi bir adresin içinde birden fazla kullanılamaz.

Alt ağ maskesi ile uç nokta adresi tek bir şekilde gösterilebilmektedir. Mesela alt ağ maskesi 2001:4BD0:2031::/48 olan bir ağda, bir sunucuya 2001:4BD0:2031::1 adresi verilmiş olsun. Bu sunucunun adresi alt ağ maskesi ile birlikte ifade edilmek istenirse 2001:4BD0:2031::1/48 şeklinde gösterilir[21].

3.2.3. Eklenti başlıkları

IPv4'te seçime bağlı alanlar için yerler ayrılmıştır. Yani o alan kullanılmasa da o yer vardır ve bu alanlar her yönlendirici tarafından tek tek incelenmektedir. Kullanılmayan yerler hem paket boyutunu arttırmakta hem de yönlendiricinin işini zorlaştırmaktadır[21].

IPv6'da İnternet katmanı bilgisi seçeneğe bağlı olarak ayrı başlıklar halinde pakete eklenebilmektedir ve bu eklenen bölüm IPv6 başlığı ile daha üst seviye protokol başlığının arasında olmaktadır. IPv6 paketi içinde bir, iki veya daha fazla eklenti başlığı olabildiği gibi hiç eklenti başlığı olmayabilir de. Eğer eklenti başlığı varsa bu sonraki başlık alanında bir önceki başlıkta ifade edilmektedir[21].



Şekil 3.6. IPv6 eklenti başlıklar

Şekil 3.6'ye göre birinci durumda IPv6 başlığından hemen sonra TCP başlığının gelmektedir yani eklenti başlığı kullanılmamaktadır. İkinci durumda ise IPv6 başlığı ile TCP başlığı arasında bir yönlendirme başlığı kullanılmıştır. Eklenti başlıkları incelenirken başlık içerikleri bir sonraki eklenti başlığının incelenip incelenmeyeceğini belirtir. Bu sebepten dolayı eklenti başlıkları her zaman bir sıraya göre eklenmelidir. Kullanılabilecek altı çeşit eklenti başlığı kullanım sırasına göre aşağıda belirtilmektedir:

- Atlama noktası seçenekleri
- Hedef seçenekleri
- Yönlendirme
- Parçalara ayırma
- Kimlik doğrulaması
- Güvenlik başlığı

Hedef seçenekleri eklenti başlığı ara düğümleri belirtmeyip sadece son noktayı belirtiyorsa, bu eklenti başlığı ikinci sıraya değil en son sıraya yerleştirilmelidir.

Ek başlık kullanmanın iki temel nedeni vardır;

- Ekonomi: Eğer ek başlık IPv6 temel başlığa IPv4'teki gibi yerleştirilseydi bazen ihtiyaç olmadığı halde bu kısımlar paket boyutunda olacaklardı ki, bu da fazladan gereksiz veri iletimi ve bant genişliği kullanma anlamına gelir. Mesela IPv4 bölümlendirme istenmeyen durumda dahi bölümlendirme bilgisi

taşırdı, ama İPv6 gerekirse bunun için ilgili ek başlığa başvurur, gerekmezse kullanmaz. Böylece gereksiz başlıkların datagramdan çıkarılması ile zaman ve bant genişliğinden tasarruf edilmiştir[21].

- Genişletilebilme ve Geliştirilebilme: IPv4 sabit bir başlık kullanmıştır ve değişiklik istenince tüm başlık değişir. IPv6 ise her değişimi yeni bir ek başlık olarak algıladığından değişime açık tasarlanmıştır. Sonraki başlık bölmesi bu işlevi sağlar. Bu nedenle, internete yeni bir özellik eklenmesi durumunda tüm interneti değiştirmek yerine yeni bir ek başlık tasarlamak yeterli olur. Mesela datagramın tamamı şifrelenmek istenirse bir adet şifre ek başlığı ile bu işlem yapılır. Ayrıca deneme amaçlı başlıklar rahatça denenip yararlı görülenler kullanılır[21].

3.2.4. IPv6 adres sayısı

IPv6'nın geliştirilmesindeki ana neden IPv4 adres aralığının er ya da geç biteceği gerçeğidir. Bu sebeple 32 bit olan IPv4 adresleme yapısı IPv6'da 128 bit'e genişletilmiştir. 128 bit ile 2^{128} adet adres sağlanabilmektedir. Bu sayı yaklaşık olarak 10^{38}'e, tam olarak da 40.282.366.920.938.463.463.374.607.431.768.211.456 adet adrese denk gelmektedir. Dünya yüzeyinin 511.263.971.197.990 metre kare olduğu bilgisi kullanılarak, dünya üzerindeki her metrekare alana yaklaşık 655,5* 10^{23} adres düşmekte olduğu hesaplanabilmektedir. Bu da inanılmaz bir adres sayısıdır[18].

3.2.5. IPv6 adres yapısı

IPv4 adresleri 8 bitlik 4 blok şeklindedir. Bloklar arasına nokta işareti koyularak ifade edilmektedir. Örnek adres gösterimi 160.75.67.1 şeklindedir. Aynı şekilde IPv6 adresleri için de tasarım zamanında noktalı bir gösterim seçilebilirdi ancak IPv4 adreslerine göre 4 kat daha uzun oldukları için değişik bir gösterim seçilmiştir. Onluk sayı sistemi yerine onaltılık sayı sistemi kullanılarak IPv6 adresinin daha kısa bir uzunlukla ifade edilmesi sağlanmış ve bloklar arasına iki nokta işareti koyulması uygun görülmüştür. 2001:4BD0:2031:2345:6AE2:FF23:245A:90BB örnek bir IPv6 adresini göstermektedir.

IPv6 adresleri üç değişik şekilde ifade edilmektedirler.

- Tercih edilen gösteriş biçimi x:x:x:x:x:x:x:x şeklindedir. Bu gösterimde her bir x onaltılık sayı düzeninde yazılmış 16 bitlik adres parçalarını ifade etmektedir. Örnek olarak

  2001:4BD0:2031:2345:6AE2:FF23:245A:90BB adresi verilebilir. Veya 2001:4BD0:2031:0:0:0:1 şeklindeki gibi 16 bitlik sayı parçalarının sol tarafındaki anlamsız 0'ları yazmadan kısaltılmış bir biçimde gösterilebilir.

- Bazı IPv6 adreslerinde birbirini takip eden uzun sıfır dizileri bulunmaktadır. Bu tür adresleri daha kolay ifade edebilmek için bir kısaltma yöntemi geliştirilmiştir. Bu yönteme göre "::" gösterimi bir veya daha çok 16 bitlik sıfır dizisini ifade etmektedir. Örnek olarak belirtilen adresler:

  2001:4BD0:2031:0:0:0:0:1 tekli-yayın adresi

  FF01:0:0:0:0:0:0:101 çoklu-yayın adresi

  0:0:0:0:0:0:0:1 loopback adresi

Aşağıdaki şekilde gösterilebilir:

2001:4BD0:2031::1 tekli-yayın adresi

FF01::101 çoklu-yayın adresi

::1 loopback adresi

- Bazı durumlarda IPv4 ve IPv6 protokolleri beraber kullanılmaktadır. Bu gibi durumlarda x:x:x:x:x:x:d.d.d.d şeklinde bir gösterim kullanılabilmektedir. X'ler 16 bitlik altı adet bloğu onaltılık sayı sisteminde, d'ler de 8 bitlik 4 det bloğu onluk sayı sisteminde göstermektedir. 2001:4BD0:0:0:0:0:160.60.67.1bu tarz gösterime bir örnektir. Bu gösterimde son 32 bit standart IPv4 adresi yapısındadır[22].

3.2.6. Yeni IP için isimlendirme

Yeni internet protokolü için önceleri IP “next generation” (yeni nesil internet) adı düşünüldü daha sonra IP’leri sürüm numarası ile ayırma fikri oluştu ve mevcutta sürüm 4 yeni olana sürüm 6 denildi. IPv4’ten sonra IPv5 değil de IPv6’ya geçişin sebebi IPv5’in bir test protokolü olan ST (Internet Stream Protocol) olarak kullanılmış olmasıdır[18].

3.2.7. Yeni nesil IP’nin yenilikleri

IPv6 adres havuzu oldukça büyüktür. IPv6 alıcı ve verici arasında yüksek kalitede yol oluşturup paketleri bu yol üzerinden iletme imkânı sunar. Bu da daha kaliteli ve performanslı iletim isteyen ses ve görüntü iletimine altyapı hazırlar, ayrıca ucuz iletim imkânı da sağlar. IPv6 başlığı basitleştirilmiştir bu nedenle işlem süresi kısalmıştır. Başlık IPv4’e göre hemen hemen tamamen değiştirilmiş, bazı kısımlar ise yer değiştirmiştir. Ayrıca paketlerin türü başlık içerisinde ayrıştırılarak gerçek zaman trafiği ile anlık iletim istemeyen trafik için yönlendiricilerin farklı davranması hedeflenerek servis kalitesi arttırılmış oldu[31].

IPv6 temel başlığının yanında ek başlık kavramını ortaya çıkarmıştır. IPv4’ün aksine IPv6 bazı bilgileri ek başlık denen başlıklar içine kodlar. Bu ek başlıklar hiç kullanılmayacağı gibi birden fazla da kullanılabilir. Bir IP paketinde ek başlık var mı yok mu bu ana başlık ta belirtilmiştir ve kolayca işlenir. Ek başlıklar her zaman kullanılmak zorunda değildir. Ek başlık kullanıldığında IPv4’teki kadar etkin bilgiyi daha az paket boyutuyla sağlar. Ek başlıklar veri bütünlüğü ve sürekliliğini sağlamaları yanında, ağ saldırılarını da belirli oranda engeller. Böylece güvenlik IPv4'te seçenekken IPv6 güvenliği gereklilik yapmıştır. IPv6’da tasarımcılara ek başlıklarla tüm mümkün yolları kullanmayıp göndericiye kendi başlık formatını oluşturması imkânı sunulmuştur. Bu durum esneklik getirmesinin yanında ilerde ihtiyaç duyulan başka ek başlıkların oluşturulabilmesine de imkân tanır. IPv6 böylece gelişebilir olarak tasarlanmıştır[31].

IPv6 başlık 40 Byte IPv4 ise 20 ile 24 Byte arası değişen veri içerir. Ancak IPv4'te 12 alan, IPv6'da 8 alan bulunur; bu da bir paketin geçeceği yolda daha kısa sürede işlenmesi demektir. IPv6'da tekli-yayın ve çoklu-yayın adreslemeye ek olarak rastgele-yayın adresleme tipi oluşturuldu. Rastgele-yayın adresleme ile adreslenmiş bir datagram bir grup bilgisayar içinden herhangi birine gider. Aynı işi gören birkaç internet sitesi bilgisayarlarından bilgi almak isteyen bir bilgisayar birbirinin aynısı olan sunuculardan kendine en yakın olana veya en uygun durumda olana bağlanıp işini yapar. IPv6 ile "seçenekler" kısmı temel başlıktan çıkarılarak ek başlıklara konmuştur. Böylece daha esnek bir yapı sağlanmıştır ve gerektiğinde kullanılabilmesi amaçlanmıştır. Temel başlık ise 40 Byte yapılarak işlem hızı arttırılmıştır [31].

3.2.8. IPv6 adres türleri

IPv6 adres uzunluğunun 128 bit seçilmesinin amacı hiyerarşik yönlendirmeyi kolaylaştırmaktır. Cihazın ağ ara yüzüne atanan 128 bitin 64 biti alt ağ tanımlayıcısı (subnet identifier), diğer 64 biti de ara yüz tanımlayıcısıdır (interface identifier). IPv4'teki sınıflandırmaya benzer şekilde IPv6'da da üst seviye bitler IPv6 adres çeşitlerini belirtmektedir. Bu üst seviye bitlere aynı zamanda FP (format prefix) de denilmektedir. Bazı çok kullanılan adreslerin FP'leri aşağıdaki gibidir:

- Loopback adresi FP= 00…1 (128 bit)
- Global tekli-yayın adresinde FP= 001
- Link-local tekli-yayın adresinde FP= 1111 1110 10
- Site-local tekli-yayın adresinde FP= 1111 1110 11
- Çoklu-yayın adresinde FP= 1111 1111

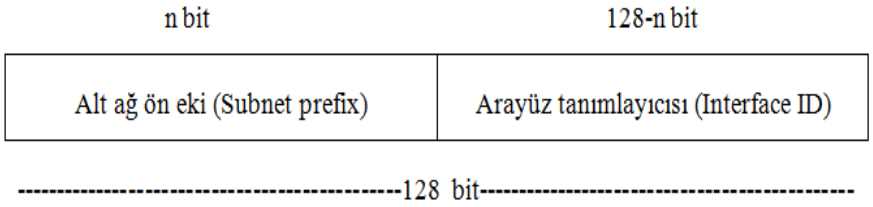
Yukarıda verilen FP (Format Prefix) örneklerinden de anlaşılabileceği gibi IPv6'da 3 temel adres çeşidi vardır. Bunlar:

- Tekli-yayın Adresi
- Çoklu-yayın Adresi
- Rastgele-yayın Adresi

IPv4'te bulunan broadcast adresi IPv6'da tamamen kaldırılmış bu görevi çoklu-yayın adresi yerine getirmektedir. Ayrıca yeni bir çeşit olan rastgele-yayın adresi getirilmiştir[16,18].

Tekli-yayın adresleri (Unicast Address)

IPv6 tekli-yayın adreslerinin yapısı, uzunluğu hariç CIDR'lı IPv4 adreslerinin yapısına çok benzemektedir. Çok çeşitli tekli-yayın adresleri vardır; global, site-local ve link-local bunlardan bazılarıdır. Ayrıca küresel tekli-yayın adreslerinin alt çeşitlerini oluşturan, kodlanmış NSAP ve IPv4 içeren IPv6 adresleri gibi özel amaçlı adresler de vardır. IPv6 kullanan cihazların bu adreslerin çeşitleri konusundaki bilgileri tamamen ağ içindeki sorumluluklarına göre değişmektedir. Basit bir son nokta cihazı sadece adres uzunluğu bilgisine sahip olup o adresin içyapısı hakkından hiç bilgi taşımayabilir. Biraz daha gelişmiş bir son kullanıcı cihazı alt ağ ön eki ve ara yüz tanımlayıcıları hakkında bilgi sahibi olmaktadır. Yönlendiriciler gibi ağ içinde önemli görevler üstlenen cihazlar ise bu adresleri çok daha iyi analiz edebilmelidirler[16,18].



Şekil 3.7. IPv6 adres bölünmesi

Şekil 3.7'deki açıklamaya göre ara yüz tanımlayıcıları kendisine atanan cihazı ağ üzerinde tanımlamakla görevlidirler. Benzersiz olmaları gerekmektedir ve aynı ağ içinde birden çok cihaza atanamazlar. Bazı durumlarda ara yüz tanımlayıcısı adresi cihazın ikinci katman fiziksel adresinden elde edilmektedir. tekli-yayın adreslerinin birçok çeşidi vardır. Bunlar; tanımlanmamış adres (unspecified address), Loopback adresi, global adres, link-local adresi, site-local adresi, IPv4 adresi içeren IPv6 adresleri, gizlilik ekleri (Privacy Extensions) ve uyumluluk (compatibility) adresleridir[16,18].

Tanımlanmamış tekli-yayın adresleri

Tüm bitleri sıfır olan adrese tanımlanmamış adres denilmektedir. Kısa gösterimi ile "::" seklinde yazılabildiği gibi 0000:0000:0000:0000:0000:0000:0000:0000 şeklinde de uzunca ifade edilebilmektedir. Bu adresin var olma amacı herhangi bir düğüme bir adresin atanmadığını ifade etmektir, hiçbir zaman bir son noktaya IP adresi olarak atanmamalıdır. Bu adresin kullanım alanlarından biri, henüz adres tanımlanmamış bir cihazın adresinin verilmesi sırasında o cihaza kaynak adresi olarak atanmaktır. Bu şekilde o cihazın bir adrese ihtiyacı olduğu belirtilmektedir ve cihazın IP yapılandırılması işlemi yerine getirilmektedir. Tanımlanmamış tekli-yayın adresleri asla IPv6 paketlerinin hedef adresi veya yönlendirme başlığı adresi olmamalıdır. Eğer kaynak adresi olarak kullanıyorsa da asla ağ içindeki yönlendirici tarafından ağ dışına gönderilmemelidir[16,18].

Loopback adresi

Sadece son biti 1 olan diğer bitleri 0 olan 0000:0000:0000:0000:0000:0000: 0000:0001 adresi loopback tekli-yayın adresidir. Kısaca ::1 şeklinde de gösterilir. Bu adres cihaz içinde sanal bir ara yüze atanarak cihazın kendi kendine IPv6 paketi göndermesini sağlamaktadır. Asla fiziksel ara yüzlere atanmaması gerekmektedir. Loopback adresi hiçbir zaman cihazın dışarıya gönderdiği IPv6 paketlerinin kaynak adresi olamamaktadır. Aynı şekilde hedef adresi loopback adresi olan bir IPv6 paketi ne cihazın dışında bir uç noktaya gönderilebilmekte ne de yönlendiriciler tarafından yönlendirilebilmektedir. Hedef adresi loopback adresi olarak atanmış, başka bir düğümden gelen bir paket kullanılmamakta ve hemen iptal edilmektedir [16,18].

Global adresler

Global tekli-yayın adresleri FP 001 değeri ile tanımlanmışlardır. İlk 16 bitlik dizi 2 veya 3 ile başlamaktadır. Bunun nedeni ilk 3 biti 001, bunu takip eden değer 0 veya 1 olabilmektedir. Eğer FP'yi takip eden değer 0 olursa IPv6 adresinin ilk rakamı 2, eğer 1 olursa adresin ilk rakamı 3 olmaktadır. IPv6 global tekli-yayın adresleri aynı IPv4 global tekli-yayın adresleri gibi, İnternet'ten herhangi bir yerden erişilebilir ve

yönlendiriciler tarafından kaynak adresi olarak kullanılan paketlerin hedef yerlere iletilmesini sağlayabilmektedirler. IETF RFC 1887 dokümanından global tekli-yayın adresleri ile ilgili daha detaylı bilgiye erişilebilmektedir[16,18].

Link-local adresleri

Link-local adresleri 10 bitlik "1111111010" bit dizisi ile başlamaktadır. Bu diziyi takip eden 54 bitlik bir 0 dizisi, sonra da ara yüz tanımlayıcısı gelmektedir. Bu sebeple bu tip adreslerin ilk 64 biti FE80:: ile ifade edilmektedir. Link-local adresler yerel alan ağı içinde kalmak üzere kullanılmakta anahtarlama cihazları tarafından hedeflere iletilmekte ancak asla yönlendiriciler tarafından dış dünyaya yönlendirilememektedir. Otomatik adres yapılandırması ve komşu keşfi gibi mekanizmalarda kullanılmaktadırlar [16,18].

