T. C.
ERCİYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

IPv4 AĞLARININ IPv6 AĞLARINA ENTEGRASYONU VE IPv6'DA FARKLI YÖNLENDİRME PROTOKOLLERİNİN BAŞARIMI

Tezi Hazırlayan
Mevlüt DOĞRU

Tezi Yöneten
Yrd. Doç. Dr. Mustafa DANACI

Bilgisayar Mühendisliği Anabilim Dalı
Yüksek Lisans Tezi

Temmuz 2010
KAYSERİ

Yrd. Doç. Dr. Mustafa DANACI danışmanlığında **Mevlüt DOĞRU** tarafından hazırlanan **"IPv4 Ağlarının IPv6 Ağlarına Entegrasyonu ve IPv6'da Farklı Yönlendirme Protokollerinin Başarımı"** adlı bu çalışma, jürimiz tarafından Erciyes Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalında **Yüksek Lisans** tezi olarak kabul edilmiştir.

02/07/2010

JÜRİ:

Başkan : Doç. Dr. Nurhan KARABOĞA

Üye : Yrd. Doç. Dr. Mustafa DANACI

Üye : Yrd. Doç. Dr. Serkan ÖZTÜRK

ONAY:

Bu tezin kabulü, Enstitü Yönetim Kurulunun 13/07/2010 tarih ve 2010/23-02 sayılı kararı ile onaylanmıştır.

13/.07/ 2010

Prof. Dr. Nusret AYYILDIZ
Enstitü Müdürü

TEŞEKKÜR

Tecrübeleri ve bilgileri ile bana yol gösteren değerli hocam Sayın Yrd. Doç. Dr. Mustafa DANACI ve Bilgisayar Mühendisliği Bölümü hocalarıma, tez çalışmamda yardımlarını esirgemeyen kıymetli arkadaşım Öğr. Gör. Hamdi ERCAN'a, maddi manevi destekleri ile her zaman yanımda olan, sevgi, saygı ve minnet sözcüklerinin yetersiz kaldığı sevgili aileme ve tüm dostlarıma teşekkürlerimi sunuyorum.

IPv4 AĞLARININ IPv6 AĞLARINA ENTEGRASYONU VE IPv6'DA FARKLI YÖNLENDİRME PROTOKOLLERİNİN BAŞARIMI

Mevlüt DOĞRU

Erciyes Üniversitesi, Fen Bilimleri Enstitüsü
Yüksek Lisans Tezi, Temmuz 2010
Tez Danışmanı: Yrd. Doç. Dr. Mustafa DANACI

ÖZET

Bir ağ iletişim protokolü olan IP'nin ilk versiyonu (sürüm) IPv4, 32 bit uzunluğunda olup 4 milyarın üzerinde bilgisayarı adreslemeyi mümkün kılmaktadır. İnternetin 1990'lı yıllardan sonra hızla gelişmesi sonucu IPv4'ün yapısal ve adresleme alanı olarak yetersiz kalmaya başlaması, IP adreslerinin verimli bir şekilde kullanılmaması gibi nedenler, geniş adres aralığı ihtiyacını doğurmuştur. Bu sebeple, 128 bit uzunluğuna sahip bir protokol olan IPv6 geliştirilmiş ve son yıllarda IPv6'ya geçiş çalışmalarına başlanmıştır. Mevcut IPv4 altyapısı üzerinde başarılı bir şekilde gerçekleştirilen yönlendirme işlemi, IPv6'daki adres girdisinin artmasından dolayı yönlendirme tablolarındaki boyutun artması ve 128 bit uzunluğundaki IPv6'nın IPv4'e göre daha fazla işlem gerektirmesi, yönlendirme işleminin önemini ortaya koymaktadır.

Bu tez çalışmasında, IPv6'nın genel özellikleri ve IPv4'ten IPv6'ya geçiş yöntemleri incelenerek modellenen örnek bir ağ üzerinde çift yığın yönteminin benzetimi Cisco Packet Tracer (CPT) programı aracılığıyla gerçekleştirilmiştir. Ayrıca, IPv6 ağlarında kullanılan yönlendirme protokolleri incelenerek, bilgisayar ortamında modellenen ağaç, halka, yıldız topolojileri ve karmaşık bir ağ yapısı üzerinde farklı IPv6 yönlendirme protokollerinin performans analizleri yapılması amaçlanmıştır. Bunun için CPT benzetim programı aracılığıyla modellenen farklı ağlar üzerinde ortalama paket gecikme süreleri ve ortalama veri transfer hızları performans kriteri olarak değerlendirilip; RIPng, OSPFv3, EIGRPv6 ve statik yönlendirme protokollerinin kıyaslamaları yapılarak performansları analiz edilmiştir.

Modellenen ağ üzerindeki benzetim sonuçları doğrultusunda karşılaştırılan yönlendirme protokollerinin paket gecikmesi ve veri transfer hızı performans kriteri olarak değerlendirildiğinde en uygun IPv6 yönlendirme protokolü olan OSPFv3 önerilmiştir.

Anahtar Kelimeler: IPv4, IPv6, yönlendirme protokolleri, OSPFv3, IPv4'ten IPv6'ya geçiş teknikleri.

THE INTEGRATION OF IPv4 NETWORKS INTO IPv6 AND PERFORMANCE OF DIFFERENT ROUTING PROTOCOLS IN IPv6

Mevlüt DOĞRU

Erciyes University, Graduate School of Natural and Applied Sciences
M. Sc. Thesis, July 2010
Thesis Supervisor: Assist. Prof. Dr. Mustafa DANACI

ABSTRACT

The first version of IP, a communication network protocol, is IPv4 which is 32 bit length and makes possible to address over 4 billion computers. As a result of Internet's developing rapidly after 1990s, vast address distance has been needed because of causes like IPv4's structural and addressing size being insufficient, IP's addresses not being used efficiently. Therefore, 128 bit length IPv6 protocol has been developed and in recent years transition studies have been made into IPv6. As a result of increasement in IPv6 address input, increasement in routing tables size and 128 bit length IPv6 requiring more transactions compared to IPv4, reveals the importance of routing transaction that is successfully implemented in existing IPv4 infrastructure.

In this thesis study, by investigating and modelling the general characteristics of IPv6 and the transition methods from IPv4 to IPv6, simulation of dual stack technique in a network modeled by means of the Cisco Packet Tracer (CPT) simulation program. Also, it is aimed to make performance analysis of different IPv6 routing protocols in a network which has tree, ring, star topologies and a complex structure, modeled in computer environment by investigating the routing protocols used in IPv6 networks. For this purpose, different IPv6 networks have been modeled by means of the CPT simulation program that the performance analysis of RIPng, OSPFv3, EIGRPv6 and static routing protocols has been compared by assessing the average of package delay times and data transfer rates as a performance criteria.

When it is assessed that performance criterias which is known package delay time and data transfer rate, the routing protocols are compared according to the results of simulations on modeled network, the most convenient IPv6 routing protocol which is OSPFv3 has been suggested.

Keywords: IPv4, IPv6, routing protocols, OSPFv3, IPv4 to IPv6 transition techniques.

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

1. BÖLÜM

GİRİŞ

IP (Internet Protocol – İnternet Protokol), 1981 yılından itibaren kullanılmaya başlanmış olup, adres yapılandırması ve yönlendirme esnekliği sağlayan bir ağ protokolüdür. IP'nin ilk versiyonu olan IPv4 (Internet Protocol version 4 – İnternet Protokol Versiyon 4), kolay uygulanabilirlik, güçlü protokol yapısı ve ortak çalışmayı destekleme gibi bazı özelliklere sahip olup, günümüze kadar önemli ölçüde bir değişikliğe uğramadan süregelmiştir. IPv4 adresi 32 bit uzunluğuna sahip olmanın yanı sıra yaklaşık olarak 4 milyarın üzerinde adresleme yapmayı mümkün kılmaktadır. Ama günümüz teknolojisine paralel olarak 1990'lı yılların başında internetin hızla gelişmesiyle birlikte 4 milyar adres yetersiz kalmaya başlamıştır. İnternet standartlarının belirlendiği uluslararası bir organizasyon olan IETF (Internet Engineering Task Force – İnternet Mühendislik Görev Gücü) tarafından yapılan çalışmalar, 2008 ile 2018 yılları arasında mevcut IP adreslerinin tükeneceğini göstermektedir. Adres alanının yetersiz olması, adreslerin mimarileri nedeniyle verimli bir şekilde kullanılamaması ve güvenlik seviyesinin artırılması ihtiyacı gibi sebeplerden dolayı 1990'lı yılların başında IETF IPv6 WG (Internet Engineering Task Force IPv6 Work Group – İnternet Mühendislik Görev Gücü IPv6 Çalışma Grubu), yeni bir adresleme mimarisi üzerinde çalışmaya başlamıştır [1-6].

Adres aralığının artırılmasına en çok Uzak Doğu ülkelerinde, özellikle de Çin'de gereksinim duyulmaktadır. Çin, sahip oldukları mevcut adreslerin 1/7'sini kullanmaktadır. Fakat yaklaşık olarak 1,5 milyar nüfusa sahip olan bu ülkede bütün öğrencilere (320 milyon adet) birer tane IP adresi dağıtılması durumunda, bütün adreslerin 1/4'ü gibi büyük bir miktarının sadece bu işe tahsis edilmesi gerekecektir [7,8]. Bu oranlar ise adres sayısının artırılması gerektiğini açıkça göstermektedir.

Yeni internet erişim protokolü için öncelikle IP “next generation” (Yeni Nesil Internet Protokolü) ismi düşünülmüştür. Fakat daha sonra IP’lere versiyon numarası verme fikri oluşmuş ve bunun üzerine, laboratuarlarda bir test protokolü olarak kullanılan ST2 (Internet Stream Protocol, version 2 – İnternet Akış Protokol, versiyon 2) Protokol’ü IPv5 (IP version 5 – IP versiyon 5), yeni IP ise IPv6 (IP version 6 – IP versiyon 6) olarak adlandırılmıştır. Deneysel bir protokol olan ST2’ye, IPv5 ismi verilerek “RFC (Request For Comments – Yorumlamak İçin İstek) 1819” dokümanında tanımlanmıştır. Bu yüzden yeni IP, IPv5 yerine IPv6 olarak adlandırılmıştır. IPv6 için ilk öneriler 1992 yılında IETF tarafından yapılmış, 1994 yılında da IPv6 adres yapısı için son tasarım oluşturulmuştur. Yeni protokolün tasarlanması üzerine birçok çalışma yapılmıştır. Günümüzde ise IPv4’ten IPv6’ya geçiş süreci başlamış ve bu süreç farklı ülkelerde farklı aşamalarda olduğundan, geçiş tamamlanıncaya kadar IPv4 ve IPv6’nın birlikte kullanılacağı bilinmektedir [1,2,9].

IP paketlerinin bulunduğu ağın dışındaki bir ağa gönderilebilmesi için ilgili ağa yönlendirilmesi gerekmektedir. Yönlendirme işlemi, bu işlemin kurallar kümesini içeren yönlendirme protokolleri doğrultusunda, yönlendirici (router) ağ cihazları aracılığıyla gerçekleştirilir [10-12]. IP yönlendirme, IPv4 protokolü için genel bir sorun olmamakla birlikte, IPv6 protokolü bazı problemleri beraberinde getirmektedir. Bu problemler aşağıdaki gibi sıralanabilir [10].

- İnternet kullanımının yaygınlaşmasıyla birlikte, günümüzde yönlendiricilerin kullanmış olduğu 40.000 ile 50.000 civarında adres girdisi içeren yönlendirme tabloları, yakın bir zamanda 250.000 ile 500.000 arasında adres girdisi içeren yönlendirme tabloları durumuna gelecektir.
- 128 bit uzunluğa sahip IPv6 adresleri, IPv4 adreslerinden dört kat daha uzundur. IPv4’te yönlendirici yazılım ve donanımları 32 bit işlemci, 32 bit veri yolu erişimi ve 32 bit hafıza erişimi kullanır. 128 bit uzunluğundaki IPv6 verisi ile işlem yapabilmek için donanımın geliştirilmesi ve bu donanım üzerinde çalışan mevcut yazılımlar için daha fazla işlem gerekmektedir.

IPv6’ya geçişle birlikte protokolün hızlı bir şekilde yaygınlaşması ve beklentilere cevap verebilmesi için, en önemli aşamalardan biri olan yönlendirme işlemi problemsiz bir biçimde gerçekleştirilmelidir. Mevcut altyapı üzerinde başarılı bir şekilde

gerçekleştirilen yönlendirme işleminin genişleyecek olan veri boyutu dikkate alındığında yetersiz kalabileceğinden dolayı yeni algoritmaların geliştirilmesi ihtiyacı doğmaktadır [13-15].