Site-local adresleri

IPv6 site-local adresleri, IPv4'te kullanılan ve RFC 1597 ve 1918 ile tanımlanmış özel adreslerin yerini almak üzere tasarlanmıştır. IPv4 özel adresleri, alt ağ maskeleri ile birlikte 10.0.0.0/8, 172.16.0.0/12, 192.16.0.0/16 seklinde ifade edilmektedir. Site-local adreslerin tasarımı FP=1111111011 olacak şekilde yapılmıştır. FEC0:: şeklinde başlamaktadır. Bu adresler link-local adresler gibi otomatik olarak atanmazlar. Kullanıcı veya ağ tarafından ihtiyaç duyulması halinde yapılandırılırlar. Yapı bakımından global tekli-yayın adreslerine çok benzerler. Global adreslerle birlikte kullanılabilirler. Yapısı ile ilgili bilgiler RFC 3513'te belirtilmiştir. RFC 4219'da belirtildiği üzere bu adresler yeni uygulamalarda kullanılmayacak, ancak eski uygulamalar desteklemeye devam edebileceklerdir. Yeni uygulamalar bu ön ekli adresi global tekli-yayın adresi olarak algılayacaklardır[16,18].

IPv4 adresi içeren IPv6 adresleri

IPv4 adreslerini IPv6 adresinin en düşük anlamlı 32 bitinde taşıyan iki çeşit adres bulunmaktadır. Bunlar, IPv4 uyumlu (IPv4-compatible) adresler ve IPv4'le eşlenmiş (IPv4-mapped) adreslerdir. IPv4 uyumlu adresler 0:0:0:0:0:0:m.n.k.l veya ::m.n.k.l şeklinde ifade edilmektedir. Adreste bulunan m.n.k.l 32 bitlik IPv4 adresidir ve daha

anlamlı 96 bit “0” ile doldurularak 128 bitlik bir IPv6 adresi elde edilmektedir. Burada kullanılan IPv4 adresi global bir adres olmalıdır. Bu adres türü artık desteklenmemektedir çünkü mevcut IPv6 geçiş mekanizmalarının hiçbiri bu adresi kullanmamaktadır. Bu sebeple yeni uygulamalar veya güncellemeler bu adresi desteklemek zorunda değildir. IPv4’le eşlenmiş adresler 0:0:0:0:0:FFFF:m.n.k.l veya ::FFFF:m.n.k.l seklinde ifade edilmektedir. Bu adres türü IPv4 düğümlerini IPv6 adresleri olarak tanımlayabilmek için kullanılmaktadır. En büyük avantajı bu adres çeşidini kullanan programlar tek adres alarak hem IPv4 hem IPv6 adresini elde etmiş olurlar. Bu adres türünde son 32 bit ile ifade edilen IPv4 adresi onluk sayı düzeninde yazıldığı gibi istenirse onaltılık sayı düzeninde de yazılabilmektedir. RFC 4038 bu adresi türünün kullanımı hakkında detaylı bilgi vermektedir[16,18].

Rastgele-yayın adresleri (Anycast Address)

Rastgele-yayın adresleri IPv4’te bulunmayan ve IPv6 için geliştirilen bir adres çeşididir. Kendisine ait bir FP’si bulunmamaktadır. Aslında yapısal olarak bir tekli-yayın adresinin tamamen aynısıdır, ancak kullanım alanı farklıdır. Bir rastgele-yayın adresi bir tekli-yayın adresinin birden çok düğüme verilmesi ile oluşmaktadır. Bu düğümlere atanan adresin rastgele-yayın adresi olduğunu belirtmek gerekmektedir çünkü yapısal olarak bu adresleri tekli-yayın adresinden ayırmak mümkün değildir. Bir grup ağ cihazına verilen rastgele-yayın adresi o gruptaki cihazların herhangi birine ulaşmak için kullanılır. Yani tekli-yayın’daki gibi birebir haberleşme veya çoklu-yayın’daki gibi grubun tamamı ile haberleşme yapılmamaktadır. Rastgele-yayın adresleri ile ilgili doğabilecek bazı sorunları engellemek için RFC 1884 ile bu adreslere bazı sınırlamalar getirilmiştir.

- Rastgele-yayın adresleri IPv6 paketlerinin kaynak adresi olarak kullanılmamalı
- Rastgele-yayın adresleri son noktalara atanmamalıdır. Bu da bu adreslerin IPv6 yönlendiricilerine atanabileceği anlamına geliyor.

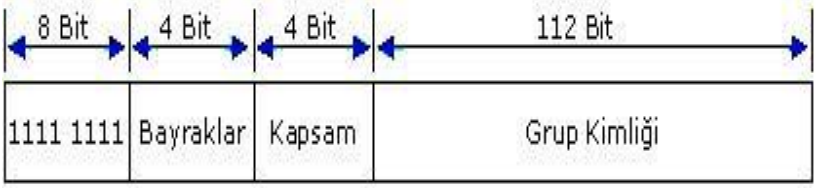
Bu adreslerin kullanım alanına yönelik bir örnek, bir firmanın yönlendirme işlevini yerine getiren cihazlara rastgele-yayın adresleri atanması olabilir. Bu yönlendiriciler firmanın internet bağlantısını sağlıyor olsunlar. Herhangi bir son nokta aynı rastgele-yayın adresi kullanan bu yönlendiricilerden herhangi birini kullanarak İnternet'e çıkabiliyor olacaktır. Bu sayede her bir yönlendiricinin adresini tek tek bilmesi gerekmeyecektir. Henüz çok fazla kullanım alanı bulamış olmalarına rağmen, IPv6 konusunda ağ tecrübeleri arttıkça rastgele-yayın adresleri de TCP/IP yapısı içindeki yerini alacaktır [16,18].

Çoklu-yayın adresleri (Multicast address)

IPv6'da çok noktaya yayın trafiği IPv4'teki ile aynı şekilde işler. Rastgele konumlandırılan IPv6 düğümleri, rastgele IPv6 çok noktaya yayın adresleri üzerindeki çok noktaya yayın trafiğini dinleyebilir. IPv6 düğümleri birden fazla çok noktaya yayın adresini aynı anda dinleyebilir. Düğümler çok noktaya yayın grubuna herhangi bir zamanda katılabilir veya gruptan çıkabilir.

IPv6 çok noktaya yayın adreslerinde ilk 8 bit 1111 1111 olarak ayarlanır. Bunlar her zaman "FF" ile başladığından bir IPv6 adresinin çok noktaya yayın olup olmadığını anlamak kolaydır. Çok noktaya yayın adresleri bir Yönlendirme başlığında kaynak adres veya ara hedef olarak kullanılamaz.

İlk 8 bitin sonrasında, çok noktaya yayın adresleri bayraklarını, kapsamlarını ve çok noktaya yayın grubunu tanımlayan ek yapı içerir. IPv6 çok noktaya yayın adresinin yapısı Şekil 3.8 'da gösterilmiştir.



Şekil 3.8. çoklu yayın adres yapısı

Bayraklar

Çok noktaya yayın adresinde ayarlanan bayrakları gösterir. Bu alan 4 bit uzunluğundadır. RFC 3513'ten itibaren tanımlanan tek bayrak Geçici (T) bayrağıdır. T bayrağı Bayrak alanının alt kısmındaki bitini kullanır. T bayrağının 0 olarak ayarlanması, çok noktaya yayın adresinin Internet Assigned Numbers Authority (IANA) tarafından kalıcı olarak atanmış, iyi bilinen bir çok noktaya yayın adresi olduğunu gösterir. T bayrağının 1 olarak ayarlanması, çok noktaya yayın adresinin IANA tarafından kalıcı olarak atanmamış, geçici bir çok noktaya yayın adresi olduğunu gösterir.

Kapsam

Çok noktaya yayın trafiği için kullanılan IPv6 ağının kapsamını gösterir. Bu alan 4 bit uzunluğundadır. Çok noktaya yayın yönlendirme protokolleri tarafından sağlanan bilgilere ek olarak, yönlendiriciler çok noktaya yayın kapsamını, çok noktaya yayın trafiğini iletip iletmeyeceklerini belirlemek için kullanır. Kapsam alanında en sık kullanılan değerler 1 (yerel arabirim kapsamı), 2 (yerel bağlantı kapsamı) ve 5'tir (yerel site kapsamı).

Örneğin, FF02::2 çok noktaya yayın adresi olan trafik yerel bağlantı kapsamına sahiptir. IPv6 yönlendiricisi bu trafiği hiçbir zaman yerel bağlantının dışına iletmez.

Grup Kimliği

Çok noktaya yayın grubunu tanımlar ve kapsam içinde benzersizdir. Bu alan 112 bit uzunluğundadır. Kalıcı olarak atanan grup kimlikleri kapsamdan bağımsızdır. Geçici grup kimlikleri yalnızca belirli bir kapsamla ilgilidir. FF01:: ile FF0F:: arasındaki çok noktaya yayın adresleri ayrılmış, iyi bilinen adreslerdir[16,18].

3.2.9. IPv6 düğümünün sahip olması gereken adresler

IPv6 adresleme yapısını iyi anlayabilmek için, bir IPv6 düğümünde hangi çeşit adreslerin bulunması gerektiğini bilmek gerekmektedir. IPv4 adresleme yapısında

düğüme tek bir IPv4 adresi atanmakta ve ağ ile ilgili tüm isler bu adres ile sağlanmaktaydı. IPv6'da ise düğüm kendisini tanımlayabilmesi için aşağıdaki adreslere ihtiyaç duymaktadır:

- Her ağ ara yüzü için bir adet link-local adresi.
- Herhangi anycast veya unicast, adres veya adresleri (bir ara yüze birden fazla unicast adres atanabilmektedir.)
- Her bir düğüm için bir adet loopback adresi
- Bir adet tüm düğümleri belirten multicast adresi (IPv4'teki karşılığı broadcast adresidir.)
- Kendisinin de üye olduğu multicast gruplarının adresleri.

Yönlendiriciler bir düğümde bulunması gereken tüm adresleri algılayabilmekte ve ayrıca ek olarak aşağıdaki adreslere ihtiyaç duymaktadırlar:

- Yönlendirici olarak davranacak tüm ara yüzlerine atanacak alt ağ yönlendirici unicast adresleri
- Yönlendiricinin yapılandırıldığı tüm diğer anycast adresleri
- Tüm yönlendiricileri belirten multicast adresi
- Tüm düğümleri belirten multicast adresi[16,18].

3.3. EUI Arayüz Tanımlayıcısı

IPv6 adres çeşitleri incelendiğinde site-local, link-local ve global adres gibi unicast adreslerin birçoğunda 64 bitlik bir ara yüz tanımlayıcısı bölümü, bir de ön ek bölümü vardır. Bu 64 bitlik ara yüz tanımlayıcısı ağ içinde adresin atandığı ara yüze özel bir bilgidir ve adres atanan ara yüzleri birbirinden ayırmaya yarayan benzersiz bir değerdir. Bu bölüm değişik şekillerde oluşturulabilir. Sunuculu (stateful) ve sunucusuz (stateless) adres atamalarındaki gibi rastgele veya belli bir aralıkta atanabildiği gibi MAC adresine göre oluşturulan ara yüz tanımlayıcıları da bulunmaktadır. IEEE, 64 bit uzunluğunda EUI-64 ismi verilen yeni bir fiziksel adres(MAC) çeşidi geliştirmiştir. Şu anda kullanılan MAC adresleri 48 bit

uzunluğundadır ve 24 biti IEEE tarafından atanan kuruluşa özel ve OUI (Organization Unique Identifier) diye adlandırılan bir değer, diğer 24 bit kuruluş tarafından atanan kendi ürünlerini ayırmaya yarayan değerdir. IEEE'nin yeni geliştirilen MAC adresine göre kuruluş 24 bitlik adresi IEEE'den aldıktan sonra kendisine özel değeri 40 bit olarak verebilmekte ve böylelikle EUI-64 standardını destekleyebilmektedir; Ayrıca EUI-64 adresi eski 48 bitlik adreslerin belli kurallara göre genişletilmesi ile de oluşturulabilmektedir. Bu konuda çeşitli kurallar bulunmaktadır, Düğümler için kullanılan EUI-64 adresleri için MAC adresi içindeki 7. bit adresin evrensel olarak geçerli mi yoksa yerel olarak mı oluşturulduğuna göre 0 veya 1 değerini alır. 48 bitlik adres içindeki 24 bitlik iki bölüm birbirinden ayrılıp araya onaltılık sayı düzeninde FFFE değeri eklenmektedir. Bu şekilde yeni adresi 64 bitlik EUI-64 adresi halinde gelmektedir. Örnek olarak MAC adresi 0012:F0E0:B6F5 olan bir cihazın EUI-64 adresi 0212:F0EF:FFE0:B6F5 olmaktadır. Site-local adresleri otomatik olarak bu değere göre oluşturulmaktadır[23].

3.4. Dünyada IPv6

IPv4'tten IPv6'ya geçiş çalışmaları dünyada birçok ülkede başlamıştır. Bu konuyla ilgili birçok ülkede forumlar düzenlenmiştir. Bu çalışmalar 1990'lı yıllardan beri başlamıştır. Bu forumlar ve çalışmalar IPv4'ün eksikleri ve sorunlarının giderilmesi amacında yapılmıştır. Dünyada yapılan bir çok çalışmalarda şimdi mevcut kullanılmakta olan IPv4 sıkıntısız ve kesintisiz bir şekilde nasıl kullanılır ve yeni nesil IP'yi elastik bir şekilde nasıl hizmete geçirilir. Bu çalışmalardan Avrupa'da 2001 yılında IPv6 görev gücü grubu kurulmuştur. Bu grubun görevi IPv6'nın yaygınlaştırılması üzerine çalışmalar yürütmektedir. Avrupa görev gücünün projelerinden U 2010 projesidir, bu proje ile IPv6'yı acil durumlarda devreye sokarak iletişimi sağlayan bir projedir. Japonya'ya bakıldığında IPv6 çalışmalarında en önde gelen ülkelerindedir. IPv6 forumları ve projeleri diğer ülkelere göre çok fazladır. U-japan projesi ile Japonya'yı dünya çapında bilgi teknolojisi açısından en gelişmiş ülke haline gelmesi hedeflemektedir. Japonya'nın hedefi sadece IPv6'ya sorunsuz bir geçiş sağlamak değil ama Japonya IPv6 alanında yönetici haline gelmesidir, çünkü Japonya

IPv4 teknolojisinde ABD'nin gerisinde kalmıştır dolayısıyla IPv6'da ABD'nin önüne geçme çapası vermektedir. Güney Kore'de diğer ülkeler gibi IPv6 çalışmaları için ciddi çabalar sarf etmektedir. Kore hükümeti IPv6 çalışmaları için yaklaşık 90 milyar Euro bir bütçe ayırmıştır. Çin IPv6 araştırmaları için yaklaşık 170 milyon Amerikan doları ayırmıştır 2002 yılında. Hindistan'da IPv6'ya geçiş için 2005 yılında TRAI çalışmaları kapsamında bir bildiri yayınlamıştır[19].

3.5. Türkiye'de IPv6

Türkiye'de 2010 yılında IPv6 geçişi için kamu kurumları ve kuruluşları " Kamu Kurum ve Kuruluşları için IPv6'ya Geçiş Planı" T.C Başbakanlık genelgesi doğrultusundan çalışmalarını yürütmektedir. IPv6 çalışmaları ile ilgili TÜBİTAK, ULAKBİM ve Gazi Üniversitesi'nin katılımıyla 2011 yılında birincisi ve 2012 yılında ikincisi düzenlenen " IPv6'ya geçiş ve sonrası" konferansında IPv6'ya geçişte sürecinde karşılaşılacak problemlere çözüm aramak ve yeni durumlar hakkında fikir alışverişinde bulunmak ve araştırma çalışmalarını paylaşmak ve tartışmak amacında katkı sağlamıştır. Türkiye'de IPv6 çalışmaları 2003 yılından beri TÜBİTAK tarafından yapılmaktadır. Başta IPv6 Forum kuruluşuyla ulusal ve ulusal arası çalışmalar ve etkinlikler yapılmaktadır. Bu konuyla ilgili yapılan çalışmalar önemli somut sonuçlar vermiştir ve Türkiye Cumhuriyeti için IPv6 yayması için yol haritası çizme konusunda çok etkin rol oynamıştır. Gazi Üniversitesi, Çanakkale 18 Mart Üniversitesi ve birçok Üniversite'de IPv6 konferanslarının ve araştırmalarının yapılması ülkemiz açısından gurur vericidir [19].

3.6. IPv6 ile IPv4'ün Yapısında Yapılan Temel Değişiklikler

IPv6 128 bit adresleme ile IPv4'e göre 2 üzeri 96 kat daha fazla adresleme aralığı sağlamayı hedeflemiştir. Bu adresleme ile yer yüzeyinde metrekareye 6x 10^{23} adet tekil IP düşmesini sağlanmıştır. En verimsiz kullanımla bile bu kadar adres uzun müddet bitirilemez. IPv4'te başlık içinde bulunan seçenekler kısmı IPv6'da çıkarılarak gerektiğinde kullanılan bir ek başlık olarak tanımlanmıştır, bu durum işlem hızını düşürdüğünden daha hızlı bir protokol oluşturulur. IPv6 oto yapılandırma yoluyla dinamik adreslemeye imkân tanımaktadır. Rastgele-yayın adres

tipi ilk kez kullanılmış ve bir paket aynı rastgele-yayın IP adresine sahip bir grup bilgisayardan gönderenin durumuna göre en uygun bilgisayara yollanır. Çoklu-yayın yönlendirme ise tarama alanı eklenerek geliştirilir. IPv6'da pakete konulan etiketle göndericiye özel veya trafik tipine özel tasıma imkânı sağlanır (canlı video yayını öncelikli tasıma gibi). Hata kontrol protokolü ICMP IPv6'ya uygun güncellenerek ICMPv6 şeklinde tasarlanır. IPv4 ve IPv6 karşılaştırması Çizelge 3.3 ve Çizelge 3.4'te gösterilmiştir[24].