Son yıllardaki IPv6 üzerine yapılan başarılı çalışmalar sonucunda, IPv6'nın yönlendirme işlemini IPv4'ten hem daha hızlı hem de işlem ve hafıza kullanımı bakımından daha verimli bir şekilde yapabildiği tespit edilmiştir [16,17]. Benzer şekilde, Üstündağ'ın yüksek lisans tez çalışmasında IPv4 ve IPv6'nın yönlendirme performansları OPNET ağ benzetim (simülasyon) programında kıyaslanarak, RIP (Routing Information Protocol – Yönlendirme Bilgisi Protokolü) yönlendirme protokolü kullanıldığında IPv6'daki veri indirme hızının daha iyi olduğu ve paket gecikmelerinin de daha kısa olduğu belirtilmiştir [18]. Diğer bazı çalışmalarda ise yönlendirme protokollerinin IPv4 ve IPv6 versiyonlarının kıyaslama çalışmaları gerçekleştirilerek [19-23], IPv6 yönlendirme protokolleri üzerine uygunluk ve verimlilik testleri yapılmıştır [20,24,25]. Bazı araştırmacılar da yönlendirme protokollerinin IPv4 ve IPv6 versiyonlarını güvenlik açısından incelemiştir [22,26]. Literatür taramasında IPv4 için çeşitli benzetim programlarında yönlendirme protokolleri analizi yapılmasına karşın IPv6 yönlendirme protokolleri için daha az çalışmanın bulunduğu görülmüştür.

Bu tez çalışmasında, günümüzde kullanılan adresleme protokolü olan IP'nin mevcut versiyonu IPv4 ve yeni versiyonu IPv6 arasındaki geçiş yöntemleri incelenerek, modellenen örnek bir ağ üzerinde çift yığın (dual stack) yönteminin benzetimi CPT (Cisco Packet Tracer) 5.2 programı aracılığıyla gerçekleştirilmiştir. Benzer şekilde CPT 5.2 ile bilgisayar ortamında modellenen ağaç (tree), halka (ring), yıldız (star) topolojileri ve karmaşık bir ağ yapısı üzerinde IPv6 yönlendirme protokolleri test edilerek kendi aralarındaki performansları karşılaştırılmıştır. Bu benzetim sonuçları değerlendirilip IPv6 yönlendirme protokollerinin seçimi için öneriler sunulmuştur.

Tez çalışmasının ikinci bölümünde, IPv6 protokolünün yapısı, yenilikleri, adresleme mimarisi, kontrol mesaj protokolü ve komşu keşfi incelenerek IPv4 ve IPv6 protokollerinin kısa bir karşılaştırılması yapılmıştır.

Üçüncü bölümde, IPv4'ten IPv6'ya geçişi mümkün kılan yöntemler hakkında temel bilgiler verilmiştir. Ayrıca IPv6'nın birçok ülkelerdeki kullanım durumu hakkında bilgi verilmiştir.

Dördüncü bölümde, IP yönlendirme algoritmaları ve yönlendirme protokolleri incelenerek, IPv6'da kullanılan yönlendirme protokolleri hakkında detaylı bilgiler verilmiştir.

Beşinci bölümde, IPv4'ten IPv6'ya geçiş yöntemlerinden olan çift yığın yönteminin benzetimi modellenen örnek bir ağ üzerinde CPT programı aracılığıyla gerçekleştirilmiştir. Benzer şekilde CPT benzetim programı kullanılarak modellenen ağaç, halka, yıldız topolojileri ve karmaşık bir ağ yapısı üzerinde, IPv6'da kullanılan farklı yönlendirme protokolleri benzetim sonuçları değerlendirilerek performansları analiz edilmiştir.

Sonuç bölümünde ise elde edilen sonuçlar değerlendirilerek en uygun IPv6 yönlendirme protokolü önerilmiş ve gelecekte yapılması planlanan çalışmalar verilmiştir.

2. BÖLÜM

YENİ NESİL İNTERNET PROTOKOLÜ

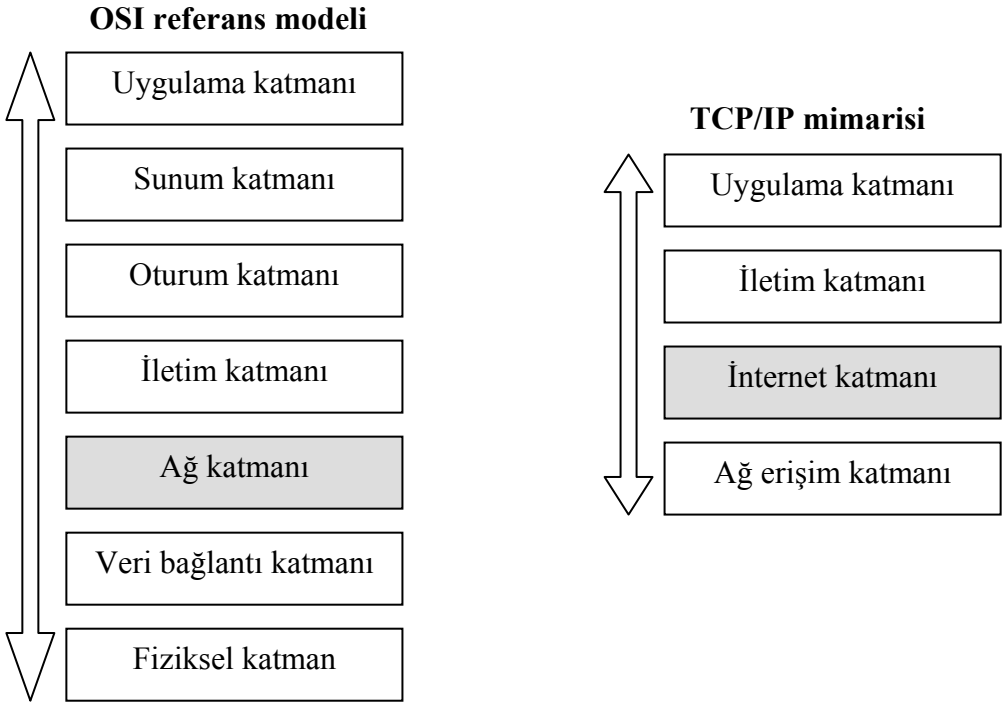
2.1. İnternet Protokolü

1983 yılında askeri birimlerin bugünkü internetin temeli olan ARPAnet'ten (Advanced Research Projects Agency Network – Gelişmiş Araştırma Projeleri Acente Ağı) TCP/IP (Transmission Control Protocol/Internet Protocol – Taşıma Kontrol Protokol/İnternet Protokol) mimarisine geçmesiyle birlikte TCP/IP, haberleşmede kullanılan protokol haline gelmiştir. Dört farklı katmana sahip olan TCP/IP mimarisinin daha iyi anlaşılabilmesi için, ISO (International Standards Organization - Uluslararası Standartlar Organizasyonu) tarafından geliştirilmiş ve yedi farklı katmana sahip olan OSI (Open Systems Interconnection - Açık Sistem Bağlantısı) referans modeli incelenerek katmanlardaki protokollerin birbirleriyle nasıl haberleştikleri öğrenilebilir. OSI referans modeli ve TCP/IP mimarisi Şekil 2.1.'de gösterilmektedir [12].

İlk katmanı uygulama katmanı olan TCP/IP'nin ikinci katmanı ise iletim katmanıdır. Bu katman, TCP (Transmission Control Protocol – Taşıma Kontrol Protokol) ve UDP (User Datagram Protocol – Kullanıcı Veri Bloğu Protokolü) protokollerini içerir. TCP/IP'nin üçüncü katmanı olan internet katmanı, ağ içerisinde en iyi yolu bulup, paketlerin iletilmesini sağlayan katmandır. Bu katmanda bulunan IP, bir paket ve adresleme yapısı belirleyip veriyi internet katmanından TCP/IP'nin dördüncü katmanı olan ağ erişim katmanına gönderir ve paketleri diğer cihazlara yönlendirir. IP, aynı zamanda OSI referans modelinin beşinci katmanı olan ağ katmanında bulunmaktadır [12].

IP, IETF belgelerinden RFC 791 standardında tanımlanmıştır. IP birbirine bağlı sistemler içerisinde kullanılmak üzere paket anahtarlamalı bilgisayar iletişim ağları

oluşturmak için tasarlanmıştır. Bu protokol, belirli bir adres atanmış kaynak bilgisayarlardan hedefe doğru veri bloğu geçişini sağlamaktadır [27]. Ayrıca, verilerin aktarılması esnasında atlama noktalarında herhangi bir veri kontrol sistemi bulunmadığından güvenilir olmayan bir protokoldür. İletim sırasında kaybolan paketin yeniden iletimi gerçekleştirilmemektedir.

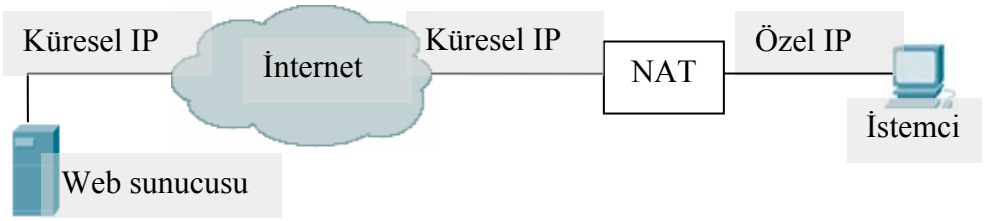


Şekil 2.1. OSI referans modeli ve TCP/IP mimarisi**.**

2.1.1. IPv6 Protokolü

İnternetin sürekli gelişimi sonucu IPv4 adres kullanımının artması ve internetteki ana sunucu (host) sayısının artmasına bağlı olarak gelecek on yıl içerisinde IPv4 adres alanının yeterli olmayacağı öngörülmektedir. IPv4 adreslerinin tükenmesiyle birlikte yeni kullanıcıların internete bağlanması imkânsız olacaktır [28]. IPv4 adreslerindeki bu sorunu çözebilmek için 1993 yılında CIDR (Classless Inter Domain Routing - Sınıfsız Alanlar Arası Yönlendirme) yöntemi geliştirilmiştir. Bu yöntemde temel amaç IPv4'te kullanılan sınıfsal adres dağıtımını kaldırarak IP adreslerini daha verimli bir şekilde kullanmaktır. Dağıtılmış olan IPv4 adresleri ve internete bağlanan cihazların artışı nedeniyle CIDR yöntemi başarılı olsa bile tam bir çözüm olamamıştır [29].

IPv4 adreslerini çözmek için geliştirilen diğer bir metot ise NAT (Network Address Translation - Ağ Adres Dönüşümü) olarak bilinen RFC 1597 ile RFC 1918'de tanımlanmış bir yöntemdir. Bu yöntemin çalışma prensibi, ağ içerisindeki adreslere özel IP adresleri vererek ağ dışına yönlendirilmesini engellemek ve internete çıkarken NAT protokolü sayesinde küresel (global) bir adres eşleştirmesi sağlamaktır. Şekil 2.2.'de özel IP adresli bir istemcinin (client) internetteki web sunucusu (server) ile NAT protokolü üzerinden haberleşmesi gösterilmektedir. Bu şekilde adres tasarrufu sağlanmaya çalışılmış fakat yetersiz kalınmıştır [12,30]. İnternetteki tahmin edilen çok büyük gelişmeler için 32 bit adres alanı olan IPv4 protokolü yeterli olamayacağından, 1996 yılında IPv6 protokolü yayımlanmıştır [28].



Şekil 2.2. NAT örneği.

128 bitten oluşan IPv6'nın getirdiği daha büyük adres alanıyla birlikte NAT ve CIDR gibi yöntemlere ihtiyaç duyulmayacaktır. IPv4'ten IPv6'ya geçişin temel nedenleri aşağıdaki gibi sıralanabilir [31].

- Kullanıcı sayısının artmasıyla birlikte IPv4 adreslerinin yetersiz kalması,
- Bilgisayar ağlarında yapılandırmayı basitleştirme ihtiyacı,
- Güvenlik seviyesinin artırılma ihtiyacı,
- IPv4'teki Hizmet Kalitesini (Quality of Service – QoS) iyileştirme ihtiyacı.

2.1.2. IPv6'nın Genel Özellikleri

IPv6 protokolünün getirdiği yenilikler ve genel özellikleri aşağıdaki gibi incelenebilir.