Çizelge 3.3. Ipv4, Ipv6 karşılaştırması [24]

Özellik	**IPv4**	**IPv6**
Adres Uzunluğu	32 bits	128 bits
Parçalama	Bilgisayarlar ve yönlendiriciler	Bilgisayarlar
Öncelik teslim desteği	Var	Geliştirildi/ Arttıldı
IPsec başlığı desteği	İsteğe bağlı	Zorunlu
2. Katman adres çözülmesi	ARP (Broadcast)	Komşu keşfi (ND-Çoklu-Yayın)
Çoklu-Yayın üyeliği	IGMP	Çoklu-Yayın Dinleyici Keşfi (MLD)
Yönlendirici keşfi	İsteğe Bağlı	Zorunlu (ICMPv6)
Broadcast mesajları	Evet	Hayır
Adres yapılandırması	Elle, DHCP	Otomatik, DHCPv6
DNS isim kaydı	(A) Kayıtları	(AAAA) Kayıtları

Çizelge 3.4. IPv4 ile IPv6 adres karşılaştırması [24]

IPv4	**IPv6**
Genel Adresler (Public)	Genel Adresler (Global)
APIPA Adresleri (169.254.0.0/16)	Yerel Bağlantı Adresleri (FE80::/8)
Genel Yayın Adresleri (Broadcast)	Kaldırıldı
-	Her Noktaya Yayın Adresleri (Rastgele-Yayın)
Özel Adresler (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)	Yerel Site Adresleri – RFC3579 kaldırıldı.
Loopback Adresi (127.0.0.1)	Loopback Adresi (::1)
Belirsiz Adres (0.0.0.0)	Belirsiz Adres (::)

3.7. IPv4'ten IPv6'ya Geçiş Süreci

IPv6'ya geçiş sürüyor ve sürecektir. Geçişte en temel etken, IPv4 adreslerin tamamen bitmesidir. IPv4'ü tasarruflu ve etkin kullandıran DHCP ve NAT gibi buluşlar geçişi yavaşlatmıştır. Bazı telefon firmalarının IP tabanlı cep telefonu üretmesi geçişe hız kazandırdı. Linux ve Windows işletim sistemlerinin IPv6'yı desteklemeye başlamasına karşın tamamen IPv6'ya geçiş sürmektedir. 1995 yılında yapılan tahminlere göre tamamen geçişin 15 sene süreceği belirtiliyordu. Geçişi yavaşlatan en önemli etkenlerden biri ise IP'nin bulunduğu katman itibariyle önemli bir yerde olmasıdır. Uygulama katmanındaki değişimler hemen hayata geçerken ağ katmanındaki bu değişim hemen uygulanamamaktadır. Bu bir binanın temel kolonu ve boyası yaklaşımı gibidir. IP temel kolon, uygulamalar ise boya gibidir. 1999 yılı başında 40 milyon olan internete bağlı cihaz sayısı 2004 yılı başında 200 milyona ulaşmıştır. Bu artış oranı ve internet servis sağlayıcılardaki gelişmeler beraber düşünüldüğünde 2012 yılı başındaki değerin bir milyarı aştığı belirtilmektedir[2].

3.8. Bilgisayar ve Ağ Sistem Geliştiricilerin IPv6 Destekleme Durumu

IPv6'nın standartlaştırma işlemleri bitmek üzeredir. Günümüzde cihaz üreticiler ve yazılım geliştiriciler kendi işletim sistemlerini ve ağla ilgili cihazlarını IPv6 destekler duruma getirmek için çalışmaktadırlar. Çizelge 3.5 ve Çizelge 3.6, üreticilerin IPv6 açısından son durumlarını göstermektedir [23].

Çizelge 3.5. Ticari yönlendiricilerin IPv6 destekleme durumu[23].

Yönlendirici Üreticisi	**IPv6'yı destekleme durumu**
JUNIPER	2001'den sonra destekliyor
CISCO	2003'ten beri destekliyor
NOKIA IP	2002'den sonra destekliyor
HITACHI	1997'den sonra destekliyor

Çizelge 3.6. İşletim Sistemlerinin IPv6 destekleme durumu [23].

İşletim Sistemi	**Destekleme Durumu**
MICROSOFT	Windows 2003'ten beri destekliyor
LINUX	2.4.X sürümünden sonraki kernel'ler destekliyor
MAC OS	Sürüm 10.2 sonrasını destekliyor
FREE BSD	Sürüm 4.0 sonrasını destekliyor
NET BSD	Sürüm 1.5 sonrasını destekliyor
OPENBSD	2.7 sürümden sonrasını destekliyor
BSD/OS	4.2 sürümden sonrasını destekliyor
SUN	Solaris 8'den sonrasını destekliyor

3.9. IPv6 'ya Geçiş için Geliştirilmiş Mevcut Teknikler

IPv6'ya üç temel geçiş yöntemi bulunmaktadır. Bu mekanizmalar:

- İkili Yığın geçiş yöntemi[22].
- Tünelleme geçiş yöntemi
  - Elle tünelleme yöntemleri
    - MCT
    - GRE
  - Otomatik tünelleme yöntemleri
    - 4 üzerinden 6
    - 6to4
    - ISATAP
    - Tunnel Broker
    - Teredo
- Çeviri geçiş yöntemi
    - Durumsuz IP/ICMP Çevirici
    - Bindirme Yöntemli Yığın
    - Bindirme Yöntemli Uygulama Ara yüzü
    - Ağ Adres Çevirisi Protokol Geçişi
    - Çoklu Dağıtım Transfer Protokolü
    - Transfer Gönderi Çevirici
    - Soket Tabanlı IPv6/IPv4 Çevirici

Bu yaklaşımlar üzerinde internet otoritelerince kabul gören çeşitli standartlar oluşmuştur. Bu standartlar Çizelge 3.7' de görülmektedir[26].

Çizelge 3.7. IPv4-IPv6 arası geçiş yöntemleri

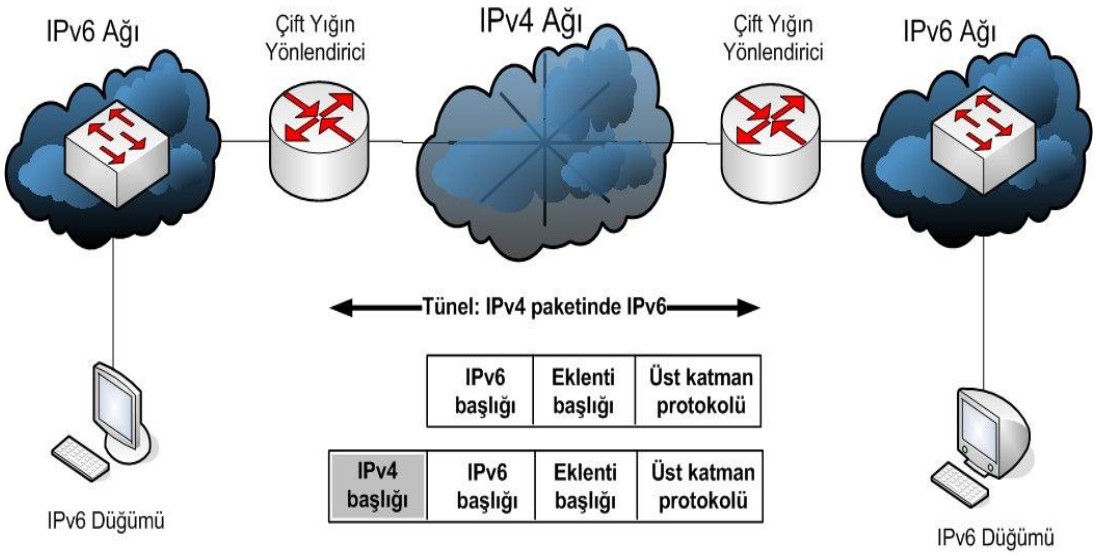
İsim	**Bağlantı**	**Tip**	**Lokasyon**
İkili Yığın	4 üzerinden 4den4e, 4 üzerinden 6dan6ya	İkili Yığın	Tek IPv4 veya IPv6 adresi veya Komşu Saptama İletişim Kuralı
Durumsuz IP/ICMP Çevirici	6dan4e, 4den6ya	Çevirici	Tek IPv4 veya IPv6 adresi veya Komşu Saptama İletişim Kuralı
Bindirme Yöntemli Yığın	4den6ya	Çevirici	Tek IPv4 veya IPv6 adresi
Bindirme Yöntemli Uygulama Ara yüzü	4den6ya	Çevirici	Tek IPv4 veya IPv6 adresi
Ağ Adres Çevirisi-Protokol Geçişi	6dan4e, 4den6ya	Çevirici	Tek Komşu Saptama İletişim Kuralı
Çoklu Dağıtım Transfer Protokolü	4den6ya, 4den6ya(çoklu dağıtım)	Çevirici	Tek Komşu Saptama İletişim Kuralı
Transfer Gönderi Çevirici	6dan4e	Çevirici	Tek Komşu Saptama İletişim Kuralı

Çizelge 3.7. IPv4-IPv6 arası geçiş yöntemleri (Devam)

İsim	**Bağlantı**	**Tip**	**Lokasyon**
Transfer Gönderi Çevirici	6dan4e	Çevirici	Tek Komşu Saptama İletişim Kuralı
Soket Tabanlı IPv6/IPv4 Çevirici	4den6ya, 4den6ya	Çevirici	IPv4 veya IPv6 adresi ile Komşu Saptama İletişim Kuralı Arasında
4 üzerinden 6	4 üzerinden 6dan6ya	Tünelleme	IPv4 veya IPv6 adresi ile Komşu Saptama İletişim Kuralı Arasında
IPv6 Site İçi Otomatik Tünel Adres Protokolü (ISATAP)	4 üzerinden 6dan6ya	Tünelleme	IPv4 veya IPv6 adresi ile Komşu Saptama İletişim Kuralı Arasında
İkili Yığın Geçiş Yöntemi	6 üzerinden 4den4e	Tünelleme	IPv4 veya IPv6 adresi ile Komşu Saptama İletişim Kuralı Arasında
6dan4e	4 üzerinden 6dan6ya	Tünelleme	İki Komşu Saptama İletişim Kuralı Arasında

Tez konusu ile ilişkin otomatik tünelleme yöntemlerinden 6to4 ve ISATAP yöntemleri aşağıda detaylı bir şekilde incelenmiştir.

3.9.1. 6to4 tünelleme yöntemi



Şekil 3.9. 6to4 tünel yaklaşımı.

6to4 dinamik tünelleme yönteminde tekli noktadan çoklu noktaya paket gönderme prensibi ile çalışmaktadır, yani 6to4 tünellerinde tünelin hedefi belirlenmemektedir. Bunun yerine önceden yapılandırılmış tunnel X olarak gösterilir. Otomatik 6to4 yöntemi (Şekil 3.9) için RFC 3056 IPv6 rezerve edilen adres aralığından 2002::/16 tanıtmıştır, bu adres aralığı ne kadar IPv6 global tekil-yayın adres (2000::/3) gibi görünse bile IANA kurumu 2002::/16 ön ek 'ini 6to4 otomatik tünelleme yöntemine rezerve etmiştir ve kesinlikle global tekil-yayın adres olarak tanıtmamıştır.

6to4 tünel yapılandırmasında 2002::/16 önek'ine tünel uçuna ve tünel sonunda bulunan IPv4 adreslerini 6to4 adresine yani 2002::/16 ön ek 'inin 2. ve 3. oktetlerine entegre etmektedir. 6to4 adres yapısı Çizelge 3.8'de gösterilmiştir[23].

Çizelge 3.8. 6to4 tünelleme yönteminin IPv6 adresi

2002 : AABB : CCDD : Subnet : : /64
Ön ek 4 Oktet IPv4 Adresi

3.9.2. ISATAP tünelleme yöntemi

ISATAP tünelleme yaklaşımı 6to4 yöntemi ile benzer tarafları çoktur ancak bunun yanında da farklılıkları da vardır. Aynen 6to4 yaklaşımındaki olduğu gibi ISATAP yaklaşımı da IPv6 uç noktaların, IPv4 ağı üzerinden haberleşmeyi sağlayan bir tünelleme yöntemidir. ISATAP adreslerinin içerisinde aynı 6to4 ve 6over4'teki gibi IPv4 adresleri bu adreslerin içine entegre edilmektedir, ancak bu mekanizmada IPv4 adresini ikinci ve üçüncü oktete değil; son iki oktete yani 7. Ve 8. Oktete entegre edilecektir ve tabii ki onaltılık haline dönüştürüldükten sonra entegre edilmektedir. ISATAP adresleri elle yazılması yanında yönlendirici tarafından da otomatik bir şekilde EUİ-64 komutunu kullanarak da yazılmaktadır. ISATAP adresleri 64 bitlik ön ek ve 64 bitlik arayüz tanımlayıcısından oluşmakta ve ::5EFE:m.n.k.l seklinde ifade edilmektedir. ISATAP arayüz tanımlayıcısı 64 bitlik herhangi bir IPv6 ön eki birleştirilebilmektedir. Link local ISATAP adresine bir örnek olarak FE80::5EFE:160.75.67.200 verilebilmektedir. IPv6 desteği sunan Microsoft işletim sistemlerinde (Windows XP, Vista ve 7) link-local ISATAP adresi otomatik olarak yapılandırılmaktadır. IPv4 bir ağ içerisinde ISATAP yapılandırılması yapılan iki bilgisayar aralarında IPv6 haberleşebilmektedirler. Bir ağda IPv4 adresleri 160.75.67.20 ve 160.75.67.21 olan iki bilgisayar olsun ve bunlar ISATAP adresi ile yapılandırılmış olsunlar. ISATAP link-local adresleri FE80::5EFE:160.75.67.20 ve FE80::5EFE:160.75.67.21 olmaktadır. Bu arayüzleri kullanarak birbirlerine IPv6 paketi gönderebilmektedirler.

IPv6 otomatik tünelleme sadece İkili Yığın çalışan iki bilgisayar arasında haberleşmeyi sağlamaktadır. Günümüzde yerini ISATAP'e devretmiştir. 4 üzerinden 6 tünelleme tekniğinin en büyük özelliği ise diğer tekniklerde olmayan IPv6 çoklu-yayın trafiği desteğidir. Ancak bu desteğin paralelinde protokol IPv4 çoklu-yayın desteğinde ihtiyaç duyduğu için çok popüler değildir. Bunu yerine de ISATAP tercih edilmektedir[23].

4. DİNAMİK TÜNELLEME YÖNTEMLERİNİN BAŞARIM ÖLÇÜMÜ VE BENZETİM AĞINDA IPv4 VE IPv6 İLE KARŞILAŞTIRMASI

Ağ performans değerlendirmesinde kullanılan benzetim programları ve hesaplanacak metrikler sırası ile açıklanmıştır.

4.1. GNS3

GNS3 bir ağ Benzetim programıdır, büyük ve karışık ağların benzetimini yapma kabiliyetine sahiptir. GNS3 birçok programa uyumlu çalışabilir, bunlar Dynamips, Dynagen, Qemu, VertualBox. Tamamen gerçekteki gibi ağları benzetimini yapabilmesinden dolayı GNS3 birçok kurum tarafından kullanılmaktadır. Bunlar Cisco ve Juniper başta gelmek üzere GNS3, Cisco IOS'i olsun Juniper JunOS'i olsun, yönlendirici özelliklerine tamamen sahiptir. Program her türlü işletim sisteminde çalışmaktadır[27].

4.2. Oracle Virtualbox

VirtualBox tüm dünyada tercih edilen bir yazılım. Bu program ile birlikte adeta bir uygulama cihaza kurulur gibi işletim sistemlerinizi kurulmasına olanak sağlamaktadır. Bu işletim sistemlerini hiçbir zorluk çekmeden kolayca aynı anda tek bir cihaz üzerinde denemenize olanak sağlamaktadır. Fakat VirtualBox'un temel amacı Masaüstü sanallaştırmada ücretsiz bir çözüm üretebilmektir. Bu program işletim sistemi bağımlı, fakat işletim sisteminin ne olduğu çok da önemli değildir. Windows, MacOS X, Linux ve Solaris üzerinde çalışır. VirtualBox'un birlikte çalışabildiği en önemli ve iyi programlardan birisi GNS3 emulatörüdür[28].

4.3. Iperf ve Jperf

Iperf, birçok parametre hesaplamak kabiliyetine sahip bir paket trafiği üreticisidir. Iperf, verim, bant genişliği, gecikme ve jitter gibi metrikleri hesaplayabilmektedir. Her işletim sisteminde kolay kurulur ve net sonuçlar verdiği için kısa zamanda çok bilgisayar uzmanı tarafından kullanılmaktadır. Jperf, Iperf programının Java ara

yüzlü programıdır, Jperf sayesinde sonuçlar grafiksel bir şekilde gösterilmektedir. Tezde Iperf 2.0.2 sürümü ve Jperf 2.0.5 sürümleri kullanılmaktadır[29].

4.4. Performans Metrikleri

IPv6 geçiş performansını değerlendirmek için üç metrik hesaplanmıştır, bunlar: Ağ verimliliği, jitter ve kayıp paket oranı.

4.4.1. Verim (Throuput)

Ağ verimliliği belli bir iletişim kanalı üzerinden başarılı şekilde eletilen paketlerin ortalamasıdır. Verim çoğu zaman (Bits/s) bazen de saniyede paket adedi (Paket/s) olarak hesaplanmaktadır. Verimlilik metriği, çalışmamızda Kbits/s olarak hesaplanmıştır. Metrik Jperf yazılımı kullanarak hesaplanmıştır ve sonuçların eğilimi grafiksel olarak gösterilmiştir[26].

4.4.2. Gecikme varyasyonu (Jitter)

Jitter, Paketlerin gecikme sürelerindeki değişimidir (farklılık). Paketlerin kaynak ile hedef arasındaki iletimi esnasında geçen süreler arası farklılığı ifade etmektedir. Jitter metriği Jperf programında UDP protokolü kullanıldığında hesaplamaktadır[26].

4.4.3. Kayıp paket oranı (Packet Loss)

Belli iletişim aracı üzerinden gönderilen paketlerin tümü hedef düğüme yetişemez ve yolda kaybolmaktadır. Çalışmada kayıp paket oranını Jperf yazılımı ile UDP veri iletim protokolünü kullanıldığında hesaplanmıştır[26].

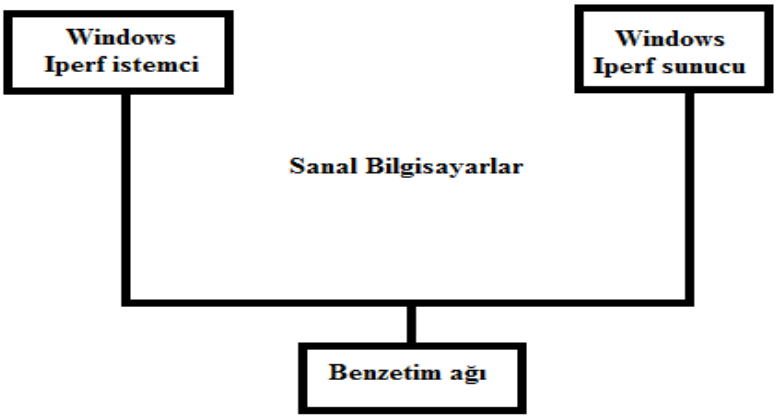
4.5. Deney Kurulumu

Denemelerde kullanılan donanımlar Çizelge 4.1'de gösterilmektedir:

Çizelge 4.1. Benzetim ağında kullanılan donanımlar.

Donanım	**Miktar**
Cisco 7200 yönlendiricisi	3 (IOS 12.4)
Windows 7	2

Benzetim laboratuvarında 3 Cisco 7200 yönlendiricisi birbirileri ile seri kablo ile bağlanmaktadır. Kenar yönlendirici 1 ve 3 'e bir adet bilgisayar ethernet kablosu ile bağlanmaktadır. Laboratuvar sanal bir şekilde tek fiziksel bilgisayar üzerinde çalıştırılmıştır. Sanal bilgisayarların ağ kartları, ağ benzetim programı GNS3 programına adapte edilmiştir. Benzetim ağların çalışma prensibini Şekil 4.1 gösterilmiştir.