Tümleşik güvenlik: IPSec protokolü IPv6'da tümleşik olarak gelmektedir. Böylece, ağ güvenliğinin sağlanabilmesi için belirli standartlara dayalı çözüm sunulmuştur [31].

Hizmet kalitesi: IPv6 paket başlığındaki akış etiketi alanı kullanılarak hedef ve kaynak arasındaki paketler dizisinin tanınma imkânı sunulmaktadır. IPv6'nın bu özelliği sayesinde trafik akışı IPv6 paket başlığında tanımlandığından dolayı IPSec ile şifrelenmiş veri taşıyan paketlerle ilgili sorunda çözülmektedir [31].

Genişletilmiş adres alanı: 32 bit olan IPv4 adreslerinin büyüklüğü IPv6'da 128 bittir. IPv6 ile birlikte, bilgisayarlar arasında yüksek kalitede yol oluşturulup veri paketlerini buradan ileterek performanslı bir şekilde ses ve görüntü iletimi gerçekleştirilebilir [5].

Genişletilebilirlik: IPv6 ile birlikte bu protokolün temel başlığının yanında ek başlık ortaya çıkmıştır. Bu ek başlık gerek duyulmadığı takdirde hiç kullanılmayabilir kullanıldığında ise bilgi, IPv4'tekine göre daha az paket boyutuyla sağlanmaktadır [5].

Yeni başlık formatı: IPv6 başlığı basitleştirilerek işlem yükü azaltılmıştır. IPv4 başlığının neredeyse tamamı değiştirilmiştir. IPv4 ve IPv6 paketleri birbirleriyle uyumsuz olduğundan dolayı, bir sistemin iki başlık formatını da kullanabilmesi için hem IPv4 hem de IPv6 protokolünü birlikte kullanması gerekmektedir [5,32].

Durum bilgisi olan ve durum bilgisi olmayan adres yapılandırması: IPv6 protokolü durum bilgisi olan ve durum bilgisi olmayan olmak üzere iki tür otomatik adreslendirme yöntemi kullanmaktadır. Durum bilgisi olan yapılandırmada, istemciler yönlendirici mesaj bilgisiyle IP adreslerini alabilecekleri DHCP (Dynamic Host Configuration Protocol - Dinamik İstemci Yapılandırma Protokolü) ana bilgisayarlarını öğrenir. Sonrasında DHCPv6 (DHCP version 6) ana bilgisayarları ile bağlantıya geçerek gerekli adres bilgisi alınır. Durum bilgisi olmayan yapılandırmada ise istemciler bağlı oldukları yönlendiricilerden önekleri (prefix) alarak IP adreslerini oluştururlar. İstemciler, yönlendirici olmadığında bile kendilerini yerel adreslerle otomatik olarak yapılandırarak el ile yapılandırmaya gerek kalmadan iletişim kurabilirler [32].

Mobil cihaz desteği: IPv6'da mobil cihazlar ne ek protokol ne de yönlendirici desteğine gerek kalmadan bir ağdan diğerine adres değişikliği olmaksızın geçiş yapabilirler. Bu yüzden IPv6, mobil uygulamalar için uygun bir platformdur [33].

2.1.3. IPv4 ve IPv6 Protokollerinin Karşılaştırılması

IPv4 ve IPv6 protokollerinin temel özelliklerinin kıyaslanması Tablo 2.1.'de verilmiştir.

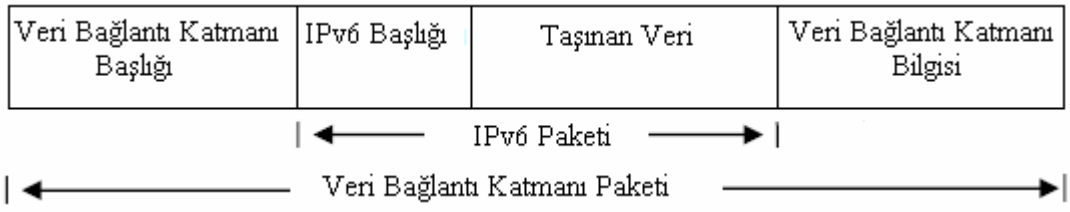
Tablo 2.1. IPv4 ile IPv6'nın karşılaştırılması [32].

IPv4	IPv6
Hedef ve kaynak adresler 32 bit (4 bayt)	Hedef ve kaynak adresler 128 bit (16 bayt)
IPSec desteği isteğe bağlı	IPSec desteği gerekli
El ile veya DHCP ile adres yapılandırması yapılmalı	El ile veya DHCP ile yapılandırmaya gerek yok
Veri parçalaması (fragmentation) hem yönlendiricilerde hem de ana sunucularda yapılır	Parçalama sadece ana sunucularda yapılır
Parçalanma olabilen 576 baytlık paket büyüklüğünü destekler	Parçalanma olmadan 1280 baytlık paket büyüklüğünü destekler
Opsiyonel veriler başlık içerisinde	Opsiyonel veriler uzantı başlıkları içerisinde
Veri Bağlantı Katmanı (Data Link Layer) adresiyle IP adresi eşleştirmesi için ARP (Address Resolution Protocol - Adres Çözme Protokolü) kullanılır	ARP yerine Komşu Sorgulama mesajları (Neighbor Solicitation messages - NS) kullanılır
Alt ağ (subnet) grup üyeliğini yönetmek için IGMP (Internet Group Managment Protocol - İnternet Grup Yönetim Protokolü) kullanılır	IGMP yerine Çoğa Gönderim Dinleyici Keşif mesajları (Multicast Listener Discovery messages - MLD) getirilmiş
En iyi varsayılan IPv4 ağ geçidini bulmak için isteğe bağlı olan ICMP (Internet Control Message Protocol – İnternet Kontrol Mesaj Protokolü) Yönlendirici Keşif protokolü kullanılır	ICMP Yönlendirici Keşif protokolünün yerine ICMPv6, Yönlendirici Sorgulama (Router Solicitation - RS) ve Yönlendirici Cevap (Router Advertisement - RA) mesajları geliştirilmiş
Bir mesajı alt ağdaki tüm düğümlere göndermek için yayın (broadcast) adresi kullanılır	Yayın adresi yerine yerel-bağlantı alanı tüm-düğümler çoklu gönderim (link-local scope all-nodes multicast) adresleri kullanılır
Paket başlığında akış etiketi yok	Paket başlığında akış etiketi var
Başlık sağlama toplamı (checksum) alanı var	Başlık sağlama toplamı alanı içermez

2.2. Ağ İletim Ortamında IPv6 Paketi

IPv6, OSI referans modeline göre üçüncü katman olan ağ katmanında yer almaktadır. IPv6 paketleri oluşturulduktan sonra ikinci katman olan veri bağlantı katmanına gönderilmektedir. Bu katmanda IPv6 paketleri kendi katman paketleri içerisine

yerleştirilmektedir. Bu işleme de sarmalama (encapsulation) adı verilmektedir. Veri bağlantı katmanındaki IPv6 paket yapısı Şekil 2.3.'de gösterilmektedir.



Şekil 2.3. Veri bağlantı katmanındaki IPv6 paket yapısı [32].

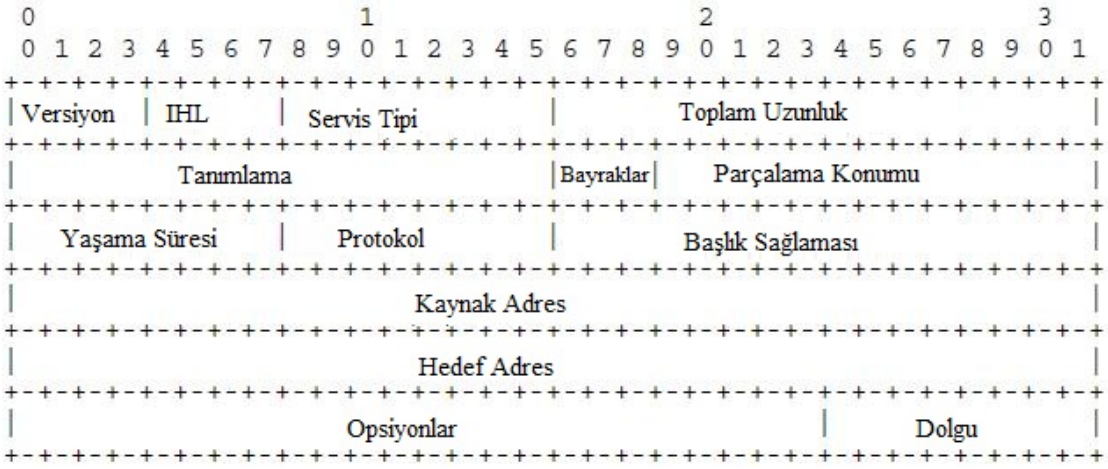
Veri bağlantı katmanında IPv6 paketlerinin başına veri bağlantı katmanı başlığı ve sonuna da veri bağlantı katmanı bilgisi eklenerek, veri bağlantı katmanı paketi oluşturulmaktadır [34].

2.3. IPv6 Başlık Yapısı

IP protokollerinde paketin başlık kısmı, yönlendirme ve paketin diğer bilgilerinden sorumludur. Bu bilgileri depolamak için tanımlanmış alanlar ve bu alanların da belirlenmiş özel değerleri vardır. Bu alanlara göre IP düğümü, paketi işlemektedir. IPv6 başlığı, IPv4 başlığında hiç kullanılmayan ve az kullanılan alanlar çıkartılarak basitleştirilmiştir. Ayrıca daha verimli iletim için yeni alanlar da eklenmiştir. IPv4 başlığında kullanılan alanlar, IPv6 başlığında uzantı başlıkları olarak tutulmaktadır. Böylece IPv6 başlığı 40 bayt ile sabitleştirilmiştir. 20 baytlık basit bir IPv4 başlığına göre 40 baytlık IPv6 başlıklı paketin işlenmesi mantıksal olarak daha zor gibi görünse bile, IPv4 paketinin daha çok alanı ve değişken boyutu olduğundan IPv6 paketlerine göre işlenmesi daha zordur [32,34].

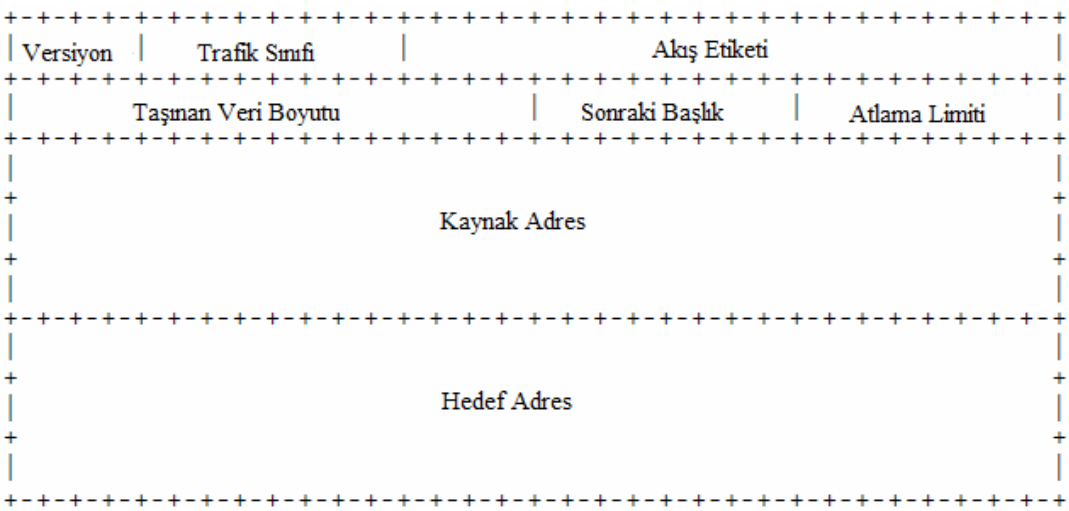
2.3.1. IPv4 ve IPv6 Başlık Yapıları

IPv4 başlık uzunluğu 20 bayt standart olmak üzere 60 bayta kadar çıkabilirken, IPv6 başlık uzunluğu 40 baytlık sabit bir başlığa ve gerek duyulduğu takdirde ilave başlıklar ile genişletilebilen bir başlık yapısına sahiptir [5]. IPv4 başlık formatı Şekil 2.4.'de, IPv6 paket başlık formatı ise Şekil 2.5.'de gösterilmektedir.



Şekil 2.4. IPv4 başlık formatı.