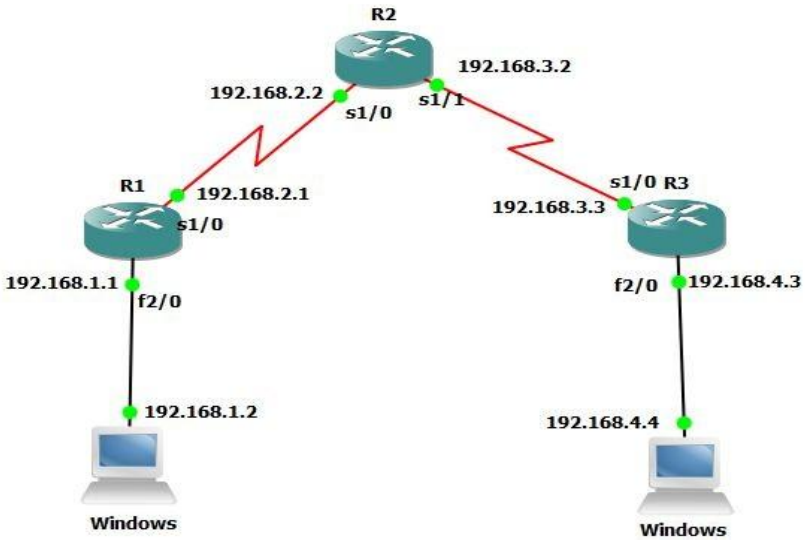
Şekil 4.1. Benzetim ağının iletişim şekli

Ağ benzetim programlarının daha iyi çalışması için TCP veri iletim protokolü kullanıldığında arabellek uzunluğunu (Buffer Length) 2 KBytes olarak yapılandırılmıştır. UDP veri iletim protokolü kullanımında bant genişliğini 128 KBytes/s olarak yapılandırılmıştır. Denemelerde 4 farklı ağın performansı ölçülmektedir bunlar:

1. IPv4
2. IPv6
3. Otomatik Tünelleme
    a. 6to4
    b. ISATAP

4.5.1. IPv4

IPv6 ve IP adresleme şeması Şekil 4.2'de gösterilmiştir:

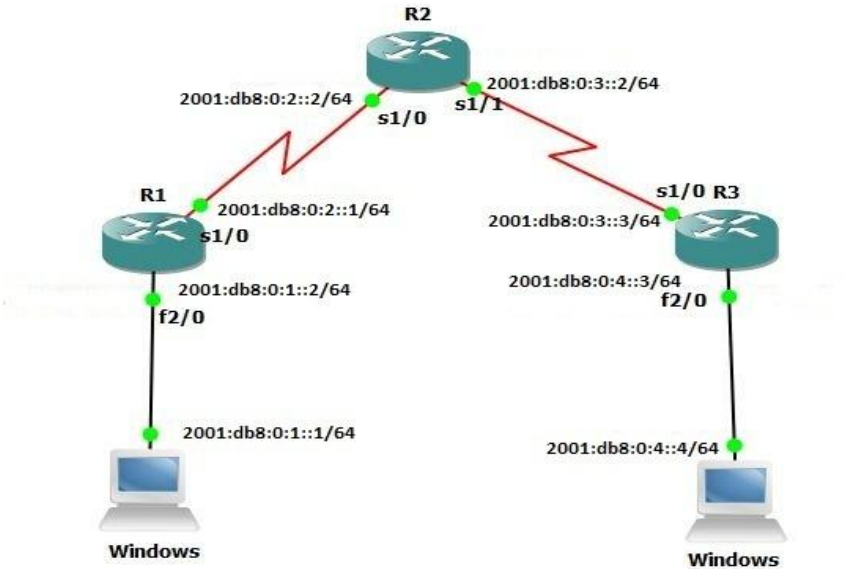


Şekil 4.2. IPv4 ağ ve adres şeması

Bu senaryoda bütün yönlendiriciler ve bilgisayarlar özel IPv4 adresleri ile yapılandırılmıştır. Yönlendirme protokolü olarak OSPF yönlendirme protokolü kullanılmıştır. Senaryo düzenli bir şekilde çalışmış ve Ping komutu ile test edilmiştir. Her iki sanal bilgisayarda Jperf programı çalışmıştır, ağın bir ucu Jperf (alıcı) diğer ucu ise Jperf (sunucu) senaryonun yönlendirici yapılandırma çıktısı eklerde bulunmaktadır.

4.5.2. IPv6

IPv4 ağ şeması ve IP adresleme şeması Şekil 4.3'de gösterilmiştir.



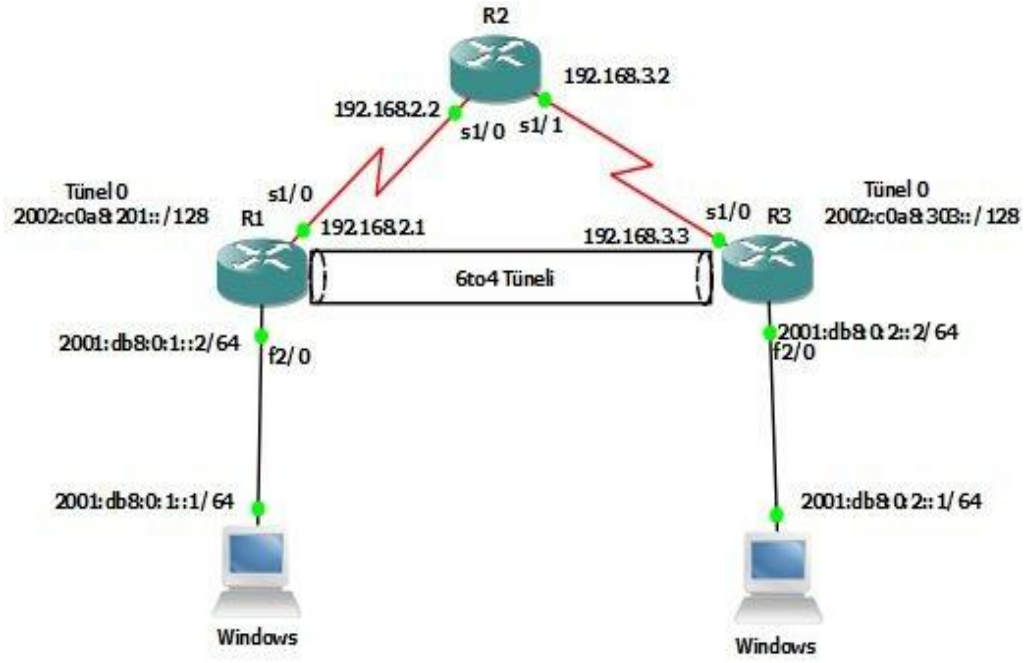
Şekil 4.3. IPv6 ağ ve adres şeması

Bu ağ senaryosunda yönlendiriciler ve bilgisayarlar 2001:DB8::/32 özel IPv6 ön ek ile yapılandırılmıştır ve bu adres aralığı IANA tarafından örnekler ve belgelendirmek için ayrılmıştır. Yönlendirme protokolü olarak RIP yönlendirme protokolü kullanılmıştır. Her iki sanal bilgisayarda Jperf programı çalışmıştır, ağın bir ucu Jperf (Alıcı) diğer ucu ise Jperf (Sunucu). Senaryonun yönlendirici yapılandırma çıktısı eklerde bulunmaktadır.

4.5.3. Otomatik tünelleme

6to4 ağı

6to4 ağ şeması ve IP adresleme şeması Şekil 4.4'de gösterilmiştir.



Şekil 4.4. 6to4 ağ ve adres şeması

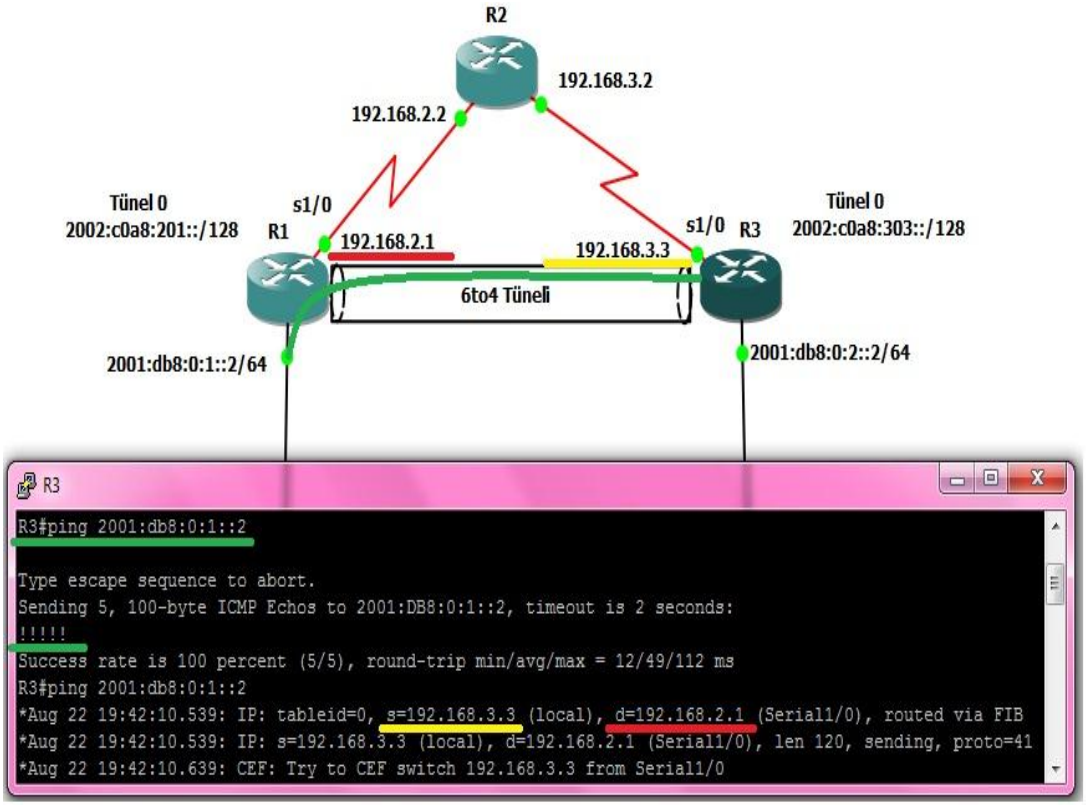
Bu senaryoda iki IPv6 ağı, IPv4 omurgalı şebekeye bağlanmıştır. Bu iki IPv6 ağı birbirleri ile iletişim kurmaları için R1 ve R3 yönlendiricilerinde 6to4 tüneli oluşturuldu. Tünelin IPv6 adresi, IANA tarafından 6to4 yöntemi için ayrılan 2002::/16 ön ek ile başlamaktadır. Tünelin IPv6 adresine R1 ve R3'ün kendi IPv4 adresini onaltılık hale dönüştürdükten sonra 2. ve 3. oktet'lere yerleştirilmiştir aşağıda Çizelge 4.2'de gösterilmiştir.

Çizelge 4.2. 6to4 tünelleme yönteminde adresi dönüştürme.

Yönlendirici	IPv4 adresi	Onaltılık adres dönüştürmesi	Tünel adresi
R1	192.168.2.1	c0a8.0201	2002:c0a8:201::/128
R2	192.168.3.3	c0a8.0303	2002:c0a8:303::/128

6to4 tünelleme yöntemi yönlendirme protokollerini desteklememektedir, bu yüzden yönlendirmeler elle yapılmıştır. Ağ performansını ölçmek için Jperf programı ağın ucunda çalışan bilgisayarlara Jperf programı çalıştırıldı. Ağın bir ucu Jperf (Alıcı) diğer ucu Jperf (Sunucu) olarak yapılandırıldı.

Şekil 4.5'te tünelin nasıl çalıştığı gösterilmektedir:

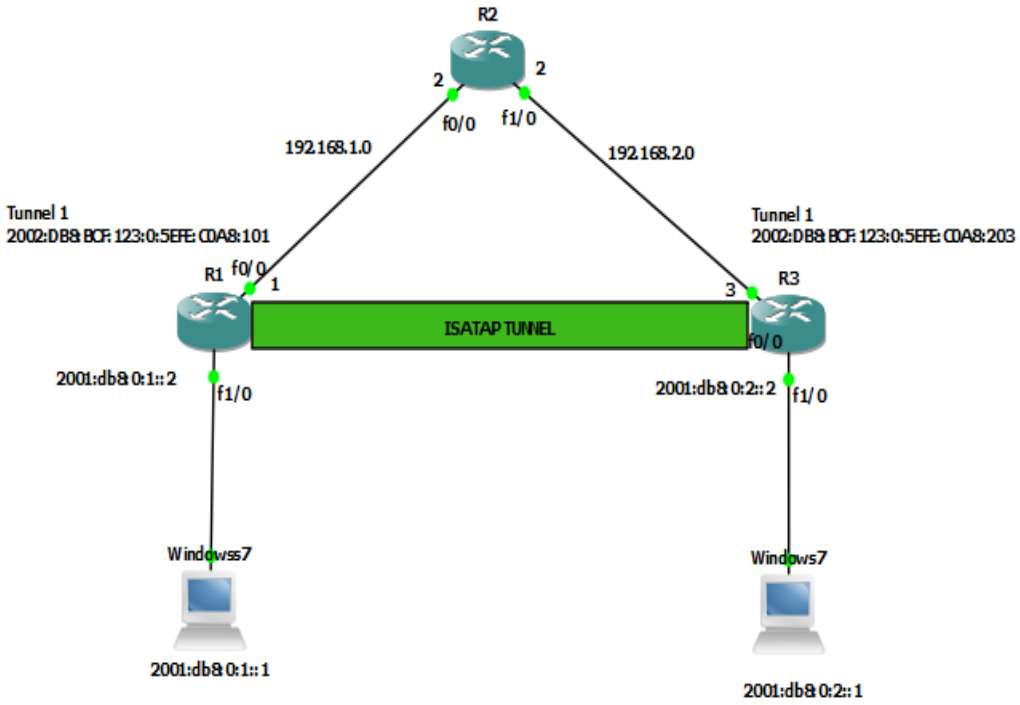


Şekil 4.5. Tünel çalışma şekli

Şekilde gösterildiği gibi, 6to4 tünelini kullanarak IPv4 omurgalı şebekede iki IPv6 adresi ile çalışan bilgisayarı birbirleri ile nasıl iletişim kurdukları gösterilmiştir. Benzetim ağında R3 ve R1 yönlendiricilerin bir arayüzü IPv4 adresi ile yapılandırılmış, diğer arayüz ise IPv6 adresi ile yapılandırılmıştır. Aynı zamanda da uç yönlendiriciler (R1, R3) tüneli oluşturdukları için sanal tünel adresine sahiptir. Bu sanal tünel sayesinde IPv6 paketleri R1'den R3'e IPv4 omurgalı R2'nin haberi olmadan gönderebilmektedir. Bu işlem de IPv6 önekli paketlerinin başına IPv4 öneki eklenmektedir, böylece paketler IPv6 ile alakası olmayan yönlendiricilere vardığında paketi IPv4 paketi sanarak rotasına yönlendirir ve paket tünelin sonuna yetiştiğinde paketten IPv4 öneki ayıklanır ve orijinal haline geri getirilir. Bütün bu işlemler önek ekleme ve ayıklama, tüneli oluşturan uç yönlendiricilerde yapılandırmaktadır. Şekil 4.5'te 6to4 tünelleme ağından örnek gösterilmiştir. Örnekte R3, R1'e Ping komutu gönderildi ve Ping komutu başarıyla gerçekleştirildi, Ping komutunun detaylarına bakıldığında Ping kaynağı ve Ping batağı yönlendiricilerin IPv4 adresin olduğu görülmektedir "şekilde sarı ve kırmızı çizgiyle gösterilmektedir" hâlbuki Ping komutu IPv6 adresinden IPv6 adresine gönderildi. Kısaca tünelleme yöntemini kullanarak IPv6 paketlerini IPv4 omurgalı ağlar üzerinden gönderilmektedir.

ISATAP

ISATAP ağ şeması ve IP adresleme şeması Şekil 4.6'de gösterilmiştir.



Şekil 4.6. ISATAP ağ ve adres şeması

Bu tünelleme yönteminin yapılandırması 6to4 yöntemi ile çok farkı olduğu söylenemez. Bu yöntemde tünel'in IPv4 adresi 7. ve 8. Oktete yerleştirilmektedir. Bu ağ senaryosunda yönlendiricilerin Fast Ethernet ara yüzleri ve bilgisayarlar 2001:DB8::/32 özel IPv6 ön ek ile yapılandırılmıştır ve bu adres aralığı IANA tarafından örnekler ve belgelendirmek için ayrılmıştır. Bu çalışmada yönlendirme protokolü olarak OSPF kullanıldı. Ağ ucunda bulunan her iki sanal bilgisayara Jperf programı yapılandırılmıştır. Ağın bir ucu Jperf (Alıcı) diğer ucu ise Jperf (Sunucu). Senaryonun yönlendirici yapılandırma çıktısı eklerde bulunmaktadır.

4.6. Deneme Sonuçları

Sonuçlar Jperf programı ekran çıktısı olarak gösterilecektir. Her ağ senaryosu hem UDP hem de TCP veri iletim protokolü kullanıldığında test edilmiştir. Sonuçlar grafiksel şekilde ve tablo şeklinde gösterilmiştir.