IPv4 paket başlığı 4 bit uzunluğunda versiyon (version) alanı, 4 bit uzunluğunda IHL (Internet Header Length - İnternet Başlık Uzunluğu) alanı, 8 bit uzunluğunda servis tipi (type of service) alanı, 16 bit uzunluğunda toplam uzunluk (total length) alanı, 16 bit uzunluğunda tanımlama (identification) alanı, 3 bit uzunluğunda bayraklar (flags) alanı, 13 bit uzunluğunda parçalama konumu (fragment offset) alanı, 8 bit uzunluğunda yaşama süresi (time to live) alanı, 8 bit uzunluğunda protokol (protocol) alanı, 16 bit uzunluğunda başlık sağlaması (header checksum) alanı, 32 bit uzunluğunda kaynak adres (source address) alanı, 32 bit uzunluğunda hedef adres (destination address) alanı, değişken uzunluğa sahip opsiyonlar (options) ve dolgu (padding) alanlarından oluşmaktadır. Opsiyonlar ve dolgu alanları kullanılmadığı takdirde IPv4 paketi en az 12 farklı alandan oluşmaktadır [27].



Şekil 2.5. IPv6 başlık formatı.

Şekil 2.5.'deki IPv6 paket başlığı içerisindeki alanlar aşağıda açıklanmaktadır [5].

Versiyon: 4 bit uzunluğunda IP'nin versiyon numarasını belirten alandır. IPv6'da bu alanın değeri 6'dır.

Trafik sınıfı (traffic class): 8 bit uzunluğunda IPv4 başlığındaki servis tipi alanının yerine getirilmiştir. IPv6 paketlerinin işlenmesi sırasında sınıf ve önem sırasını belirtir.

Akış etiketi (flow label): 20 bit uzunluğundaki bu bölüm IPv6 yönlendiricileri için paket sırasını tutmaktadır. İstemci veya yönlendirici akış etiketi alanını desteklemiyor ise bu alana sıfır değeri atanır. Paket yönlendiriliyorsa alanın değeri hiç değiştirilmeden yönlendirilir. Eğer paket alınan tarafsa bu alan ihmal edilir.

Taşınan veri boyutu (payload length): 16 bit uzunluğundaki alan, bütün uzantı başlıkları dahil olmak üzere IPv6 başlığıyla birlikte taşınan verinin boyutunu ifade etmektedir. IPv4'te bu alan toplam uzunluk alanı olarak ifade edilmektedir.

Sonraki başlık (next header): 8 bit uzunluğundaki bu alan, sonraki alanın uzantı başlık tipini veya iletim katmanı protokol tipi (TCP, UDP vb.) ile ilgili bilgiyi içermektedir.

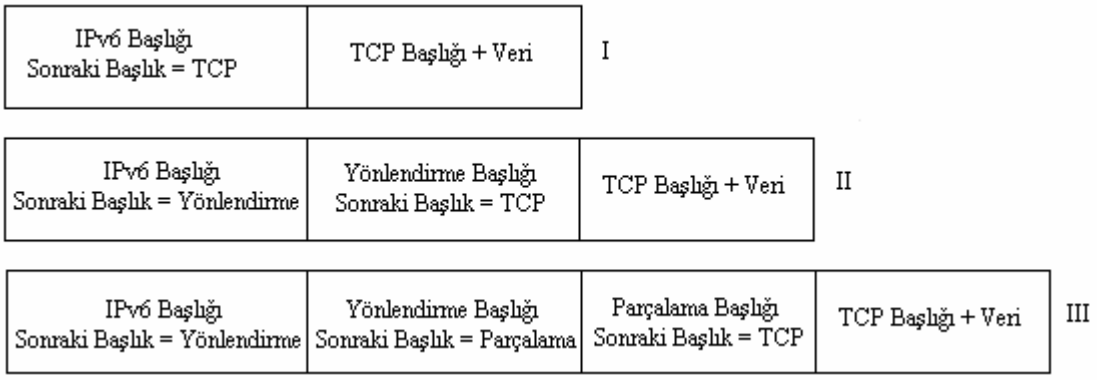
Atlama limiti (hop limit): 8 bit uzunluğundadır. IPv6 paketinin dolaşabileceği en fazla düğüm sayısını verir. Paket her bir düğümden geçtiğinde bu alanın değeri bir azaltılır ve sıfır olduğunda paket atılır.

Kaynak adres: 128 bit uzunluğundaki bu alan kaynak adresi göstermektedir.

Hedef adres: 128 bitlik IP paketinin gönderildiği hedef adresi belirtir.

2.3.2. IPv6'da Ek Başlık Yapısı

IPv4'te her zaman kullanılmasa bile duruma göre kullanılabilen alanlar yer almaktadır. Bu alanlar kullanılmasa da yönlendirici tarafından işleme alındığından yönlendiricinin iş yükünü ve paketin boyutunu artırmaktadır. IPv6'da ise her zaman kullanılmayıp gerektiğinde istenildiği sayıda kullanılabilen ve temel başlığı izleyen ek başlıklar vardır. Bu başlıklar eğer kullanılıyorsa, temel başlıktan sonraki alanda ifade edilmektedir [12].



Şekil 2.6. IPv6 eklenti başlıkları [5].

IPv6 eklenti başlıkları yapısı Şekil 2.6.'da gösterilmektedir. I. durumda eklenti başlığı kullanılmadığından IPv6 başlığından sonra TCP başlığı gelmektedir. II. durumda IPv6 başlığının sonraki başlık alanı yönlendirmeyi gösterdiğinden, yönlendirme başlığı IPv6 başlığına ek başlık olarak kullanılmaktadır. III. durumda ise IPv6 başlığının sonraki başlık alanı yönlendirmeyi göstermekte, yönlendirme başlığının sonraki başlık alanı da parçalamayı gösterdiği için parçalama ek başlığı da ilave edilerek iki farklı eklenti başlığının IPv6 başlığına eklentisini göstermektedir. Eklenti başlıkları, ek başlık içerisine eklenmek istenen başlığın kodunun belirli bir sıraya göre IPv6 sonraki başlık alanına girilerek eklenmesiyle oluşmaktadır. Bu ek başlıklar aşağıdaki sırada maddeler halinde açıklanabilir [5, 35].

- **Düğümler (bilgisayarlar, yönlendiriciler vb.) arası geçiş başlığı (Hop-by-Hop Options header):** Sonraki başlık kodu 0 olan bu ek başlık, paketin alıcısına giderken ara düğümlerde kullanılacak kontrol bilgisini taşımak için kullanılmaktadır.
- **Yönlendirme başlığı (Routing Header):** Sonraki başlık kodu 43 olan yönlendirme başlığı, paketin hedef düğüme ulaşırken üzerinden geçmesi gereken düğümlerin listesini tutmaktadır.
- **Parçalama başlığı (Fragment header):** Sonraki başlık kodu 44 olan bu ek başlık, kaynaktan gönderilen IPv6 paketinin boyutu hedef düğüme giderken geçtiği yolun MTU (Maximum Transmission Unit - Maksimum İletim Birimi) değerinden daha büyük olması durumunda kullanılır.
- **Sonraki hedef seçenekleri başlığı (Destination Options header):** Sonraki başlık kodu 60 değerini almaktadır. Hedef düğümler için değerlendirilmesi

istenen ek bilgileri taşımaktadır. Ek başlık sıralamasında iki kez kullanılan tek başlıktır.

- **Doğrulama başlığı (Authentication header):** Sonraki başlık kodu 51 olarak belirlenmiştir. Taşınan paketin veri bütünlüğü, veri gizliliği ve veri doğruluğunu sağlamak için kullanılmaktadır.
- **Veri güvenlik başlığı (Encapsulating Security Payload header):** Sonraki başlık kodu 50 olarak belirlenmiştir. IPv4 ve IPv6'da IPSec güvenlik protokolüne destek vermek amacıyla tasarlanmıştır. Taşınan paket ele geçirilse bile şifreleyerek paketin anlaşılmaması için veri gizliliği, paketin asıl kaynaktan gönderilen paket olup olmadığının tespiti için veri doğruluğu ve paketin hedefe giderken kopyalanıp yeniden gönderilmesini engellemek için yineleme engeli işlemleri veri güvenlik desteğini sağlamaktadır. Aynı zamanda bu ek başlık, paket doğrulama başlığı ile birlikte de kullanılabilir.

2.4. IPv6 Adresleme Mimarisi

32 bitlik IPv4 adreslerinde var olan adres sıkıntısını gidermek amacıyla IPv6 adresleri 128 bitten meydana gelmektedir. 128 bitlik adres boyutu ile 2^{128} ($3{,}4x10^{38}$) adet farklı adresin kullanılmasına izin verilmektedir. Bu sayı, dünyadaki her bir metrekareye $6{,}5x10^{23}$ adet adres düşmesine izin verildiği olanağını göstermektedir [31,32,35,36]. Bu sayısal değerler ile IPv6'nın çok büyük bir adresleme olanağı sunduğu görülmektedir.

2.4.1. IPv6 Adres Gösterimi

IPv4 adresleri 8'er bitlik 4 blok halinde ve bloklar arasında nokta işareti konularak gösterilmektedir. Örnek bir IPv4 adresi 160.75.67.1 şeklinde gösterilebilir. IPv4 adreslerine göre 4 kat daha uzun olan IPv6 adresleri için farklı bir gösterim kullanılmaktadır. Onluk sayı sistemi yerine onaltılık sayı sistemi kullanılarak IPv6 adreslerinin daha kısa uzunlukta gösterilmesi sağlanmıştır. IPv6 adresleri 16'şar bitlik 8 blok şeklinde ve her bir blok 4 adet onaltılık formatta olan sayılardan oluşmaktadır. Bloklar arası iki nokta üst üste işareti (:) ile ayrılarak gösterilmektedir. Bir bloğun en büyük onaltılık değeri FFFF'dir. Örnek bir IPv6 adresi 69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF şeklinde gösterilebilir [12,31,37].

IPv6 adresleri üç farklı şekilde gösterilmektedir [12,31,37].

- Tercih edilen format x:x:x:x:x:x:x:x şeklindedir. Bu gösterimdeki x, dört adet onaltılık sayı değerini ifade etmektedir. Örnek olarak ABCD:EF01:2345:6789:ABCD:EF01:2345:6789 adresi verilebilir. Veya 2001:DB8:0:0:8:800:200C:417A şeklindeki gibi 16 bitlik sayı bloklarından sol tarafındaki sıfırlar yazılmadan da kısaltılmış şekilde gösterilebilir.
- Bazı IPv6 adresleri arka arkaya gelen uzun sıfır dizilerinden oluşmaktadır. Bu tür adresleri daha kolay gösterebilmek için sıfırları sıkıştırarak oluşturulmuş olan gösterim geliştirilmiştir. Buna göre "::" gösterimi bir yada daha fazla 16 bitlik sıfır dizisini göstermektedir. Bir adreste "::" işareti sadece bir defa kullanılabilir. Örnek olarak belirtilen adresler aşağıdaki gibi gösterilmektedir.

  2001:4BD0:2031:0:0:0:0:1
  FF01:0:0:0:0:0:0:101
  0:0:0:0:0:0:0:1

  Yukarıda belirtilen adresler aşağıdaki gibi kısaltılarak da gösterilebilir.

  2001:4BD0:2031::1
  FF01::101
  ::1
- Bazı durumlarda IPv4 ve IPv6 adresleri birlikte kullanılabilmektedir. Bu gibi durumlar için x:x:x:x:x:x:d.d.d.d şeklindeki gösterimde x'ler 16 bitlik altı adet bloğu onaltılık sayı sisteminde, d'ler ise 8 bitlik dört adet bloğu onluk sayı sisteminde göstermektedir. Bu gösterimde d ile ifade edilen kısımlar standart IPv4 adresleme gösterimidir. 2001:4BD0:0:0:0:0:160.75.67.1 adresi bu tip gösterime örnek olarak verilebilir.

2.4.2. IPv6 Adres Önek Gösterimi

Önekler, adresin değişmeyen veya ağ tanımlayıcısına ait bitleri gösteren bölümdür. IPv6 öneklerinin gösterimi IPv4 CIDR gösterimiyle aynı şekildedir. Bir IPv6 öneki, adres/önek uzunluğu formatında gösterilir. 24 bitlik alt ağ maskesine sahip olan bir IPv4 adresi 192.168.2.0/24 şeklinde gösterilirken, 48 bitlik bir öneke sahip olan IPv6 adresi de 2001:0:2310::/48 şeklinde gösterilmektedir.