4.6.1. IPv6 ağı

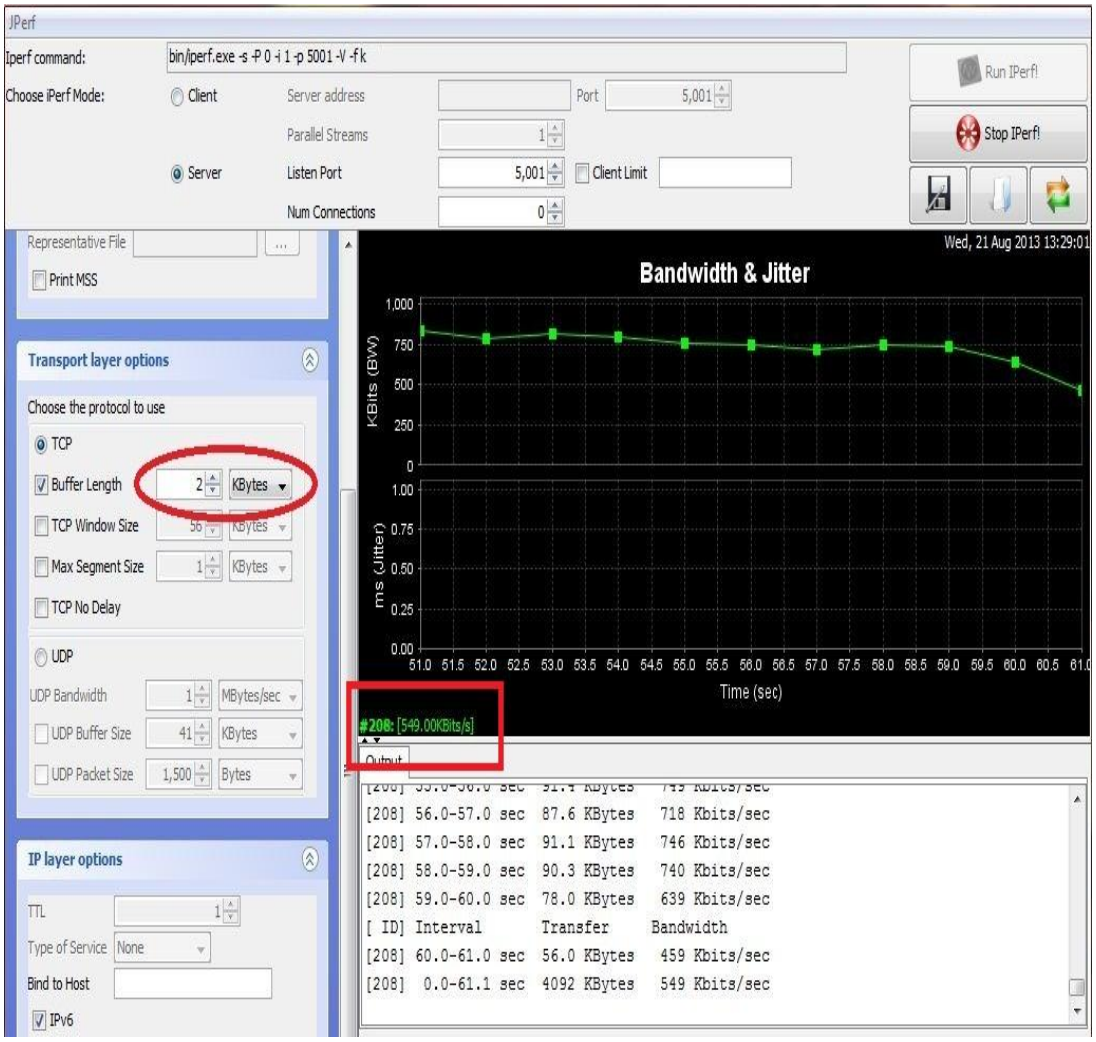
Verim ve Jitter

Jperf programı UDP denemesi başlatıldığında ekrana yansıyan bildirimler şu şekildedir:-

```
Bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -V -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 8 KByte (default)
local 2001:db8:0:1::1 port 5001 connected with 2001:db8:0:4::4 port 55454
------------------------------------------------------------
```

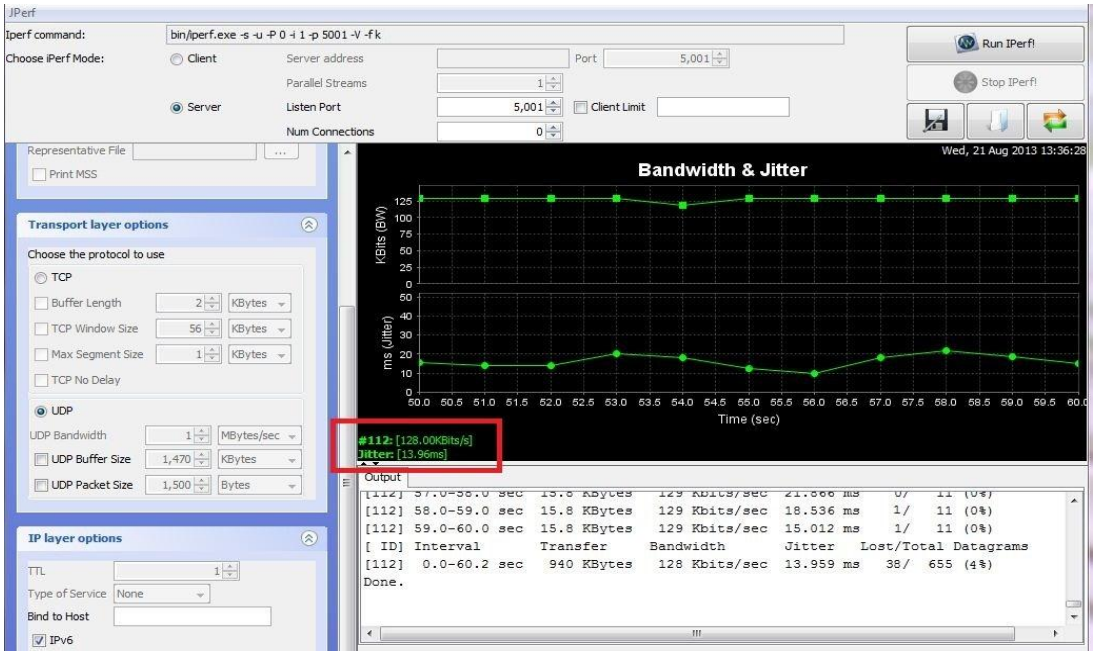
Jperf programı ile elde edilen sonuçlara göre, denemenin en iyi sonuç vermesi için 10 kez tekrarlandı. IPv6 ağ denemesi 60 saniye sürmüştür. TCP veri iletim protokolü kullanıldığında IPv6 ağ verimliliği yaklaşık %80 performans göstermiştir ayrıca veri aktarım sırasında bant genişliği ara sıra sıfıra düşmüştür bu da veri kaybına neden olmuştur. Bunun sebebi de veri aktarım sırasında karşı taraf verileri almakta yetiştirememesi ve bu da verilerin taşmasına (overflow) neden olmuştur.

Şekil 4.7'de Jperf alıcı tarafları TCP protokolü kullanıldığında yapılan denemeden ekran çıktıları gösterilmiştir.



Şekil 4.7. IPv6 ağı TCP kullanıldığında Jperf programı alıcı taraf ekran çıktısı

IPv6 senaryosu ile UDP veri iletim protokolü kullanıldığında ağ verimliliği 128 Kbits/s ve bu da %98 performans sergilediği anlamına gelmektedir. Jitter oranı 13.96 ms olarak rastlanmıştır. Jperf UDP sonuçları aşağıdaki Şekil 4.8'de gösterilmiştir:



Şekil 4.8. IPv6 ağı UDP kullanıldığında Jperf programı alıcı taraf ekran çıktısı

10 saniyelik Jperf sonuç çıktıs paket alıcı tarafta kaydediği gibi Şekil 4.9 gösterilmiştir :

```
[112] 50.0-51.0 sec  15.8 KBytes   129 Kbits/sec  13.961 ms    0/   11
[112] 51.0-52.0 sec  15.8 KBytes   129 Kbits/sec  13.723 ms    0/   11
[112] 52.0-53.0 sec  15.8 KBytes   129 Kbits/sec  20.142 ms    0/   11
[112] 53.0-54.0 sec  14.4 KBytes   118 Kbits/sec  17.967 ms    1/   10
[112] 54.0-55.0 sec  15.8 KBytes   129 Kbits/sec  12.159 ms    0/   11
[112] 55.0-56.0 sec  15.8 KBytes   129 Kbits/sec  9.566 ms     2/   11
[112] 56.0-57.0 sec  15.8 KBytes   129 Kbits/sec  18.252 ms    0/   11
[112] 57.0-58.0 sec  15.8 KBytes   129 Kbits/sec  21.866 ms    0/   11
[112] 58.0-59.0 sec  15.8 KBytes   129 Kbits/sec  18.536 ms    1/   11
[112] 59.0-60.0 sec  15.8 KBytes   129 Kbits/sec  15.012 ms    1/   11
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[112] 0.0-60.2 sec   940 KBytes 128 Kbits/sec 13.959 ms   38/655 (4%)
```

Şekil 4.9. IPv6 UDP kullanıldığında Jperf sonuç çıktısı

Şekil 4.9'de görüldüğü gibi 940 KByte veri 128 Kbits/s bant genişliğinde aktılmıştır. Aktarma sırasında jitter değeri 13.959 ms olarak görülmüştür. Ağ verimliliğin % 98 olmaktadır.

4.6.2. IPv4 ağı

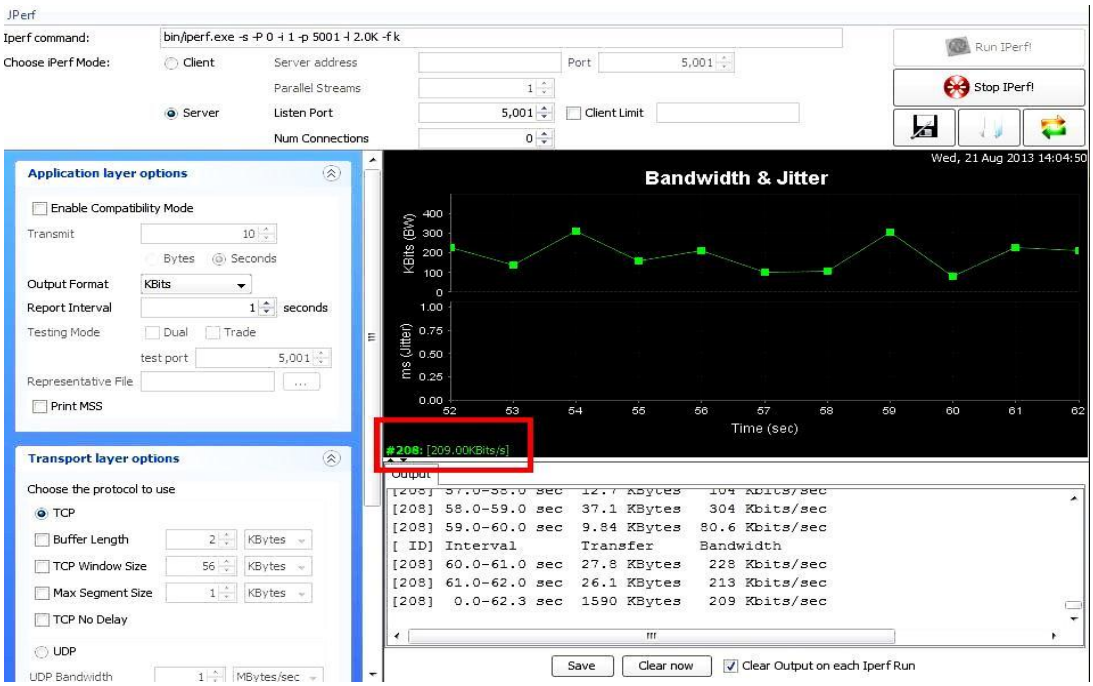
Verim ve Jitter

Denemenin iyi sonuç vermesi için 10 kez tekrarlandı. IPv4 ağ denemesi 60 saniye sürmüştür. Jperf programı UDP denemesi başlatıldığında ekrana yansıyan bildirimler şu şekildedir:-

```
Bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 8 KByte (default)
local 192.168.1.2 port 5001 connected with 192.168.4.4 port 56268

------------------------------------------------------------
```

IPv4 ağ senaryosunda, jperf programı ile hem UDP hem de TCP protokolleri test edilmiştir. Deneme TCP kullanıldığında veri iletim performansı IPv6 ağına göre %40 daha düşük performans göstermiştir. Şekil 4.10 jpef alıcı tarafında TCP protokolü kullanıldığında yapılan denemeden ekran çıktısı gösterilmiştir.



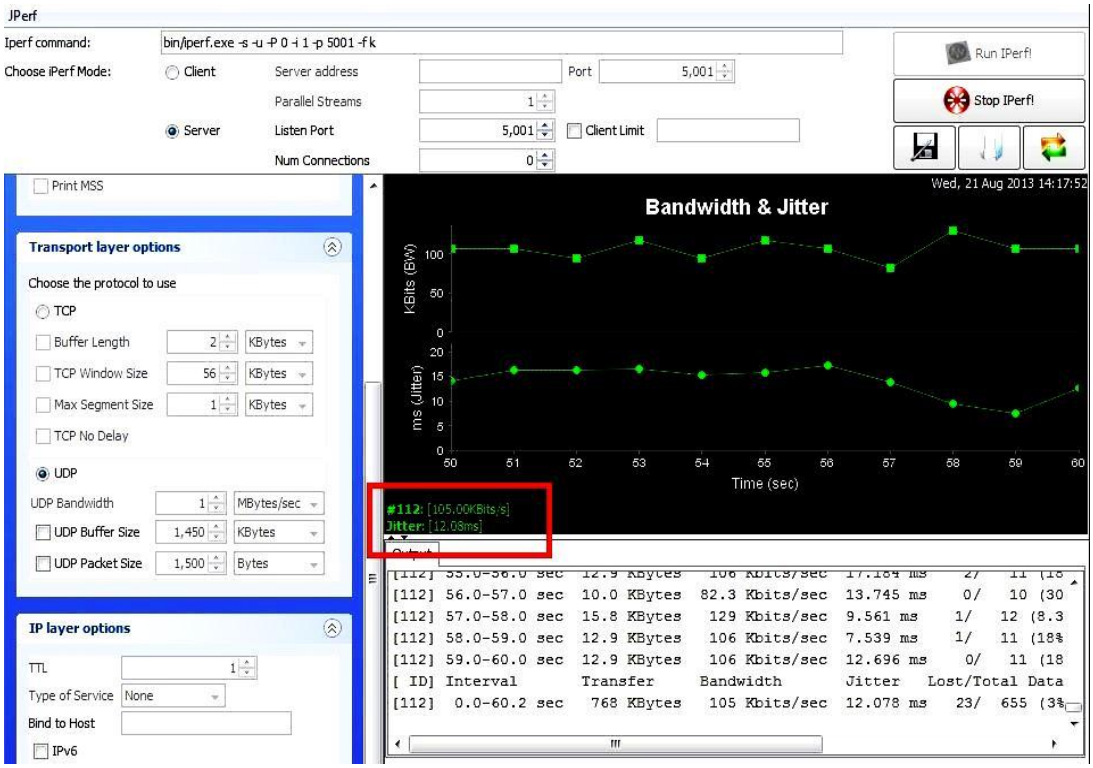
Şekil 4.10. IPv4 ağı TCP kullanıldığında Jperf programı alıcı taraf ekran çıktısı

IPv4 ağ senaryosunda UDP protokolü kullanıldığında ağ verimliliği 105 Kbits/s olarak görünmüştür. Bu oranda IPv6 ağına göre daha düşüktür. 10 saniyelik jperf alıcı taraf sonuç çıktısı aşağıdaki Şekil 4.11'de gösterilmişti:

```
[112] 50.0-51.0 sec  12.9 KBytes   106 Kbits/sec  16.319 ms     1/   11
[112] 51.0-52.0 sec  11.5 KBytes  94.1 Kbits/sec  16.221 ms     0/   10
[112] 52.0-53.0 sec  14.4 KBytes   118 Kbits/sec  16.522 ms     0/   12
[112] 53.0-54.0 sec  11.5 KBytes  94.1 Kbits/sec  15.236 ms     0/   10
[112] 54.0-55.0 sec  14.4 KBytes   118 Kbits/sec  15.702 ms     1/   11
[112] 55.0-56.0 sec  12.9 KBytes   106 Kbits/sec  17.184 ms     2/   11
[112] 56.0-57.0 sec  10.0 KBytes  82.3 Kbits/sec  13.745 ms     1/   10
[112] 57.0-58.0 sec  15.8 KBytes   129 Kbits/sec  9.561 ms      1/   12
[112] 58.0-59.0 sec  12.9 KBytes   106 Kbits/sec  7.539 ms      1/   11
[112] 59.0-60.0 sec  12.9 KBytes   106 Kbits/sec  12.696 ms     0/   11
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[112] 0.0-60.2 sec  768 KBytes  105 Kbits/sec  12.078 ms  23/  655 (3%)
```

Şekil 4.11. IPv4 UDP kullanıldığında Jperf sonuç çıktısı

60 saniye süren denemede Şekil 4.11'de görüldüğü gibi, 768 KByte veri 105 Kbits/s bant genişliğinde aktarılmıştır. Jitter oranı 12.078 ms bu oranda IPv6 ağ senaryosuna göre daha düşük gecikme oranıdır. Sonuçlar Şekil 4.12'da gösterilmiştir:



Şekil 4.12. IPv4 ağı UDP kullanıldığında Jperf programı alıcı taraf ekran çıktısı

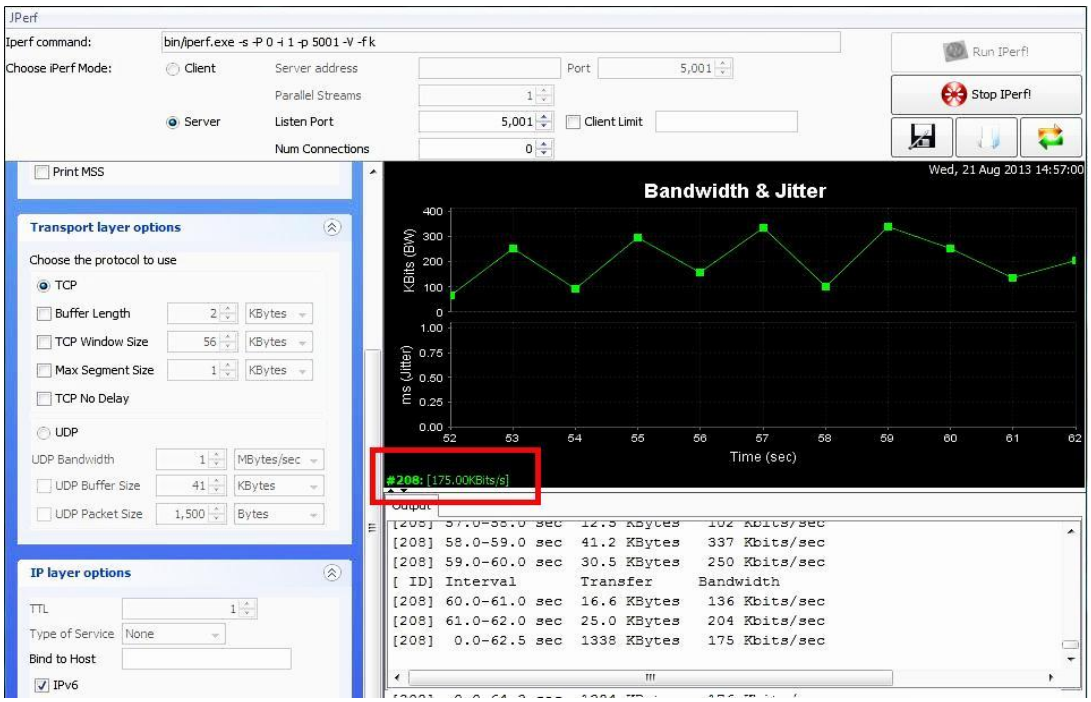
4.6.3. 6to4 ağı

Verim ve Jitter

Denemenin iyi sonuç vermesi için 10 kez tekrarlandı. 6to4 ağ denemesi tam 60 saniye sürmüştür. Jperf UDP denemesi başlatıldığında ekrana yansıyan bildirimler aşağıda gösterilmiştir:

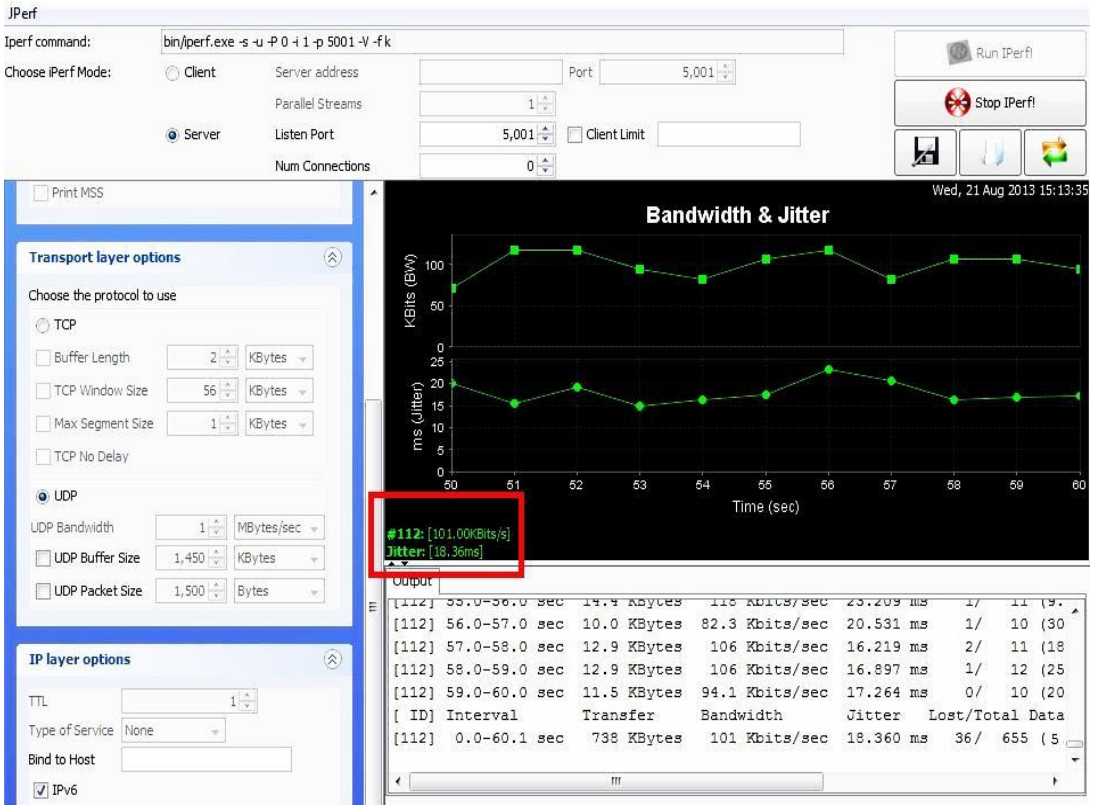
```
Bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -V -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 8 KByte (default)
[112] local 2001:db8:0:1::1 port 5001 connected with 2001:db8:0:2::1 port
57825
------------------------------------------------------------
```

TCP veri iletim protokolü kullanıldığında 6to4 tünelleme yöntemi ağı IPv4 ve IPv6 ağlarının gerisinde kalan bir performans göstermiştir. Şekil 4.13'da Jperf alıcı tarafında TCP protokolü kullanıldığında yapılan çalışmanın ekran çıktıları gösterilmiştir:



Şekil 4.13. 6to4 ağı TCP kullanıldığında Jperf programı alıcı taraf ekran çıktısı

6to4 UDP protokolü kullanıldığında jitter değeri ve kayıp paket oranı IPv4 ve IPv6 ağlarından daha da yüksek olduğu görülmüştür. Şekil 4.14'de Jperf alıcı tarafı UDP protokolü kullanıldığında alınan ekran çıktıları gösterilmiştir:



Şekil 4.14. 6to4 ağı UDP kullanıldığında Jperf programı alıcı taraf ekran çıktısı

10 saniyelik 6to4 ağ senaryosu UDP veri iletim protokolü kullanıldığında alınan sonuçların çıktısı Şekil 4.15'de gösterilmiştir:

```
[112] 50.0-51.0 sec  14.4 KBytes   118 Kbits/sec  15.580 ms    2/   12
[112] 51.0-52.0 sec  14.4 KBytes   118 Kbits/sec  19.237 ms    1/   11
[112] 52.0-53.0 sec  11.5 KBytes  94.1 Kbits/sec  14.959 ms    0/   10
[112] 53.0-54.0 sec  10.0 KBytes  82.3 Kbits/sec  16.253 ms    1/    9
[112] 54.0-55.0 sec  12.9 KBytes   106 Kbits/sec  17.407 ms    3/   13
[112] 55.0-56.0 sec  14.4 KBytes   118 Kbits/sec  23.209 ms    1/   11
[112] 56.0-57.0 sec  10.0 KBytes  82.3 Kbits/sec  20.531 ms    1/   10
[112] 57.0-58.0 sec  12.9 KBytes   106 Kbits/sec  16.219 ms    2/   11
[112] 58.0-59.0 sec  12.9 KBytes   106 Kbits/sec  16.897 ms    1/   12
[112] 59.0-60.0 sec  11.5 KBytes  94.1 Kbits/sec  17.264 ms    0/   10
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[112] 0.0-60.1 sec  738 KBytes 101 Kbits/sec  18.360 ms  36/  655 (5%)
```

Şekil 4.15. 6to4 UDP kullanıldığında Jperf sonuç çıktısı

60 saniye süren denemede, Şekil 4.15'te görüldüğü gibi, 738 KByte veri 101 Kbits/s bant genişliğinde aktarılmıştır. Jitter oranı IPv4 ve IPv6'ya göre daha yüksektir 18.360 ms.

4.6.4. ISATAP ağı

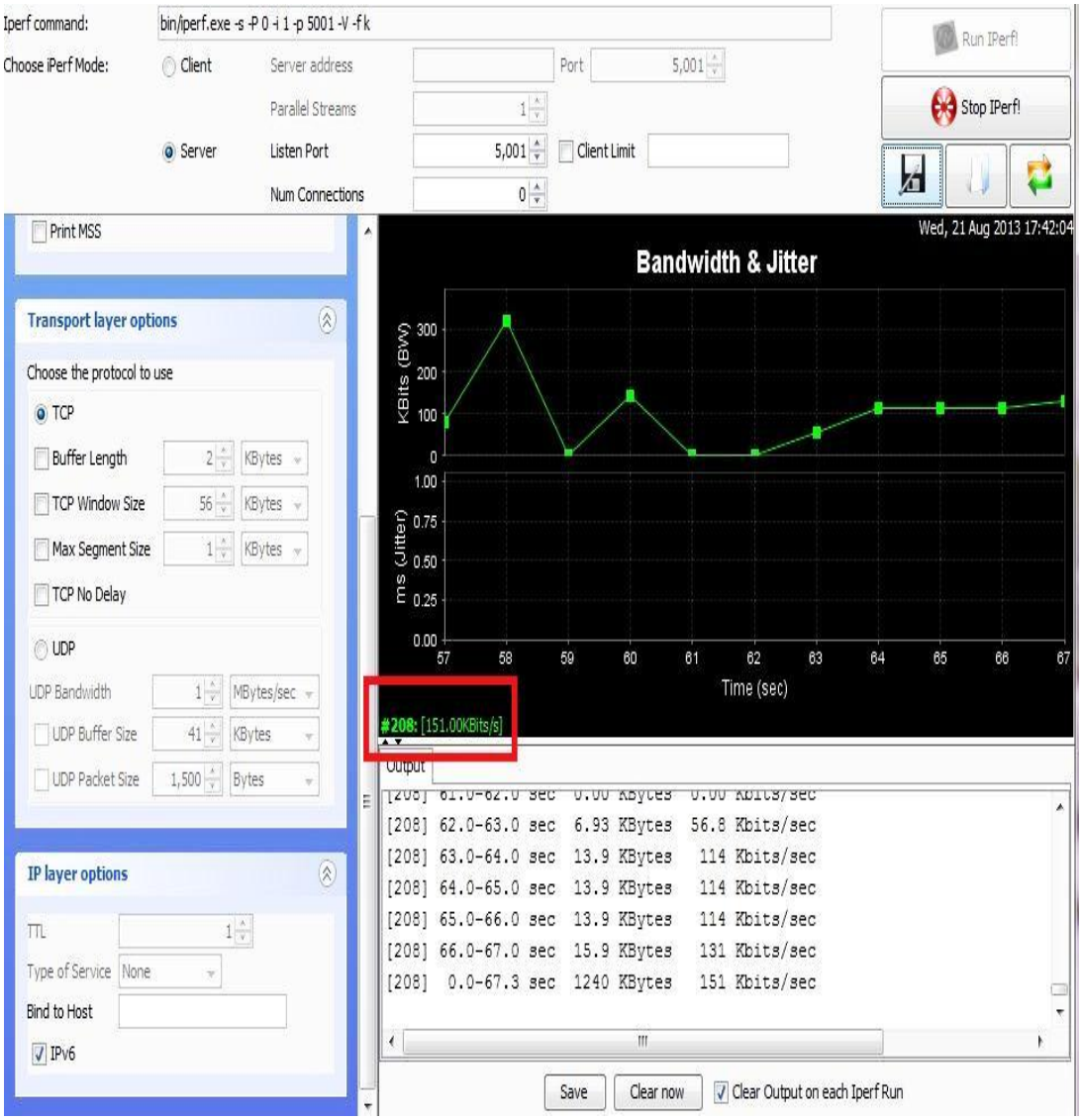
Verim ve Jitter

Denemenin iyi sonuç vermesi için 10 kez tekrarlandı. ISATAP ağ denemesi tam 60 saniye sürmüştür

Jperf programı UDP denemesi başlatıldığında ekrana yansıyan bildirimler şu şekildedir:-

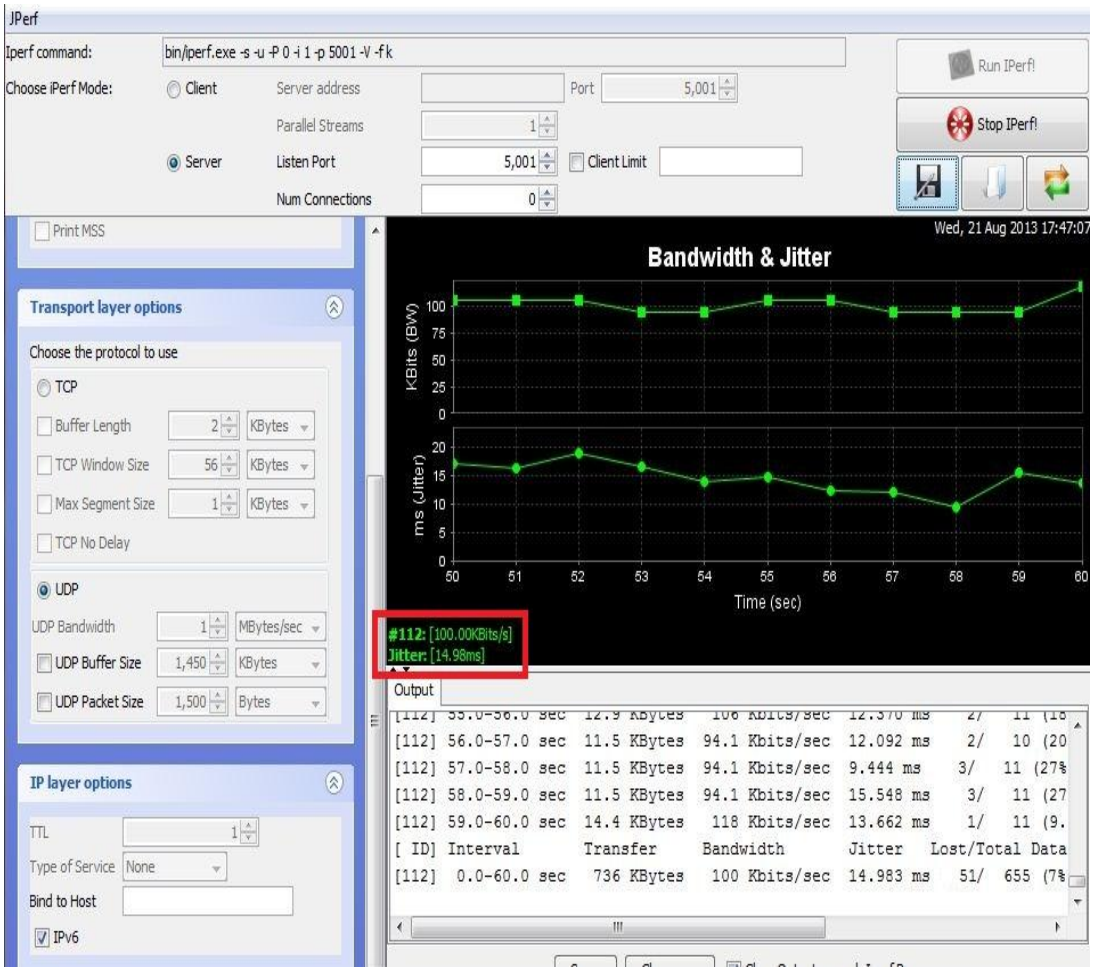
```
Bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -V -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 8 KByte (default)
[112] local 2001:db8:0:1::1 port 5001 connected with 2001:db8:0:2::1 port
50525
------------------------------------------------------------
```

ISATAP ağ senaryosuda, jperf programı ile hem UDP hem de TCP protokolleri test edilmiştir. ISATAP ağı, 6to4 ağ senaryosuna hem TCP'de hem de UDP protokolleri denemesinde birbirlerine yakın bir performans sergilemiştir. Denemede, paket gönderen taraf 1240 KByte veriyi jperf paket alıcı tarafına 161 Kbits/s bant genişliğinde göndermiştir. Şekil 4.16'te Jperf alıcı tarafında TCP protokolü kullanıldığında alınan ekran çıktıları gösterilmiştir:



Şekil 4.16. ISATAP ağı TCP kullanıldığında Jperf alıcı taraf ekran alıntısı

ISATAP UDP protokolü kullanıldığında jitter oranı 6to4 ağına göre daha da düşük olduğu saptanmıştır. Kayıp paket oranı ve ağ verimliliği 6to4 ağ senaryosu ile benzer sonuçlar vermiştir. Şekil 4.17'de Jperf alıcı tarafından UDP protokolü kullanıldığında ekran çıktıları gösterilmiştir:



Şekil 4.17. ISATAP ağ UDP kullanıldığında Jperf alıcı tarafından ekran alıntısı

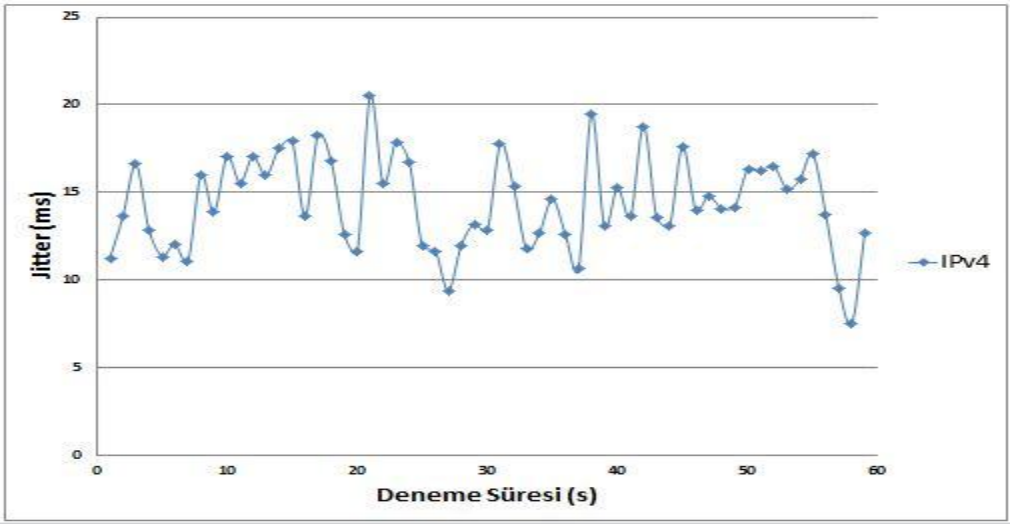
10 saniyelik ISATAP ağ senaryosu UDP veri iletim protokolü kullanıldığında alınan sonuç çıktıları Şekil 4. 18'de gösterilmiştir:

```
[112] 50.0-51.0 sec  12.9 KBytes    106 Kbits/sec  16.222 ms     0/    9
[112] 51.0-52.0 sec  12.9 KBytes    106 Kbits/sec  18.801 ms     4/   13
[112] 52.0-53.0 sec  11.5 KBytes   94.1 Kbits/sec  16.509 ms     2/   10
[112] 53.0-54.0 sec  11.5 KBytes   94.1 Kbits/sec  13.890 ms     2/   10
[112] 54.0-55.0 sec  12.9 KBytes    106 Kbits/sec  14.691 ms     3/   12
[112] 55.0-56.0 sec  12.9 KBytes    106 Kbits/sec  12.370 ms     2/   11
[112] 56.0-57.0 sec  11.5 KBytes   94.1 Kbits/sec  12.092 ms     2/   10
[112] 57.0-58.0 sec  11.5 KBytes   94.1 Kbits/sec  9.444 ms      3/   11
[112] 58.0-59.0 sec  11.5 KBytes   94.1 Kbits/sec  15.548 ms     3/   11
[112] 59.0-60.0 sec  14.4 KBytes    118 Kbits/sec  13.662 ms     1/   11
[ ID] Interval       Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[112] 0.0-60.0 sec 736 KBytes  100 Kbits/sec 14.983 ms  51/  655 (7%)
```

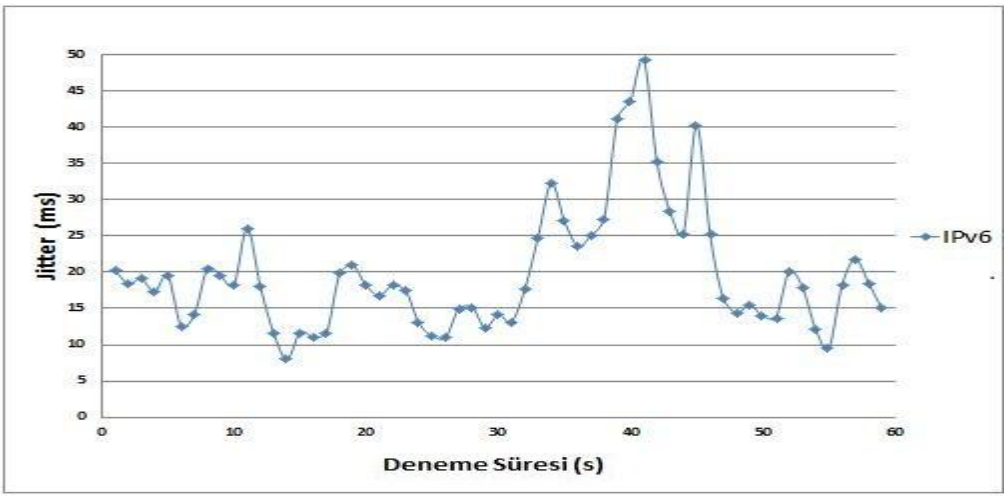
Şekil 4.18. ISATAP UDP kullanıldığında Jperf sonuç çıktısı

60 saniye süren denemede Şekil 4.18'da görüldüğü gibi, 736 KByte veri 100 Kbits/s bant genişliğinde aktarılmıştır. Jitter oranı 14.938 ms bu oran da 6to4 ağ senaryosu performansına göre daha düşüktür.