Alt ağ maskesi ile hedef adres bitişik bir şekilde gösterilebilmektedir. Örneğin alt ağ maskesi 2001:4BD0:2031::/48 olan bir ağda, bir istemciye 2001:4BD0:2031::2 adresi verilsin. Bu istemcinin adresi alt ağ maskesi ile bitişik bir şekilde göstermek istenirse 2001:4BD0:2031::2/48 şeklinde gösterilebilmektedir. IPv4 uygulamaları alt ağ olarak bilinen ağ önekinin noktalı ondalık gösterimini kullanmaktadır. IPv6'da alt ağ maskesi yerine sadece önek uzunluğu gösterimi desteklenmektedir [12,31].

2.4.3. IPv6 Adres Çeşitleri

2001::/16 adresleri IPv6'ya geçmiş olan internet servis sağlayıcılar tarafından kullanılabilir. 2002::/16 adresleri 6'dan 4'e adresler olarak tanımlanmıştır ve IPv6 ağlarının IPv4 ağlarına bağlanmasında kullanılmaktadır.

IPv6 adresleri IPv4'de olduğu gibi iki kısımdan oluşmaktadır. 128 bitten oluşan IPv6 adreslerinin ilk 64 bitlik kısmı bulunulan ağı yani alt ağ tanımlayıcısını (subnet identifier), son 64 bitlik kısmı ise ağdaki bilgisayarı yani arayüz tanımlayıcısını (interface identifier) göstermektedir. Ağı gösteren ilk 64 bitin son 16 biti IPv6'da alt ağ olarak adlandırılabilen IPv6 önekini göstermektedir. Bir ağda en çok 2^{16} adet alt ağ, her alt ağ içerisinde de 2^{64} adet bilgisayar bulunabilmektedir. IPv4'de olduğu gibi IPv6'da da üst seviye bitler IPv6 adres çeşitlerini belirtmektedir. Bu üst seviye bitlere FP (format prefix) de denilmektedir. Bazı çok kullanılan adreslerin FP'leri aşağıda listelenmiştir [37].

- Geri dönüşüm (loopback) adresi FP= 00…1 (128 bit)
- Küresel tekli yayın (global unicast) adresinde FP= 001
- Yerel-bağlantı tekli yayın (link-local unicast) adresinde FP= 1111 1110 10
- Yerel-bölgesel tekli yayın (site-local unicast) adresinde FP= 1111 1110 11
- Çoklu yayın (multicast) adresinde FP= 1111 1111

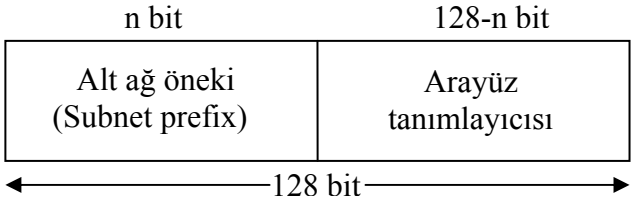
Yukarıdaki verilen FP önekleri de dikkate alındığında IPv6'da üç temel adresleme yapısının olduğu görülür. Bunlar:

- Tekli yayın (unicast) adresler
- Rasgele yayın (anycast) adresler
- Çoklu yayın adresler

IPv4'deki yayın adresi tamamen kaldırılarak, IPv6'da bu görev çoklu yayın adresi tarafından yerine getirilmektedir.

2.4.3.1. Tekli Yayın Adresler

Tekli yayın adresler bir bilgisayarı belirtmek için kullanılan adreslerdir. Tekli yayın adresine gönderilmiş paketler sadece o adresi gösteren bilgisayara iletilir [37]. Şekil 2.7.'de IPv6 adres bölümlemesi gösterilmektedir.



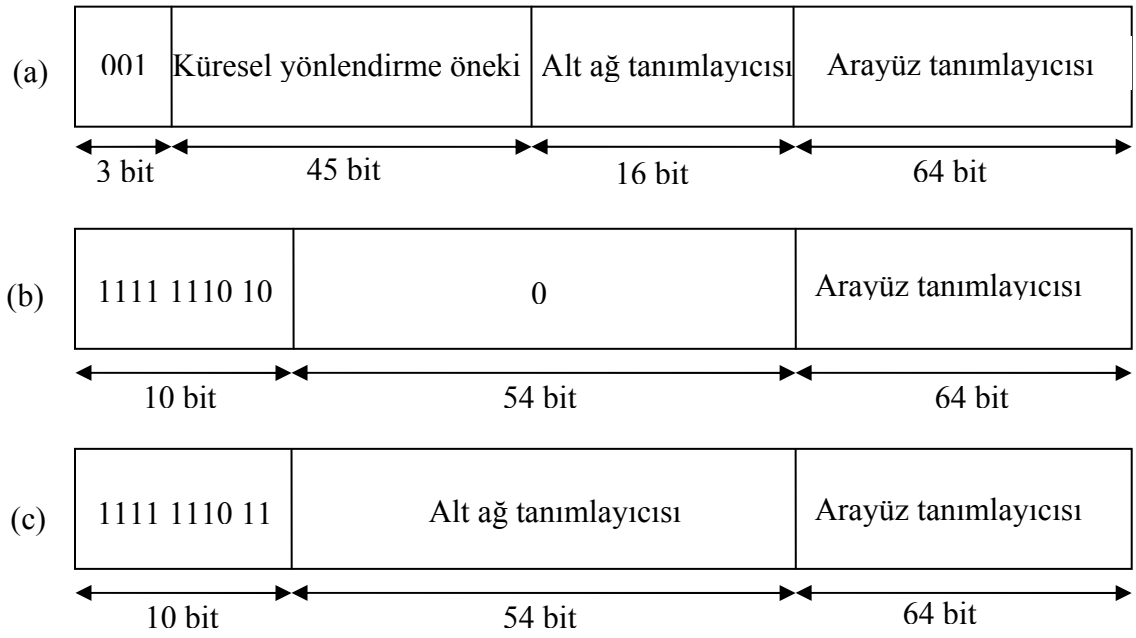
Şekil 2.7. IPv6 adres bölümlemesi.

Şekil 2.7.'de belirtilen arayüz tanımlayıcıları, atandığı cihazın ağ üzerinde tanımlanmasını sağlayan kısımdır. Aynı ağ içerisindeki bir arayüz tanımlayıcısı yalnızca bir cihaza atanabilir. Alt ağ öneki ise bulunulan ağı belirtmektedir [37]. Tekli yayın adresleri üç grupta listelenebilir [6,32,37,38]. Bunlar aşağıdaki gibi açıklanabilir.

- **Küresel tekli yayın adresleri:** Günümüzde genel olarak internette kullanılan adreslerdir. IPv4 küresel tekli yayın adreslerinde olduğu gibi IPv6 küresel tekli yayın adresleri yönlendiriciler tarafından kullanılabilmektedir. RFC 3587'de tanımlanmış olan bu adreslerde ilk 3 bit olan FP değeri "001" olmaktadır. Bundan sonraki 45 bit küresel yönlendirme önekini (global routing prefix), sonraki 16 bitlik kısım alt ağ tanımlayıcısını (subnet ID) ve son 64 bitlik kısım ise arayüz tanımlayıcısını (interface ID) göstermektedir. Küresel tekli yayın adreslerinin yapısı Şekil 2.8.(a)'da gösterilmektedir.
- **Yerel-bağlantı tekli yayın adresleri:** Aynı bağlantı üzerindeki komşu düğümlerle iletişimde kullanılan adreslerdir. Bu adresler komşu sorgulama, otomatik adres yapılandırması veya bağlantının bağlı olduğu herhangi bir yönlendirici olmadığı durumlarda düğümler arası iletişimin sağlanması gibi amaçlar için kullanılmaktadır. Yönlendiriciler bu tür adresleri bağlantı dışına

yönlendirmezler. Bu adreslerde ilk 10 bit olan FP değeri “1111 1110 10” olmaktadır. Sonraki 54 bit “0”, son 64 bit ise arayüz tanımlayıcısını göstermektedir. Bu tür adreslerin ilk 64 bitlik kısmı FE80:: ile ifade edilmektedir. Yerel-bağlantı tekli yayın adreslerinin yapısı Şekil 2.8.(b)’de gösterilmektedir.

- **Yerel-bölgesel tekli yayın adresleri:** Aynı site içerisinde kullanılan adreslerdir. Bu adresler, herhangi bir işyerinin ağ adresleri veya evde kullanılan adresler olarak düşünülebilir. Paketler yönlendiriciler tarafından site içerisinde kalacak şekilde yönlendirilebilirler. Bu adresler yerel-bağlantı adresleri gibi otomatik olarak yapılandırılmayıp kullanıcı veya ağ tarafından ihtiyaç duyulması durumunda yapılandırılırlar. Küresel adreslerle birlikte kullanılabilen yerel-bölgesel adresleri, yapı bakımından küresel tekli yayın adreslerine benzemektedir. Bu adreslerde ilk 10 bit olan FP değeri “1111 1110 11” olmaktadır. Sonraki 54 bit alt ağ tanımlayıcısını ve kalan 64 bit ise arayüz tanımlayıcısını göstermektedir. Yerel-bölgesel tekli yayın adreslerinin yapısı Şekil 2.8.(c)’de gösterilmektedir.



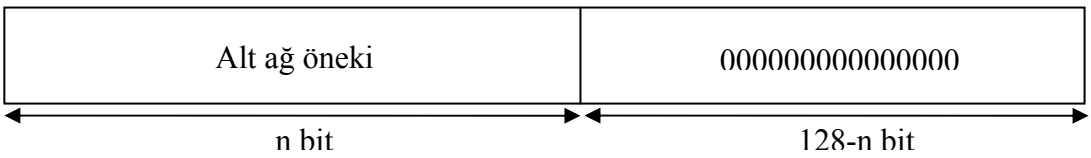
Şekil 2.8. IPv6 tekli yayın adresleri a) Küresel tekli yayın adresleri b) Yerel-bağlantı tekli yayın adresleri c) Yerel-bölgesel tekli yayın adresleri.

Diğer IPv6 tekli yayın adres türleri de aşağıdaki gibi listelenebilir [12,31].

- **Tanımlanmamış adres:** Tüm bitleri sıfır olup IPv6 adres gösterimi 0:0:0:0:0:0:0:0 veya :: şeklinde olan adreslere tanımlanmamış adres denir. Bu adresin amacı herhangi bir düğüme bir adresin atanmadığını göstermektir. Ayrıca bu adres hiçbir zaman hedef adres olarak kullanılmaz.
- **Geri dönüşüm adresi:** Sadece son biti bir, diğer bitleri sıfır olan ve IPv6 adres gösterimi 0:0:0:0:0:0:0:1 veya ::1 şeklinde olan adrese geri dönüşüm adresi denir. Bu adres bir düğümün kendi kendine paket göndermesini sağlamak için kullanılır. Ayrıca bu adres hiçbir zaman IPv6 paketlerinin kaynak adresi olarak kullanılamaz.
- **IPv4 içeren IPv6 adresleri:** IPv4'ten IPv6'ya geçişte her iki türdeki ana bilgisayarın birlikte kullanılmasını kolaylaştırmak için tanımlanan adreslerdir. Bunlar IPv4 uyumlu ve IPv4 ile eşleşmiş adreslerdir. IPv4 uyumlu adresler, 0:0:0:0:0:0:w.x.y.z veya ::w.x.y.z şeklinde gösterilen adreslerdir. Gösterilen adresteki w.x.y.z adresi IPv4 adresini göstermektedir. Mevcut IPv6 geçiş mekanizmaları tarafından desteklenmediğinden dolayı bu adres türü artık kullanılmamaktadır. IPv4 ile eşleşmiş adresler, 0:0:0:0:0:FFFF:w.x.y.z veya ::FFFF:w.x.y.z şeklinde gösterilen adreslerdir. Bu adresler, IPv4 düğümlerini IPv6 adresleri olarak gösterebilmek için kullanılmaktadır. Bu adres türünün kullanılmasındaki en önemli avantaj, bu adresi kullanan programın hem IPv4 hem de IPv6 adresini aynı anda elde edebilmesidir.

2.4.3.2. Rasgele Yayın Adresler

Rasgele yayın adresleri IPv4'te bulunmayıp IPv6 için geliştirilmiş ve genellikle farklı düğümlere ait bir grup arayüzü ifade etmek için kullanılan adreslerdir. Rasgele yayın adresine gönderilmiş olan bir paket bu adrese sahip tek bir arayüze gönderilir. Bu adresler, IPv6 paketlerinin sadece hedef adresleri olarak kullanılmaktadır. Rasgele yayın adreslerinin yapısı Şekil 2.9.'de gösterilmektedir [6,37].