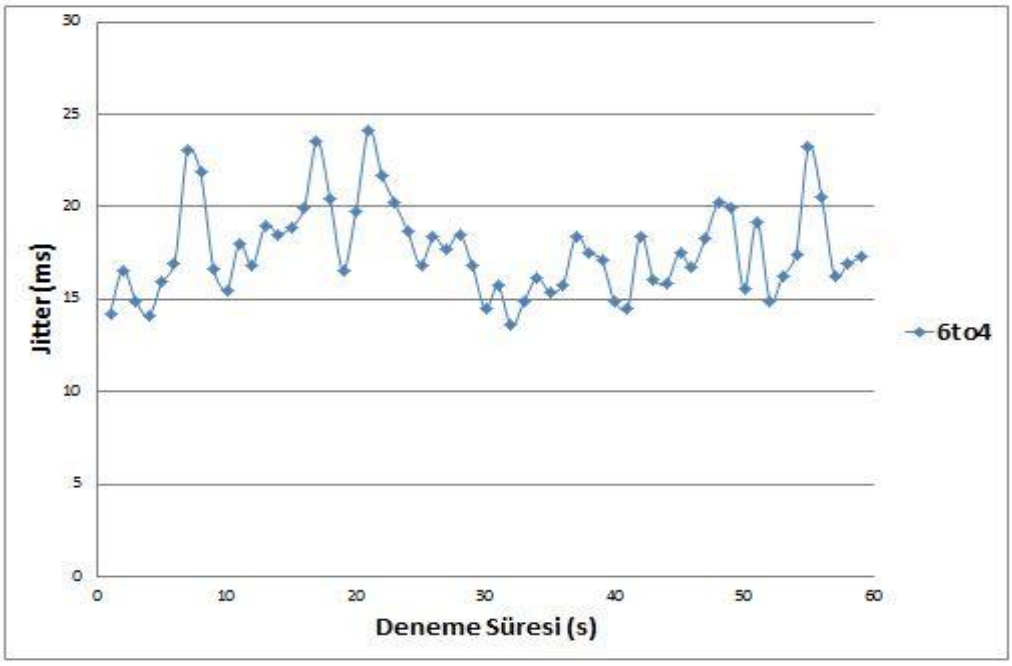
60 saniyelik deneme süre içerisinde oluşan jitter değerileri Şekil 4.19, Şekil 4.20, Şekil 4.21 ve Şekil 4.22 gösterilmiştir:



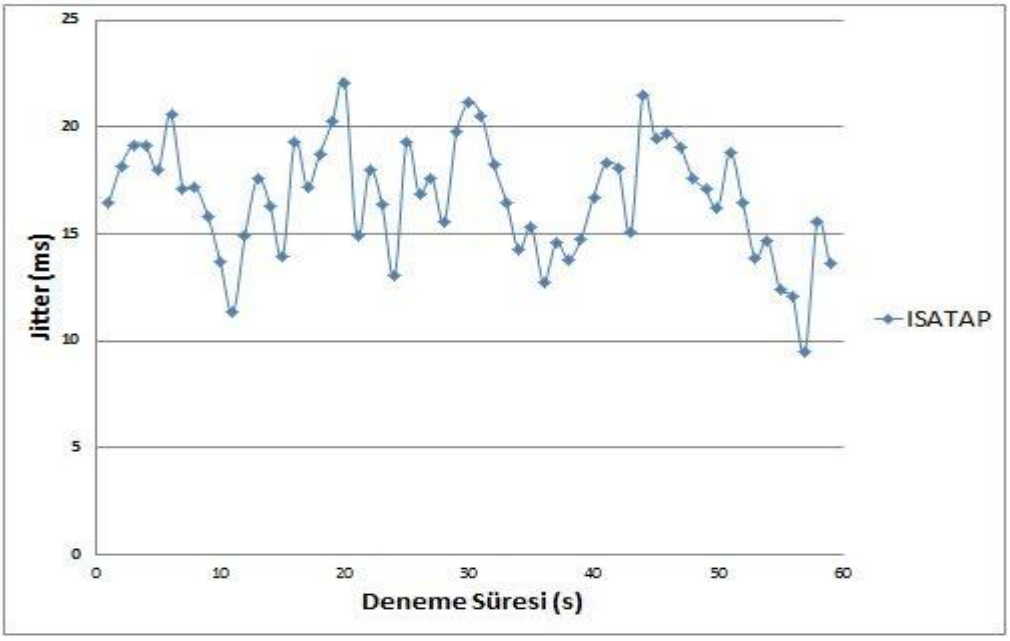
Şekil 4.19. IPv4 ağında oluşan jitter değerleri



Şekil 4.20. IPv6 ağında oluşan jitter değerleri



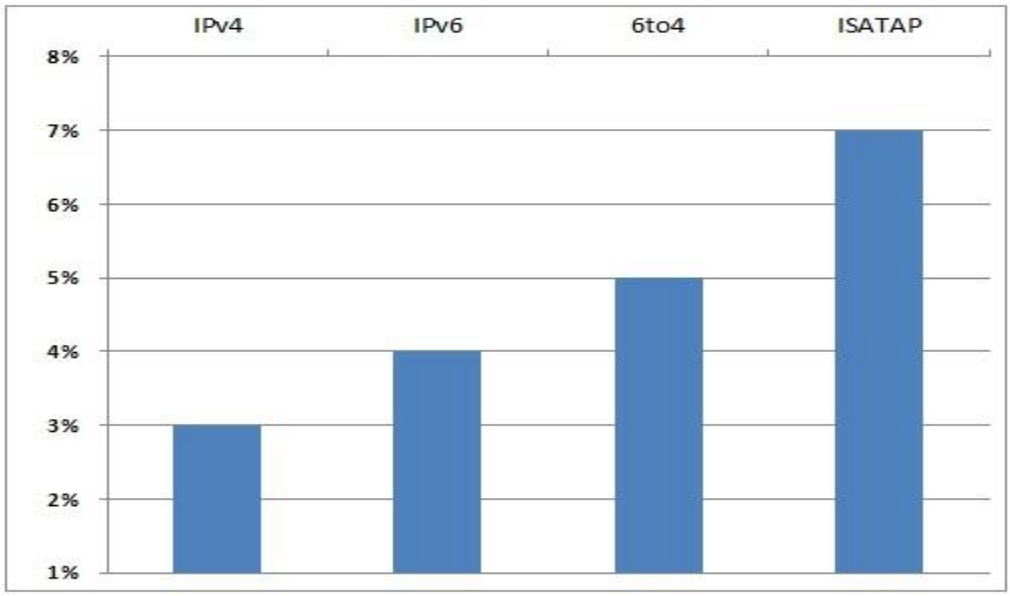
Şekil 4.21. IPv4 ağında oluşan jitter değerleri



Şekil 4.22. ISATAP ağında oluşan jitter değerleri

4.7. Kayıp Veri Oranları

Kayıp veri oranı bütün senaryolar için UDP veri iletim protokolü kullanıldığında jperf programı ile hesaplanmıştır. Şekil 4.23'de ağ senaryolarında oluşan veri kaybı ortalaması gösterilmiştir.



Şekil 4.23. Kayıp veri oranı

En çok kayıp veri oranı otomatik tünelleme yöntemlerinde oluşmuştur bunun nedeni tünellin uc yönlendiricilerinde yapılan veri kapsülleme işlemlerinden kaynaklanmıştır.

4.8. Sonuç Tartışması

TCP protokolü kullanıldığında her ağ senaryosu için ağ verimliliği Çizelge 4.3'de gösterilmiştir. TCP protokolü kullanıldığında en yüksek ağ verimliliği 549 Kbits/s ortalama verimlilik oranıyla IPv6 ağ senaryosu göstermiştir, bu oran 209 Kbits/s ortalamasıyla IPv4 ağı ile karşılaştırılırsa, IPv6 %50 daha hızlı ve daha verimli bir şekilde çalışmıştır. Otomatik tünelleme yöntemlerinde TCP veri iletim protokolü kullanıldığında 6to4 yönteminde ağ verimlilik ortalaması 182 Kbits/s ISATAP yönteminde ise 151 Kbits/s. Otomatik tünelleme ağlarının performansları arasında

büyük bir fark gözükmemektedir bunun yanısıra IPv4 ağı ile de çok farkı olduğu söylenemez ancak IPv6 ağ senaryosunun performansı ile karştırılırsa diğer yöntemlerin iyi performans sergilediği söylenemez.

Çizelge 4.3. TCP protokolü kullanıldığında bant genişliği kullanım oranları

Ağ Senaryoları Kbits/s	**Maksimum verimlilik Kbits/s**	**Minimum verimlilik Kbits/s**	**Verimlilik ortalaması Kbits/s**
IPv6	980 Kbits/s	11.7 Kbits/s	549 Kbits/s
IPv4	472 Kbits/s	34.6 Kbits/s	209 Kbits/s
6to4	300 Kbits/s	56.8 Kbits/s	182 Kbits/s
ISATAP	299 Kbits/s	34.1 Kbits/s	151. Kbits/s

UDP veri iletim protokolü kullanıldığında veri aktarımı yapıldığında ağ verimliliği ve gecikme değerleri Çizelge 4.4'te gösterilmiştir. Çizelge 'de görüldüğü gibi IPv6 ağı 128 Kbits/s verimlilik değeri ile 100% verimlilik göstermiştir bu oranla da UDP veri iletim protokolü kullanıldığında IPv6 ağı diğer protokollerden üstünlüğü görülmüştür. IPv4 ağı verimliliği 105 Kbits/s verimlilikle tünelleme yöntemlerinden az ölçüde olsa da iyi performans sergilemiştir. Gecikme değeri (Jitter) tünelleme yöntemlerinde diğer ağ senaryolarından yüksektir. Bu metrikler sanal ortam ağlarında benzetim programları kullanarak elde edilmiştir.

Çizelge 4.4. UDP kullanıldığında bant genişliği ve jitter değeri oranları

Ağ senaryoları	**Verimlilik ortalaması Kbits/s**	**Jitter ortalaması**
IPv6	128 Kbits/s	13.96 ms
IPv4	105 Kbits/s	12.08 ms
6to4	101 Kbits/s	18.36 ms
ISATAP	100 Kbits/s	14.98 ms

5. SONUÇ VE ÖNERİLER

Bu tez çalışmasında, günümüzde yaygın olarak kullanılan ve internet ağının temelini oluşturan internet protokolleri (IP) günümüzü ve gelecekte izleyeceği yol haritası üzerine bilgiler sunulmuştur. Günümüzde kullanılan IPv4 üzerine ve gelecekte kullanılacak IPv6 temel yapıları incelenmiştir. IPv6 geçiş sürecinde günümüze kadar yapılan çalışmalar incelenip, eksik yönlerini göz önüne alarak benzetim ağları geliştirilmiştir. Benzetim programları kullanılarak IPv4, IPv6 ve otomatik tünelleme yöntemleri (6to4, ISATAP) ağları yapılandırılıp birbirleriyle karşılaştırma yapılmıştır.

IPv6'ya geçiş süreci sırasında otomatik 6to4 tünelleme yöntemi 6to4 elde edilen sonuçlara göre gerek TCP gerekse UDP denemesinde ISATAP yönteminden daha iyi başarım göstermiştir.

IPv6, eski sürüm internet protokolü olan IPv4'ün yerini almak için geliştirilmiştir, bu nedenle IPv4'ten daha iyi çalışması için eski sürümdeki bütün hatalar giderilmeye çalışılmıştır. IPv6 öneki IPv4 önekinden daha basit bir yapıya sahiptir. örnek olarak seçenek alanı IPv4 başlığına dahildir, IPv6 önekinde ise bir uzantıdır. IPv6 başlığı IPv4 başlığına göre daha az karmaşıktır. IPv4'te hata algılaması (Checksum) IPv6'ten kaldırılmıştır hata algılaması diğer katmanlarda yapılmaktadır IPv6'da, denemelerden çıkan sonuçlar bütün bunları desteklemektedir.

Çalışmada küçük paket boyutları kullanılmıştır, gelecekteki çalışmalarda büyük paket boyutları kullanılarak performans değerlendirmesi yapılabilir.

Çalışmalar sanal ortamda, benzetim programları kullanılarak gerçekleştirilmiştir, ileri çalışmalarda gerçek donanımlar kullanılarak bu çalışma izlenebilir.

KAYNAKLAR

[1] Prabuwono, A., Bahaman, N " Network Performance Evaluation of 6to4 Tunneling" ***International conference on Innovation, Management and Technology Research(ICIMTR2012),*** Malacca, Malaysia, 459-460 (2012) ,

[2] Yoshfji, H., Hiromi, R., "Problems on IPv4-IPv6 network transition", ***Proceedings of the International Symposium on Applications and the Internet Workshops (SAINT)***, 38-42 (2006).

[3] Govil, J., Kaur, H., and Govil, J., Kaur, N., "An examination of IPv4 and IPv6 networks: Constraints and various transition mechanisms", ***Proceedings of IEEE Sounteastcon***, 178-185, (2008).

[4] Choe, B., Park, E, and Lee J. "An IPv4-to-IPv6 dual stack transition mechanism supporting transparent connections between IPv6 hosts and IPv4 hosts in integrated IPv6/IPv4 network", ***Proceedings of the IEEE International Conference on Communications***, USA, vol. 2, 1024-1027, (2004).

[5] Taa, M., Nasir, N. Tahir, H., B., "Implementation of IPv4 Over IPv6 using Dual Stack Transition Mechanism (DSTM) on 6iNet", ***Proceedings of the International Conference on Information & Communication Technologies: From Theory to Applications (lCTTA)***, USA, 3156 -3162, (2006).

[6] Kitatsuji, Y. ve Arkadaşları, "JGN IPv6 network", ***Proceedings of the Symposium on Applications and the Internet Workshops***, Malaysia, 161-166, January (2003).

[7] ngxian, Qi. and Xiaorui K. "Discovering IPv6 network topology", ***Proceedings of the IEEE International Symposium on Communications and Information Technology (lSCIT),*** Zhengzhou, China, 1313- 1319, (2005).

[8] Awan, I., Mellor, j. and , Aua'afreh, R., "Comparison Between the Tunneling Process and MapPing Schemes for IPv4/IPv6 Transition" ***Proceedings of the***

International Conference on Advanced Information Networking and Applications Workshops (WAINA), Malaysia ,601-606, (2009).

[9] Zeadally, S. and Raicu "Evaluating IPv4 to IPv6 transition mechanisms", ***Proceedings of the 10th International Conference on Telecommunications (lCT)***, 1091-1098, (2003).

[10] Hong, Y., and Kim, H. Shin M. , "Application translation for IPv6 at NAT-PT", ***Proceedings of the 9th Asia-Pacific Conference on Communications (APCC)***, China, 201-209, (2003).

[11] Taib, A., AI-tamimi, B. and Budiarto, R. , "Protecting teredo clients from source routing exploits", ***Proceedings of the First International Conference on Distributed Framework and Applications (DFmA)***, 123-138, (2008).

[12] Kim, H., Santay, D. and Montgomery, D. and Shin, M. "An empirical analysis of IPv6 transition mechanisms", ***Proceedings of the 8th International Conference on Advanced Communication Technology (ICACT)***, China, 1990-1996, (2006)

[13] Karuppiah, E. "Application Performance Analysis in Transition Mechanism from IPv4 to IPv6". Research & Business Development Department, Faculty of Information Technology, ***Multimedia University (MMU)***, Jalan Multimedia, 143-161, (2001).

[14] Kevin, R. ve Arkadaşları, "Analysis of the IPv4 Address Space Delegation Structure "***,IEEE.,*** 4244-1521, (2007).

[15] Deering, S., Hinden, R. '' Internet Protocol'', ***İnternet engineering task force magazine, RFC 791,*** (1981).

[16] Deering, S., Hinden, R. "Internet Protocol Version 6 (IPv6) Addressing Architecture", ***İnternet engineering task force magazine, RFC 3513,*** (2003).

[17] Gerich, E., "Guidelines for Management of IP Address Space", ***İnternet engineering task force magazine, RFC 1466***, (1993).

[18] Deering, S., Hinden, R., "Internet Protocol, Version 6 (IPv6) Specification", ***İnternet engineering task force magazine, RFC 2460***, (1998).

[19] Internet: Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi, http://www.ipv6.net.tr/ (2012).

[20] Comer, D., "Computer Networks And internet with internet applications international", ***Prentice Hall***, Pearson, 341-359 (2004).

[21] Ullanderson, E., "CCNP ROUTE 642-902 Official Certification Guide", ***Cisco***, New York, 529-661, (2010)

[22] Dupont, F. ve Arkadaşları, "Dual Stack Transition Mechanism (DSTM)", ***Proceedings of the 8th International Conference on Advanced Communication Technology (ICACT)***,(2002).

[23] Subramanian, S., "IPv6 Transition Strategies", ***White paper, WIPRO Co***., (2003).

[24] İnternet: Microsoft White Paper, 2005. "IPv6 Transition Technologies", http://download.microsoft.com/download/7/4/1/741daf62-02d6-40f3-b082-701b5acc56d6/IPv6Trans.doc (2013).

[25] İnternet: Benzetim Ağ Simülatör Programı https://www.gns3.net (2013).

[26] İnternet: Sanal Bilgisayar Simülatörü https://www.virtualbox.org (2013).

[27] İnternet: Veri Akış Üreticisi www.iperf.fr (2013).

[28] ERDĞAN, K., "İPv4'ten İPv6'ya geçiş süreci için İPv6 tünel ve sanal hedef IP teknikleri", Yüksek Lisans Tezi, ***Gazi Üniversitesi, Elektrik Elektronik Mühendisliği,*** Ankara, 278-292, 301-308, 615-621, 688-690 (2007).

[29] Miller, P., Miller, M., "Implementing IPv6: Supporting the Next Generation Internet Protocols", ***M&T Books***, Boston, Volume 2, (2000).

[30] Waddington, D. , Chang, F., "Realizing the Transition to IPv6", ***Bell Research Laboratories, IEEE Communications Magazine***, 136-150 (2002).