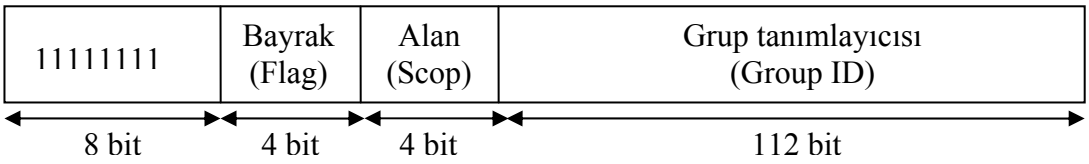
Şekil 2.9. Rasgele yayın IPv6 adres yapısı.

Şekil 2.9.'daki rasgele yayın adresinin ilk n biti, ara yüzün ait olduğu alt ağ önekini ifade etmektedir. Geri kalan 128-n bitine ise sıfır değeri atanmaktadır.

Rasgele yayın adresi, tekli yayın adresinin birden fazla düğüme verilmesiyle oluşmaktadır. Bu adresler yapısal olarak tekli yayın adresleri ile benzer, kullanım alanı olarak farklıdır. Bir grup ağ cihazına atanmış olan tekli yayın adresi o gruptaki cihazlardan herhangi birisine ulaşmak için kullanılmaktadır. Yani rasgele yayın adreslerinde tekli yayın adresindeki gibi birebir haberleşme yapılmamaktadır [37].

2.4.3.3. Çoklu Yayın Adresler

Çoklu yayın adresleri, rasgele yayın adreslerine benzer şekilde farklı düğümlere ait bütün grup arayüzleri göstermek için kullanılır. Çoklu yayın adreslerine gönderilen paket bu adrese sahip bütün arayüzlere gönderilir. Ayrıca çoklu yayın adresleri yalnızca hedef olarak kullanılabilmektedir [6,32,37].



Şekil 2.10. Çoklu yayın adres yapısı.

Şekil 2.10.'da gösterilen çoklu yayın adreslerinin ilk 8 biti yani FF değeri, adresin çoklu yayın adresi olduğunu belirtmektedir. Sonraki bayrak bölümü 4 bitten oluşmaktadır. Sonraki alan bölümü çoklu yayın adresinin kullanım kapsamını gösteren 4 bitlik bir alandır. En son 112 bitlik grup tanımlayıcı alanı ise çoklu yayın gruplarını tanımlamak için kullanılan alandır [37].

2.5. Komşu Keşif Mesajları

Komşu Keşif mesajları (Neighbor Discovery messages – ND messages) IPv6 ile birlikte gelen yeniliklerdendir. ND mesajları, IPv4'te bulunan ARP, ICMP Yönlendirici Keşif ve ICMP Yönlendirme mesajlarını yerine getirmiştir [32]. Düğümler, aynı bağlantı üzerindeki komşularının veri bağlantı katmanı adreslerinin öğrenilmesinde ve hafızada

tutulan önceki bilgilerin geçerliliğinin kontrol edilmesinde ND mesajlarını kullanmaktadır. Ayrıca, düğümler aynı bağlantı üzerindeki yönlendiricileri sorgulamak ve bu yönlendiricilerden adres, önek ve diğer yapılandırma bilgilerini almak için de ND mesajlarını kullanmaktadır. Yönlendiriciler ise bu mesajları paket yönlendirmede hedef düğümün tespiti ve yapılandırma bilgilerini düğümlere yayımlamada kullanmaktadır. ND mesajları aşağıda maddeler halinde açıklanmıştır [39,40].

- **Yönlendirici Sorgulama (Router Solicitatin - RS):** IPv6 düğümleri tarafından aynı bağlantı üzerindeki yönlendiricilerin bulunması için kullanılmaktadır.
- **Yönlendirici Bildirisi (Router Advertisement - RA):** IPv6 yönlendiricileri tarafından RS mesajlarına cevap olarak gönderilir.
- **Komşu Sorgulama (Neighbor Solicitation - NS):** IPv6 düğümleri tarafından komşu düğümlerin veri bağlantı katmanı adreslerini öğrenmede veya veri bağlantı katmanı adresleri sayesinde hala geçerli olan komşuluk keşfi için kullanılmaktadır.
- **Komşu Bildirisi (Neighbor Advertisement - NA):** NS mesajına cevap olarak sorgulanan düğüm tarafından veri bağlantı katmanı adresini bildirmek için kullanılmaktadır.
- **Yönlendirme (Redirect):** Yönlendiriciler tarafından hedefe ulaşmak için en iyi ilk düğümü belirtmede kullanılmaktadır.

3. BÖLÜM

IPv6'NIN ÜLKELERDEKİ KULLANIMI ve IPv4'TEN IPv6'YA GEÇİŞ SÜRECİ

3.1. IPv6'nın Türkiye'deki Durumu

Türkiye'deki IPv6 hakkında yapılan çalışmalar, 2003 yılından itibaren TÜBİTAK (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu) [41] çatısı altında ULAKBİM (Ulusal Akademik Ağ ve Bilgi Merkezi) [42] tarafından yürütülmektedir. ULAKBİM, Türkiye ile Avrupa Akademik Ağı (GEANT) arasında olan internet bağlantısı çalışmalarını 2003 yılında tamamlayarak kendisine bağlı bütün üniversitelerin ve araştırma kurumlarının GEANT'a IPv6 bağlantısı yapabilmesi için gerekli altyapıyı oluşturmuştur. 2004 yılından itibaren talep eden üniversitelere IPv6 adresleri tahsis edilebilir duruma gelinmiştir. 2006 yılı sonunda TÜBİTAK-ULAKBİM tarafından bazı üniversitelerin de katılımıyla birlikte IPv6 destekli ULAKNET (Ulusal Akademik Ağ) düğümlerinin oluşturduğu ULAK6NET Görev Gücü adı ile anılan bir çalışma grubu oluşturulmuştur [43].

Bilgi Teknolojileri ve İletişim Kurumu (BTK)'nun kurum içi uzmanlık tez çalışmalarında IPv6 konusu ağırlıklı olarak incelenmiş ve 2007 yılında IPv6 için gerekli donanım ve yazılım altyapısının geliştirilmesi amaçlanmıştır [44]. BTK ve TÜBİTAK-ULAKBİM arasında 14 Şubat 2007'de imzalanan Ar-Ge (Araştırma - Geliştirme) İşbirliği Protokolü ile Türkiye'nin teknolojik alanda öncü bir rolü üstlenme hedefleri vurgulanmıştır [45]. 2009 yılı başında ULAKBİM, Çanakkale 18 Mart Üniversitesi ve Gazi Üniversitesi işbirliği ile "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" adı altında bir çalışma başlatılmıştır [43]. Tablo 3.1.'de, Türkiye'deki üniversitelerin bir kısmının IPv6 adresini aldıkları tarihleriyle birlikte şimdiki ULAK6NET katkı seviyeleri gösterilmektedir [43].

Tablo 3.1. Türkiye'de IPv6 adresi alan üniversiteler ve katkı seviyeleri.

Üniversiteler	**Seviye**
Celal Bayar Üniversitesi	8
Çanakkale 18 Mart Üniversitesi	8
Marmara Üniversitesi	8
Orta Doğu Teknik Üniversitesi	8
Süleyman Demirel Üniversitesi	7
Gazi Üniversitesi	4
İstanbul Teknik Üniversitesi	3
Sivas Cumhuriyet Üniversitesi	3
Doğu Akdeniz Üniversitesi	2
Ege Üniversitesi	2
Eskişehir Osmangazi Üniversitesi	2
Şırnak Üniversitesi	2
Çukurova Üniversitesi	1
Sabancı Üniversitesi	1
Bahçeşehir Üniversitesi	1
Selçuk Üniversitesi	1
Uludağ Üniversitesi	1
Boğaziçi Üniversitesi	1
Bilkent Üniversitesi	1
Abant İzzet Baysal Üniversitesi	1
Yıldız Teknik Üniversitesi	1
Gaziantep Üniversitesi	1
Trakya Üniversitesi	1
Aksaray Üniversitesi	1
Nevşehir Üniversitesi	1
Adnan Menderes Üniversitesi	1
Hitit Üniversitesi	1

Tablo 3.1.'deki verilen seviyelerin anlamları aşağıdaki gibi belirlenmiştir.

- Seviye 1: IPv6 adresi almak.
- Seviye 2: Ana yönlendiricisinde IPv6 yönlendirme ayarlarını yapmak.

- Seviye 3: Güvenlik duvarını IPv6 destekler hale getirmek.
- Seviye 4: İç Alan ağında sunucularda en az 3 adet deneme servisleri vermek (dns,ftp vb.).
- Seviye 5: www,smtp,dns,ftp servislerini IPv6'dan hizmet verir hale getirmek.
- Seviye 6: IPv6 istatistiklerini ayrı olarak web sayfasında yayınlamak.
- Seviye 7: Gerçek ortamda yerel alan ağında kullanılan en az 10 adet bilgisayarı IPv6 kullanır hale getirmek.
- Seviye 8: En az bir bölümü IPv6 destekler hale getirmek (fizik, kimya vb.).

Tablo 3.1.'den, Türkiye'de IPv6 altyapı çalışmaları ve sisteme uyum sürecinde çoğu üniversitenin başlangıç aşamasında olması, Türkiye'nin IPv6'ya geçiş sürecinde geç kaldığını ve çalışmaların yetersiz olduğunu göstermektedir.

3.2. IPv6'nın Gelişmiş Ülkelerdeki Durumu

IPv6 araştırma çalışmaları ülke veya bölge olarak değerlendirildiğinde Uzakdoğu, ABD ve Avrupa'da yapılan çalışmalar olarak gruplandırılabilir.

Uzakdoğu ülkelerinden Japonya, IPv6 üzerinde en fazla araştırma yapan ülkelerden biri özelliğini taşımaktadır. Japonya'daki IPv6 Tanıtım Kurulu, internetin geliştirilmesinde uluslararası düzeyde öncülük etmeyi, ileri düzey bir bilgi ve telekomünikasyon ağ toplumu için insan kaynağı sağlamayı ve donanım-yazılım servisleri ile yeni iş alanları sağlama ve desteklemeyi hedeflemektedir [46]. Japonya, u-japan projesi ile 2010 yılına kadar "herkes, her zaman ve her yerden her uygulama ile bir ağa erişim sağlayabilir" başlığı içerisinde Japonya'nın "her yeri kapsayan ağ toplumu" olmasını hedeflemektedir [47].

Diğer bir Uzakdoğu ülkesi olan Çin'de, 2002 yılında IPv6 test ağı oluşturulması için hükümet tarafından 170 milyon dolarlık kaynak ayrılmıştır [43]. Çin ve Japonya'nın birlikte IPv6 üzerine yaptığı çalışmalar sonucunda 2002'de başlatılmış olan Çin-Japonya IPv6 ağı, 2005 yılında tamamlanmıştır [48].

IPv6 üzerine araştırmalar yapan diğer Uzakdoğu ülkeleri Güney Kore ve Hindistan'dır. Güney Kore, 2004 yılında IPv6 işlevselliğinin doğrulanması için KoreV6 araştırma

ağını oluşturmuştur. Hindistan'da ise 2005'te IPv6 geçiş aşamaları için önerileri içeren bildiriler yayınlanmıştır [43].

ABD'de hükümet tarafından yayınlanan "Memorandum For the Chief Information Officers" başlıklı belgede IPv6 geçiş sürecinde yapılması gerekenler aşamalı olarak belirtilmiş ve 30 Ağustos 2008 tarihine kadar tüm kurum ağlarının IPv6 hizmeti sunmaya hazır halde olması gerektiği vurgulanmış ve IPv6'ya geçilmiştir [43,49,50].

2001 yılında başlatılan Avrupa IPv6 Görev Gücü ve IPv6 Forum çalışmaları ile çeşitli projeler yürütülerek Avrupa'da IPv6 için önemli bir yol kat edilmiştir. Avrupa Birliği'nin projelerinin yanı sıra, birçok Avrupa ülkesi kendi içlerinde IPv6 araştırma çalışmalarını devlet desteğiyle oluşturulan IPv6 Görev Gücü ekiplerince yürütmektedir. Başlıca Avrupa ülkelerinden biri olan Almanya'daki IPv6'ya geçiş çalışmaları 2004 yılında Alman Savunma Bakanlığı'nın düzenlediği "Alman IPv6 Zirvesi" ile başlatılmıştır. Diğer Avrupa ülkelerinden biri olan İspanya'da Mayıs 2003 tarihinden itibaren, Fransa'da ise Eylül 2003 tarihinden itibaren internet siteleri IPv6 desteği sunmaktadır. Bir diğer Avrupa ülkesi olan İngiltere'de ise UK6X isimli internet geçiş ağı 2002 yılından beri IPv6 hizmeti sunmaktadır [43,49,51].

3.3. IPv6'ya Geçiş Süreci

IPv6'ya geçiş işleminde öncelikle sistemde gerek duyulan bütün donanım ve yazılımın IPv6 ile uyumlu olması sağlanmalıdır. Bir sistemde IPv4 ile IPv6 aynı anda çalışabilmelidir. Sistem çalışırken IPv6'ya geçiş gerçekleştirilebilir. Eski cihazların IPv6'ya dönüşümü sağlandığı takdirde, IPv6 maliyetleri minimuma indirgenmiş olmaktadır. Bu geçiş işlemi, mevcut çalışan sistem önemli bir kesintiye uğratılmadan ve sistemin olabildiğince az etkilenmesi sağlanarak gerçekleştirilmelidir. Dolayısıyla iki protokolün 10 yılı aşkın bir süre daha birlikte çalışabileceği tahmin edilmektedir [52].

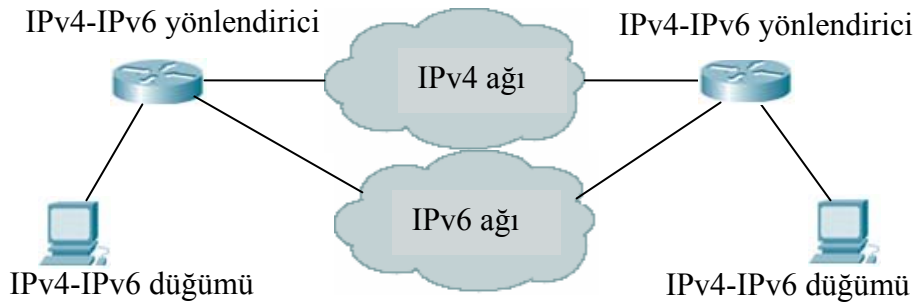
Ağ tasarımcıları, IPv6'ya geçiş için ağ içinde küçük bir alandan başlanarak tüm ağa uygulanmasının en uygun geçiş yöntemi olacağını düşünmektedir. Böylece küçük bir alan içindeki başarılı bir iletim sonrasında sistem genişletilerek bütün ağı kapsayacak şekilde IPv6 geçişinin gerçekleştirilmesi sağlanacaktır [6].

3.4. IPv4'ten IPv6'ya Geçiş Yöntemleri

IPv4'ten yeni nesil IP protokolüne geçiş sürecinde amaç, mevcut olan IPv4 altyapısı ile IPv6 ağlarının birlikte belirli bir süre çalışabilmesini sağlamaktır. IPv6'ya geçiş için kullanılacak yöntemler temel olarak çift yığın, tünelleme ve dönüştürücü şeklinde gruplandırılabilir [53].

3.4.1. Çift Yığın Yöntemi

Bu geçiş yöntemi bir düğümde IPv4 ve IPv6 protokollerinin kullanılmasına olanak sağlamaktadır. Bir düğümün haberleşeceği adres eğer IPv4 ise düğüm içerisinde IPv4 protokolü kullanılarak, IPv6 ise IPv6 protokolü kullanılarak iletişim kurulmaktadır [10]. Şekil 3.1.'de çift yığın kullanarak IPv4 ve IPv6 ağlarına erişim işlemi gösterilmektedir.

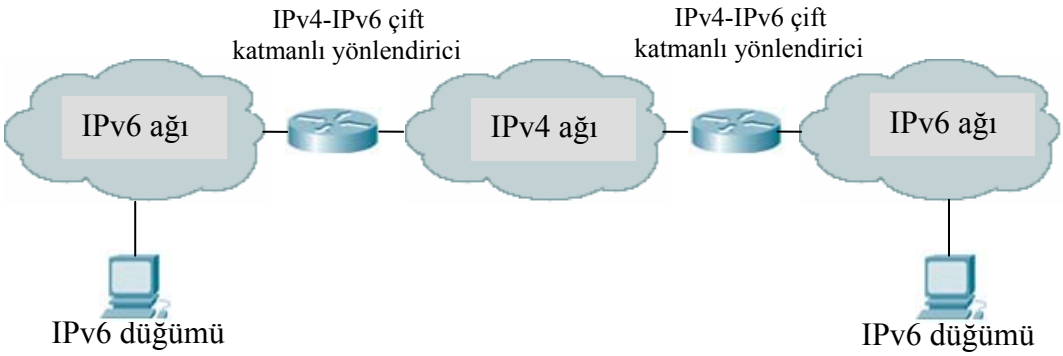


Şekil 3.1. Çift yığın yöntemiyle IPv4 ve IPv6 ağlarına erişim işlemi.

Çift yığın yönteminin temel özelliği IPv4 ve IPv6 paketlerini alıp-gönderme işlemini sağlamaktır. Bu yöntemle ilgili temel sorun, her düğüme verilebilecek sayıda yeterli IPv4 adresinin bulunamayabileceğidir. Bu durum için DSTM (Dual Stack Transition Mechanism – Çift Yığın Geçiş Mekanizması) geliştirilmiştir. DSTM mekanizması, ihtiyaç durumunda geçici olarak IPv4 adreslerinin düğümlere atanması mekanizmasıdır. Böylece çok sayıdaki çift yığın şeklinde yapılandırılmış düğümlerde, az sayıdaki IPv4 adresleri ile yapılandırma işlemi gerçekleştirilmektedir [54].

3.4.2. Tünelleme Yöntemi

İnternet altyapısı ve tüm yerel ağların IPv4 alt yapısına sahip olduğu düşünüldüğünde, IPv6 verilerinin mevcut alt yapı üzerinden bir IPv4 verisi gibi iletilmesini sağlamak geçiş için en temel çözümdür. Bu teknikte temel amaç, IPv6 paketlerinin IPv4 paket başlığındaki veri alanına yerleştirilmesi ve IPv6 paketlerinin hedefe bu şekilde IPv4 ağı üzerinden ulaştırılıp, hedefe ulaştıktan sonra ise IPv6 paketlerinin ayrıştırılarak kullanılmasıdır. İnternetin çok büyük bir kısmı IPv4 protokolüne sahip olduğundan, tünelleme mekanizmaları geçiş için kullanılan en temel yöntemdir. Şekil 3.2.'de IPv4 ağı üzerinden IPv6 ağına tünelleme yapısı gösterilmektedir [10,12].



Şekil 3.2. Tünelleme yapısı.

Şekil 3.2.'deki örnek şemada IPv6 kullanan iki uçtaki cihazlar, çift katmanlı yönlendiriciler aracılığıyla verilerini IPv6 ağından IPv4 ağına bağlayarak IPv4 ağı üzerinden aktarmaktadır.

Temel olarak dört farklı tünelleme yapısı bulunmaktadır. Bunlar aşağıdaki gibi sıralanabilir [55].

- **Yönlendiriciden yönlendiriciye (router to router):** Çift katmanlı yönlendiricilerin arasında eğer IPv4 ağı varsa bu yapıya yönlendiriciden yönlendiriciye tünel kurulan yapı ismi verilir. Bu yapıda IPv6 paketleri IPv4 ağı içerisinden hedefe iletilmektedir.
- **Ana sunucudan yönlendiriciye (host to router):** IPv4 ve IPv6 destekli bir ana sunucudan IPv6 paketleri iletebilmek için çift katmanlı bir yönlendirici

üzerinden iletim işlemi gerçekleştirilen yapıya ana sunucudan yönlendiriciye kurulan yapı ismi verilmektedir.

- **Ana sunucudan ana sunucuya (host to host):** Çift yığın yapısında olan iki ana sunucu arasında bağlantı kurulan yapıdır.
- **Yönlendiriciden ana sunucuya (router to host):** Bazı durumlarda çift katmanlı bir yönlendiricinin çift yığın yapıda olan bir ana sunucuya tünel kurması gerekebilmektedir. Bu durumda yönlendiriciden ana sunucuya ismi verilen yapı kullanılmaktadır.

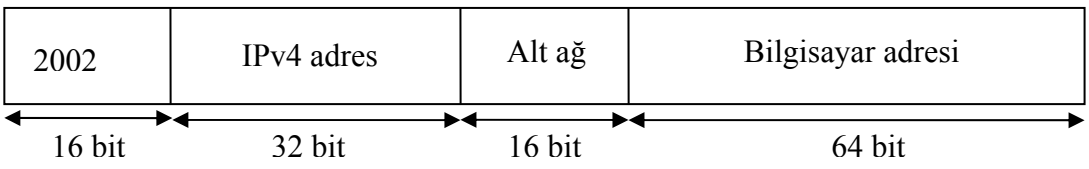
Ağ yapıları çok çeşitli olup bu ağ yapısına göre ihtiyaçlar değiştiğinden dolayı birden fazla tünelleme tekniği geliştirilmiştir. Temel olarak bu teknikler, yapılandırılmış ve otomatik yapılandırılmış tünelleme teknikleri olarak sınıflandırılabilir. Otomatik yapılandırılmış tünelleme teknikleri ise 6to4, Teredo, ISATAP ve 6over4'dür [54].

3.4.2.1. Yapılandırılmış Tünelleme

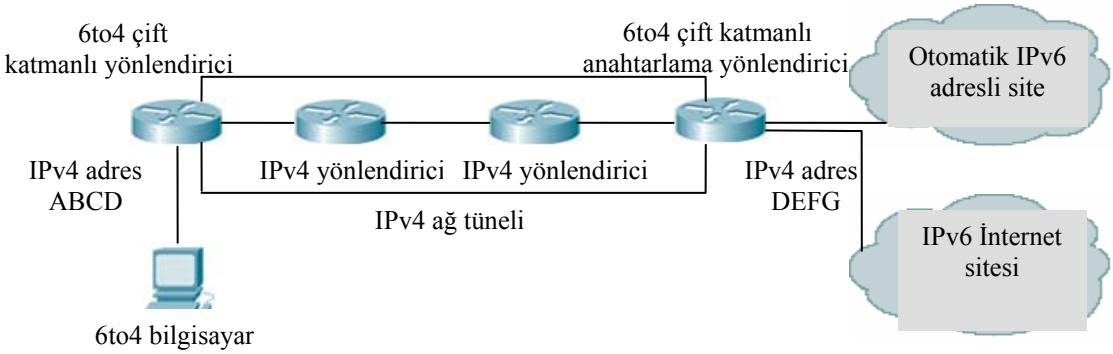
En basit geçiş metodu olmasına karşın adreslerin elle yapılandırılması diğer metotlara göre kolay onarılabilirliği azaltmaktadır. Bu tünelleme tekniğinin otomatik tünelleme metotlarından temel farkı elle yapılandırma işleminin gerçekleştirilmesidir [54].

3.4.2.2. 6to4

6to4 tünelleme tekniği, diğer IPv6 kullanıcısı ile arasında bir tünel oluşturulmadan çift katmanlı yönlendiriciler arasında sadece aynı ağda değil internet üzerinden de haberleşebilen IPv6 bağlantısı amaçlayan bir yöntemdir [54]. 6to4 adresleri, 2002 ile başlayan ve içerisinde 32 bit IPv4 adresinin onaltılık sistemdeki gösterimini içeren Şekil 3.3.'deki gibi gösterilen adres yapısıdır [56].



Şekil 3.3. 6to4 adres formatı.



Şekil 3.4. 6to4 Tünelleme örneği.

Şekil 3.4.'te 6to4 tünelleme yapısı kullanarak IPv6 bağlantısı örneklendirilmiştir. Buna göre IPv4 tünelinin çıkışında iki farklı IPv6 sitesi bulunmaktadır. Bunlardan biri otomatik IPv6 adrese sahip site, diğer ise "001::" şeklindeki küresel IPv6 adrese sahip internet sitesidir. Bu iki siteyi ayırmak için de gerekli cihaz olan anahtarlama yönlendiricisi kullanılmıştır. Anahtarlama yönlendiricileri çift katmanlı ve otomatik IPv6 adresli yapıya sahiptir [57,58].