[31] Huitema, C., "IPv6 The New Internet Protocol", ***Prentice Hall***, Pearson, Volume 2, (1998).

[32] Raicu, I., " An Empirical analysis of internet protocol version 6 (IPv6)", Yüksek Lisans Tezi, ***School of Wayne State University***, Michigan, 11-50 (2002)

[33] Bieringer, P., "Status of IPv6 (Information & Workshop) ", ***IEEE CNF, Applications and the Internet Workshops***, 52 – 59(2005).

EKLER

EK-1 IPv4 AĞININ YAPILANDIRMASI

****

R1

****

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
boot-start-marker
boot-end-marker
no aaa new-model
ip subnet-zero
no ip domain lookup
ip domain name lab.local
ip cef
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex half
```

EK-1 (Devam) IPv4 ağının yapılandırması

R1

****

```
interface Serial1/0
ip address 192.168.2.1 255.255.255.0
serial restart-delay 0
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/4
```

EK-1 (Devam) IPv4 ağının yapılandırması

R1

****

```
no ip address
shutdown
serial restart-delay 0
interface Serial1/5
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/6
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/7
 no ip address
 shutdown
 serial restart-delay 0
ip classless
```

EK-1 (Devam) IPv4 ağının yapılandırması

R1

****

ip route 192.168.3.0 255.255.255.0 192.168.2.2

ip route 192.168.4.0 255.255.255.0 192.168.2.2

no ip http server

gatekeeper

shutdown

line con 0

 exec-timeout 0 0

 privilege level 15

 logging synchronous

 stopbits 1

line aux 0

 exec-timeout 0 0

 privilege level 15

 logging synchronous

 stopbits 1

line vty 0 4

EK-2 IPv4 ağının yapılandırması

R2

****

login

end

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname R2

boot-start-marker

boot-end-marker

no aaa new-model

ip subnet-zero

no ip domain lookup

ip domain name lab.local

ip cef

interface FastEthernet0/0

no ip address

EK-2 (Devam) IPv4 ağının yapılandırması

R2

****

shutdown

duplex half

interface Serial1/0

 ip address 192.168.2.2 255.255.255.0

 serial restart-delay 0

interface Serial1/1

 ip address 192.168.3.2 255.255.255.0

serial restart-delay 0

interface Serial1/2

 no ip address

 shutdown

 serial restart-delay 0

interface Serial1/3

no ip address

shutdown

serial restart-delay 0

EK-2 (Devam) IPv4 ağının yapılandırması

R2

****

interface Serial1/4

no ip address

shutdown

serial restart-delay 0

interface Serial1/5

no ip address

shutdown

serial restart-delay 0

interface Serial1/6

no ip address

shutdown

serial restart-delay 0

interface Serial1/7

no ip address

shutdown

serial restart-delay 0

EK-2 (Devam) IPv4 ağının yapılandırması

R2

****

ip classless

ip route 192.168.1.0 255.255.255.0 192.168.2.1

ip route 192.168.4.0 255.255.255.0 192.168.3.3

no ip http server

gatekeeper

shutdown

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

login

end

EK-3 IPv4 ağının yapılandırması

R3

****

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname R3

boot-start-marker

boot-end-marker

no aaa new-model

ip subnet-zero

no ip domain lookup

ip domain name lab.local

ip cef

interface FastEthernet0/0

EK-3 (Devam) IPv4 ağının yapılandırması

R3

****

ip address 192.168.4.3 255.255.255.0

duplex half

interface Serial1/0

ip address 192.168.3.3 255.255.255.0

serial restart-delay 0

interface Serial1/1

no ip address

shutdown

serial restart-delay 0

interface Serial1/2

no ip address

shutdown

serial restart-delay 0

interface Serial1/3

no ip address

shutdown

EK-3 (Devam) IPv4 ağının yapılandırması

R3

****

serial restart-delay 0

interface Serial1/4

no ip address

shutdown

serial restart-delay 0

interface Serial1/5

no ip address

shutdown

serial restart-delay 0

interface Serial1/6

no ip address

shutdown

serial restart-delay 0

interface Serial1/7

no ip address

shutdown

EK-3 (Devam) IPv4 ağının yapılandırması

R3

****

serial restart-delay 0

ip classless

ip route 192.168.1.0 255.255.255.0 192.168.3.2

ip route 192.168.2.0 255.255.255.0 192.168.3.2

no ip http server

gatekeeper

shutdown

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

login

end

EK-3 IPv6 AĞININ YAPILANDIRMASI

****

R1

****

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname R1

boot-start-marker

boot-end-marker

no aaa new-model

ip subnet-zero

no ip domain lookup

ip domain name lab.local

EK-3 (Devam) IPv6 ağının yapılandırması

R1

****

```
ip cef
ipv6 unicast-routing
interface FastEthernet0/0
no ip address
shutdown
duplex half
interface Serial1/0
no ip address
ipv6 address 2001:DB8:0:2::1/64
ipv6 enable
ipv6 rip ersen enable
serial restart-delay 0
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
```

EK-3 (Devam) IPv6 ağının yapılandırması

R1

****

interface Serial1/2

no ip address

shutdown

serial restart-delay 0

interface Serial1/3

no ip address

shutdown

serial restart-delay 0

interface Serial1/4

no ip address

shutdown

serial restart-delay 0

interface Serial1/5

no ip address

shutdown

serial restart-delay 0

EK-3 (Devam) IPv6 ağının yapılandırması

R1

****

```
interface Serial1/6
no ip address
shutdown
serial restart-delay 0
interface Serial1/7
no ip address
shutdown
serial restart-delay 0
interface FastEthernet2/0
no ip address
duplex auto
speed auto
ipv6 address 2001:DB8:0:1::2/64
ipv6 enable
ipv6 rip ersen enable
interface FastEthernet2/1
```

EK-3 (Devam) IPv6 ağının yapılandırması

R1

****

no ip address

shutdown

duplex auto

speed auto

ip classless

no ip http server

ipv6 router ospf 10

log-adjacency-changes

ipv6 router rip ersen

gatekeeper

shutdown

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

login

end

EK-4 IPv6 ağının yapılandırması

R2

****

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname R2

boot-start-marker

boot-end-marker

no aaa new-model

EK-4 (Devam) IPv6 ağının yapılandırması

R2

****

ip subnet-zero

no ip domain lookup

ip domain name lab.local

ip cef

ipv6 unicast-routing

interface FastEthernet0/0

no ip address

shutdown

duplex half

interface Serial1/0

no ip address

ipv6 address 2001:DB8:0:2::2/64

ipv6 enable

ipv6 rip ersen enable

serial restart-delay 0

interface Serial1/1

EK-4 (Devam) IPv6 ağının yapılandırması

R2

****

no ip address

ipv6 address 2001:DB8:0:3::2/64

ipv6 enable

ipv6 rip ersen enable

serial restart-delay 0

interface Serial1/2

no ip address

shutdown

serial restart-delay 0

interface Serial1/3

no ip address

shutdown

serial restart-delay 0

interface Serial1/4

no ip address

shutdown

EK-4 (Devam) IPv6 ağının yapılandırması

R2

****

serial restart-delay 0

interface Serial1/5

no ip address

shutdown

serial restart-delay 0

interface Serial1/6

no ip address

shutdown

serial restart-delay 0

interface Serial1/7

no ip address

shutdown

serial restart-delay 0

ip classless

no ip http server

ipv6 router ospf 10

EK-4 (Devam) IPv6 ağının yapılandırması

R2

****

log-adjacency-changes

ipv6 router rip ersen

gatekeeper

shutdown

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

end

EK-5 IPv6 ağının yapılandırması

R3

****

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname R3

boot-start-marker

boot-end-marker

no aaa new-model

ip subnet-zero

no ip domain lookup

ip domain name lab.local

ip cef

ipv6 unicast-routing

interface FastEthernet0/0

no ip address

shutdown

EK-5 (Devam) IPv6 ağının yapılandırması

R3

****

duplex half

interface Serial1/0

no ip address

ipv6 address 2001:DB8:0:3::3/64

ipv6 enable

ipv6 rip ersen enable

serial restart-delay 0

interface Serial1/1

no ip address

shutdown

serial restart-delay 0

interface Serial1/2

no ip address

shutdown

serial restart-delay 0

interface Serial1/3

EK-5 (Devam) IPv6 ağının yapılandırması

R3

****

no ip address

shutdown

serial restart-delay 0

interface Serial1/4

no ip address

shutdown

serial restart-delay 0

interface Serial1/5

no ip address

shutdown

serial restart-delay 0

interface Serial1/6

no ip address

shutdown

serial restart-delay 0

interface Serial1/7

EK-5 (Devam) IPv6 ağının yapılandırması

R3

****

no ip address

shutdown

serial restart-delay 0

interface FastEthernet2/0

no ip address

duplex auto

speed auto

ipv6 address 2001:DB8:0:4::3/64

ipv6 enable

ipv6 rip ersen enable

interface FastEthernet2/1

no ip address

shutdown

duplex auto

speed auto

ip classless

EK-5 (Devam) IPv6 ağının yapılandırması

R3

****

no ip http server

ipv6 router rip ersen

gatekeeper

shutdown

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

end

EK-6 6TO4 AĞININ YAPILANDIRMASI

****

R1

****

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
boot-start-marker
boot-end-marker
no aaa new-model
ip subnet-zero
no ip domain lookup
ip domain name lab.local
ip cef
ipv6 unicast-routing
interface Tunnel0
no ip address
```

EK-6 (Devam) 6to4 ağının yapılandırması

R1

****

no ip redirects

ipv6 address 2002:C0A8:201::/128

tunnel source 192.168.2.1

tunnel mode ipv6ip 6to4

interface FastEthernet0/0

no ip address

shutdown

duplex half

interface Serial1/0

ip address 192.168.2.1 255.255.255.0

serial restart-delay 0

interface Serial1/1

no ip address

shutdown

serial restart-delay 0

interface Serial1/2

EK-6 (Devam) 6to4 ağının yapılandırması

R1

****

no ip address

shutdown

serial restart-delay 0

interface Serial1/3

no ip address

shutdown

serial restart-delay 0

interface Serial1/4

no ip address

shutdown

serial restart-delay 0

interface Serial1/5

no ip address

shutdown

serial restart-delay 0

interface Serial1/6

EK-6 (Devam) 6to4 ağının yapılandırması

R1

****

no ip address

shutdown

serial restart-delay 0

interface Serial1/7

no ip address

shutdown

serial restart-delay 0

interface FastEthernet2/0

no ip address

duplex auto

speed auto

ipv6 address 2001:DB8:0:1::2/64

ipv6 enable

interface FastEthernet2/1

no ip address

shutdown

EK-6 (Devam) 6to4 ağının yapılandırması

R1

****

duplex auto

speed auto

router ospf 1

router-id 10.10.10.10

log-adjacency-changes

network 0.0.0.0 255.255.255.255 area 0

ip classless

no ip http server

ipv6 route 2001:DB8:0:1::/64 2002:C0A8:303::

ipv6 route 2001:DB8:0:2::/64 2002:C0A8:303::

ipv6 route 2002::/16 Tunnel0

gatekeeper

shutdown

line con 0

exec-timeout 0 0

privilege level 15

EK-6 (Devam) 6to4 ağının yapılandırması

R1

****

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

login

end

EK-7 6to4 ağının yapılandırması

R2

****

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

EK-7 (Devam) 6to4 ağının yapılandırması

R2

****

```
no service password-encryption
hostname R2
boot-start-marker
boot-end-marker
no aaa new-model
ip subnet-zero
no ip domain lookup
ip domain name lab.local
ip cef
interface FastEthernet0/0
no ip address
shutdown
duplex half
interface Serial1/0
ip address 192.168.2.2 255.255.255.0
serial restart-delay 0
```

EK-7 (Devam) 6to4 ağının yapılandırması

R2

****

```
interface Serial1/1
ip address 192.168.3.2 255.255.255.0
serial restart-delay 0
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
interface Serial1/4
no ip address
shutdown
serial restart-delay 0
interface Serial1/5
```

EK-7 (Devam) 6to4 ağının yapılandırması

R2

****

no ip address

shutdown

serial restart-delay 0

interface Serial1/6

no ip address

shutdown

serial restart-delay 0

interface Serial1/7

no ip address

shutdown

serial restart-delay 0

router ospf 1

router-id 20.20.20.20

log-adjacency-changes

network 0.0.0.0 255.255.255.255 area 0

ip classless

EK-7 (Devam) 6to4 ağının yapılandırması

R2

****

```
no ip http server
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
end
```

EK-8 6to4 ağının yapılandırması

R3

****

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname R3

boot-start-marker

boot-end-marker

no aaa new-model

ip subnet-zero

no ip domain lookup

ip domain name lab.local

ip cef

ipv6 unicast-routing

interface Tunnel0

no ip address

no ip redirects

EK-8 (Devam) 6to4 ağının yapılandırması

R3

****

ipv6 address 2002:C0A8:303::/128

tunnel source 192.168.3.3

tunnel mode ipv6ip 6to4

interface FastEthernet0/0

no ip address

shutdown

duplex half

interface Serial1/0

ip address 192.168.3.3 255.255.255.0

serial restart-delay 0

interface Serial1/1

no ip address

shutdown

serial restart-delay 0

interface Serial1/2

no ip address

EK-8 (Devam) 6to4 ağının yapılandırması

R3

****

```
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
interface Serial1/4
no ip address
shutdown
serial restart-delay 0
interface Serial1/5
no ip address
shutdown
serial restart-delay 0
interface Serial1/6
no ip address
shutdown
serial restart-delay 0
```

EK-8 (Devam) 6to4 ağının yapılandırması

R3

****

interface Serial1/7

no ip address

shutdown

serial restart-delay 0

interface FastEthernet2/0

no ip address

duplex auto

speed auto

ipv6 address 2001:DB8:0:2::2/64

ipv6 enable

interface FastEthernet2/1

no ip address

shutdown

duplex auto

speed auto

interface Ethernet3/0

EK-8 (Devam) 6to4 ağının yapılandırması

R3

****

no ip address

shutdown

duplex half

interface Ethernet3/1

no ip address

shutdown

duplex half

interface Ethernet3/2

no ip address

shutdown

duplex half

interface Ethernet3/3

no ip address

shutdown

duplex half

interface Ethernet3/4

EK-8 (Devam) 6to4 ağının yapılandırması

R3

****

no ip address

shutdown

duplex half

interface Ethernet3/5

no ip address

shutdown

duplex half

interface Ethernet3/6

no ip address

shutdown

duplex half

interface Ethernet3/7

no ip address

shutdown

duplex half

router ospf 1

EK-8 (Devam) 6to4 ağının yapılandırması

R3

****

router-id 30.30.30.30

log-adjacency-changes

network 0.0.0.0 255.255.255.255 area 0

ip classless

no ip http server

ipv6 route 2001:DB8:0:1::/64 2002:C0A8:201::

ipv6 route 2002::/16 Tunnel0

gatekeeper

shutdown

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

exec-timeout 0 0

privilege level 15

EK-9 ISATAP AĞININ YAPILANDIRMASI

****

R1

****

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
boot-start-marker
boot-end-marker
no aaa new-model
ip subnet-zero
no ip domain lookup
ip domain name lab.local
ip cef
ipv6 unicast-routing
interface Loopback1
 no ip address
```

EK-9 ISATAP(Devam) ağının yapılandırması

R1

****

```
interface Tunnel0
no ip address
 no ip redirects
 ipv6 address 2002:DB8:BCF:123::/64 eui-64
 no ipv6 nd suppress-ra
 tunnel source 192.168.1.1
 tunnel mode ipv6ip isatap
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex half
interface FastEthernet1/0
 no ip address
 duplex half
 ipv6 address 2001:DB8:0:1::2/64
 ipv6 enable
router ospf 1
```

EK-9 ISATAP(Devam) ağının yapılandırması

****

R1

****

```
router-id 10.10.10.10
 log-adjacency-changes
network 0.0.0.0 255.255.255.255 area 0
ip classless
no ip http server
ipv6 route 2001:DB8:0:2::/64 2002:DB8:BCF:123:0:5EFE:C0A8:203
ipv6 route 2002::/16 Tunnel0
ipv6 router rip ersen
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
```

EK-9 ISATAP(Devam) ağının yapılandırması

R1

****

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

login

end

EK-10 ISATAP ağının yapılandırması

R2

****

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname R2

EK-10 (Devam) ISATAP ağının yapılandırması

R2

****

boot-start-marker

boot-end-marker

no aaa new-model

ip subnet-zero

no ip domain lookup

ip domain name lab.local

ip cef

interface FastEthernet0/0

ip address 192.168.1.2 255.255.255.0

duplex half

interface FastEthernet1/0

ip address 192.168.2.2 255.255.255.0

duplex half

router ospf 1

router-id 20.20.20.20

log-adjacency-changes

EK-10 (Devam) ISATAP ağının yapılandırması

R2

****

network 0.0.0.0 255.255.255.255 area 0

ip classless

no ip http server

gatekeeper

shutdown

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

login

end

EK-11 ISATAP ağının yapılandırması

R3

****

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname R3

boot-start-marker

boot-end-marker

no aaa new-model

ip subnet-zero

no ip domain lookup

ip domain name lab.local

ip cef

ipv6 unicast-routing

interface Loopback1

EK-11(Devam) ISATAP ağının yapılandırması

R3

****

```
no ip address
interface Tunnel0
no ip address
no ip redirects
ipv6 address 2002:DB8:BCF:123::/64 eui-64
no ipv6 nd suppress-ra
tunnel source 192.168.2.3
tunnel mode ipv6ip isatap
interface FastEthernet0/0
ip address 192.168.2.3 255.255.255.0
duplex half
interface FastEthernet1/0
no ip address
duplex half
ipv6 address 2001:DB8:0:2::2/64
ipv6 enable
```

EK-11(Devam) ISATAP ağının yapılandırması

R3

****

```
router ospf 1
router-id 30.30.30.30
log-adjacency-changes
network 0.0.0.0 255.255.255.255 area 0
ip classless
no ip http server
ipv6 route 2001:DB8:0:1::/64 2002:DB8:BCF:123:0:5EFE:C0A8:101
ipv6 route 2002::/16 Tunnel0
ipv6 router rip ersen
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
```

EK-11(Devam) ISATAP ağının yapılandırması

R3

****

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

login

end

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı: HAMEED, Arsan Adnan Hameed

Uyruğu: IRAK

Doğum tarihi ve yeri: 08.10.1987 Kerkük

Medeni hali: Bekâr

E-mail: ersenadnan@yahoo.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	Kerkük üniversitesi/ Bilgisayar Bilimleri	2009
Lise	El-Sadır Fen Lisesi	2005

Yabancı Dil

İngilizce, Arapça

Yayınlar

1. Erdem, A. & Hameed, A, "Sanal Altyapı Ortamında Farklı İşletim Sistemi Kullanarak IPv4 ve IPv6 Performans Değerlendirmesi", ***Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi***, (basımda), (2013).

Hobiler

Bilgisayar teknolojileri, futbol, seyahat, yüzmek