6to4 bilgisayar, otomatik IPv6 adresli site veya küresel IPv6 adresli internet sitesinden biriyle haberleşirken kaynak adres olarak kendi IPv6 adresini, hedef adres olarak da bu iki siteden herhangi birinin adresi olacak şekilde bir IPv6 paketi oluşturup 6to4 çift katmanlı yönlendiricisine vermektedir. Bu cihaz 2002:0A0B:0C0D:: şeklindeki bir IPv6 adrese sahiptir. Bu adresten A.B.C.D biçimindeki IPv4 adresi otomatik olarak üretilir. Benzer şekilde 6to4 çift katmanlı anahtarlama yönlendirici cihazı da 2002:0D0E:0F0G:: adresi içerisinden D.E.F.G şeklindeki IPv4 adresini otomatik olarak üretmektedir.

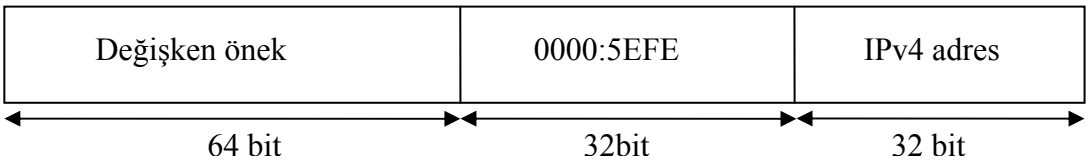
6to4 çift katmanlı yönlendirici cihazı, otomatik IP adresli internet sitesinden gelen IPv6 paketini kaynak adres A.B.C.D ve hedef adres D.E.F.G olacak şekilde IPv6 adresi ile kaplayıp bu IPv4 paketini tünele göndermektedir. Paket tünel boyunca IPv4 paketi olarak ilerleyip, 6to4 çift katmanlı anahtarlama yönlendiricisine gelir. Bu cihaz, öncelikle paketi IPv6 başlığından ayıklayıp orijinal IPv4 paketine ulaşmaktadır. Daha sonra iki farklı IPv6 sitesinden hangisine gidileceği bu cihaz sayesinde yapılan anahtarlamanın sonucunda orijinal IPv6 paketi hedefe ulaştırılmaktadır [57,58].

3.4.2.3. Teredo

Teredo, IPv4 NAT sistemi arkasında çalışan birçok istemcinin IPv6 bağlantısı sağlayabilmesi için geliştirilmiş bir geçiş mekanizmasıdır. Yapılandırılmış tünelleme ve 6to4 tünelleme teknikleri IPv4'ün 41. protokolünü kullanmaktadır. Bu protokol, TCP ve UDP protokollerinden farklı bir protokoldür. NAT sistemindeki istemciler için bu protokolün tünellemede kullanılması sorunlar oluşturmaktadır. Bu yüzden NAT sistemi içerisindeki IPv6 tünellemesi UDP paketleri kullanılarak yapılmaktadır. Teredo, 6to4 tekniğine benzer biçimde teredo sunucularıyla ve yönlendiricilerle yapılabilmektedir. Bu teknik şuanda deneysel aşamadadır ve çok fazla kullanılan bir tünelleme mekanizması değildir [54].

3.4.2.4. ISATAP

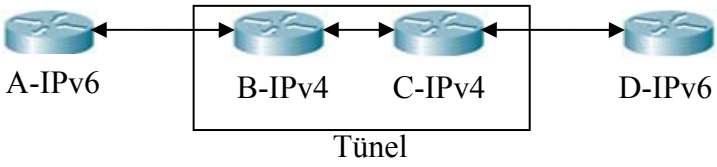
ISATAP, IPv4 ağı üzerinden IPv6 ağının haberleşmesi için tasarlanmış bir tünel mekanizması tekniğidir. ISATAP arayüzleri IPv4 ağını kullanarak IPv6 paketlerini IPv4 tüneli üzerinden geçirmektedir. Bu geçiş için tünelleme arayüzü kaynak adres olarak, IPv6 içerisinde IPv4 adresi içeren ISATAP adreslerini kullanmaktadır. Şekil 3.5.'de ISATAP adres yapısı gösterilmektedir [59].



Şekil 3.5. ISATAP adres formatı.

3.4.2.5. 6over4

6over4 tünelleme yaklaşımında, IPv4 ağı sanal ağ gibi kullanılarak bu ağ üzerinden tünelleme işlemi gerçekleştirilmektedir. Gönderici, hedef IPv6 adresi çözümler ve sanal ağın çıkışındaki IPv4 adresi olarak gönderir. Çift yığın yönteminde orijinal IPv6 paket başlığı bozulurken, tünel metodu ile çift yığın yöntemi birlikte kullanıldığı zaman ise paket kaynaktan hedefe giderken herhangi bir değişikliğe uğramadan gönderilmektedir. Şekil 3.6.'da örnek 6over4 tünelleme yaklaşımı gösterilmektedir [11,60].



Şekil 3.6. 6over4 tünelleme örneği.

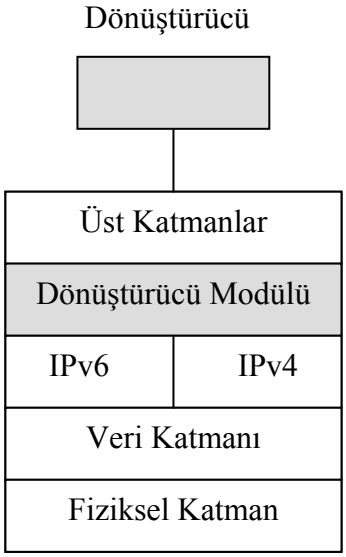
Şekil 3.6.'daki örnek yapıya göre, A'da üretilen bir paketin hedefi D olarak belirlensin. A ve D hem IPv4 hem de IPv6'nın birlikte çalıştığı, B ve C ise sadece IPv4'ün çalıştığı yönlendiricilerdir. Buna göre B ve C yönlendiricileri tünel olarak adlandırılmaktadır. A, IPv6 paketini üretir ve bu paketi IPv4 başlığı ile kaplayarak D cihazının IPv4 adresini vererek tünele gönderir. Tünelde bilgi taşınırken D'ye doğru IPv4 paketi olarak iletilir. D cihazı gelen IPv4 paketi içerisinden orijinal IPv6 paket bilgisini alır. Tünel sayesinde paketin içeriğine bakılmadan IPv6 yapıdaki A ve D, komşu iki cihazmış gibi haberleşmektedir [11,60].

3.4.3. Dönüştürücü Yöntemi

Sadece IPv4 destekli istemcilerin sadece IPv6 destekli istemcilerle iletişim kurabilmesi için NAT-PT (Network Address Translation-Protocol Translation - Ağ Adres Dönüşümü-Protokol Dönüşümü), BIS (Bump-In-The-Stack – Yığında Çarpmak) ve SOCKS64 [61] gibi dönüştürücü mekanizmaları mevcuttur [54]. Dönüştürücüler ağların birbiriyle çalıştırılabilmesini sağlar. Dönüştürücü olarak kullanılan bilgisayarlarda TCP/IP modülüne ek bir modül yerleştirilmektedir. Dönüştürücü geçiş yönteminin uygulaması kolay, geniş alanlarda yönetimi zordur. Şekil 3.7.'de katmanlı mimarideki dönüştürücü modülü gösterilmektedir [11,61]. Bu şekle göre dönüştürücü modülü, IPv4 ve IPv6'nın bulunduğu ağ katmanının hemen üstünde ara katman olarak yer almaktadır.

NAT-PT ve BIS dönüştürücü yöntemlerinde temel olarak SIIT algoritması (Stateless IP/ICMP Translation Algorithm – Durumsuz IP/ICMP Dönüşüm Algoritması) kullanılır. SIIT algoritması, IPv4 ve IPv6 paketleri arasında kullanılan iki yönlü dönüşüm algoritmasıdır. Bu algoritma, geçiş işleminde TCP ve UDP başlıklarının etkilenmemesini sağlayacak şekilde tasarlanmıştır. SOCKS64 dönüştürücü yönteminde ise çift yığın özelliğindeki SOCKS64 yönlendiricileri sayesinde IPv4 ve IPv6 ağları

arasındaki haberleşme sağlanmaktadır. Uygulamalarda SOCKS64 kütüphanesi kullanılmaktadır. Bu kütüphane ile IP adres haritası tutulmaktadır [61].



Şekil 3.7. Katmanlı mimarideki dönüştürücü modülünün yeri.

3.5. IPv6'ya Geçiş Yönteminin Seçimi

IPv6'ya geçiş yöntemleri olan çift yığın, dönüştürücü ve tünelleme metotlarının hepsinin birbirine göre farklı uygulanabilir ağ yapıları vardır. Ağ yapıları kurulacak alan ve ihtiyaçlara göre çok çeşitli olduğundan, kurulacak ağ yapısına göre bir geçiş yöntemi belirlenmelidir. Ayrıca daha önceden ağda kullanılan donanımlar da yöntemin belirlenmesinde önemli bir rol üstlenmektedir.

Çift yığın mekanizması, bir düğümde hem IPv4 hem de IPv6 adreslemeyi destekleyebilirken, yeteri kadar IPv4 adreslemenin olabilmesi için farklı bir çözüme başvurulması gerekmektedir. Dönüştürücü tekniklerinde, yine ağdaki ihtiyaçlara göre sadece IPv4 destekli ağların sadece IPv6 destekli ağlara haberleşmesi gerektiğinde başvurulabilecek bir tekniktir. Diğer bir teknik olan tünelleme tekniğinin temel çalışma prensibi, IPv4 ağı üzerinden IPv6 paketlerinin gönderilmesidir. Tünelleme tekniği, internetin IPv4 altyapısını tamamen desteklemesi sebebiyle tercih edilebilecek en temel yöntemlerden biridir.

Türkiye'de ULAKBİM tarafından IPv6'ya geçiş aşamasında birkaç yıl boyunca omurga ve uç birimlerde çift yığın yönteminin kullanılması planlanmaktadır. Fakat IPv6'ya geçiş belirli bir süre alacağı için, IPv6 ağlarının IPv4 ağları ile haberleşmesinde 6to4 tünelleme tekniğinin de kullanılması gerekecektir. Uç birimler için üniversite kampüs ağları örnek verilebilir [54].

4. BÖLÜM

IPv6'DA YÖNLENDİRME PROTOKOLLERİ

4.1. IP Yönlendirme

Yönlendirici vasıtasıyla ağdaki verinin başka bir ağa aktarılma işlemi, yönlendirme olarak adlandırılmaktadır. Yönlendirme işlemi, OSI'nın 3. katmanı olan ağ katmanında gerçekleşir. Ağ katmanının temel görevi veri paketlerini kaynaktan hedefe ulaştırmaktır. Yönlendirme algoritmaları, kaynak ile hedef aynı ağ içerisinde bulunmadığında ağ katmanına gelen paketlerin izleyeceği yola karar verir. Doğruluk, uyumluluk, basitlik, sağlamlık ve kararlılık [62], belirlenmesi gereken yol için göz önünde bulundurulması gereken performans kriterleridir.

Ağ üzerinde kullanılan yönlendirme algoritmasının yönlendirmeyi doğru gerçekleştirmesi gerekmektedir. Algoritma, performans kriterlerinden olan uyumluluk özelliğiyle ölçüt değere göre en iyi yolu seçmelidir. Seçilen algoritma olabildiğince basit, yani yönlendirme işlemini gerçekleştirirken daha uygun yazılım ve kaynak gerektirmelidir. Yönlendirici algoritması önceden karşılaşılmamış durumlara göre doğru çalışarak sağlam ve kararlı olmalıdır. Yönlendiricilerin yanlış çalışması bütün ağdaki paketlerin yanlış iletilmesine sebep olmaktadır [62].

Yönlendirme bilgileri yönlendirme tablosu içerisinde tutulur ve bu tabloya göre yönlendirme işlemi gerçekleştirilir. Bu tablo, her yönlendiricide yönlendirme işlemini gerçekleştirmek için tutulan ve hedef yönlendirici için en uygun yolun belirlenmesinde gerekli parametrelerin bir arada tutulduğu tablodur [63].

Kaynaktaki bilgilerin hedefe ulaşabilmesi için, IPv6 paketlerinin genellikle bir kaç tane IPv6 yönlendiriciden geçmesi gerekir. Gönderilen IPv6 paketleri Windows XP işletim

sistemi ve bütün UNIX tabanlı işletim sistemleri (Linux, BSD, MacOS vb.) tarafından desteklenmektedir [63].

IPv6 yönlendirme girişi elle veya yönlendirici mesajından alınan bilgiye göre yapılabilir. Paket gönderilirken hangi ağa ulaşılacağını saptamak için yönlendirme tablosunda bütün IPv6 yönlendiricileri bulunmak zorundadır. IPv6 yönlendirme tablosu kontrol edilmeden önce, hedef ön belleğin hedef adreslerden biriyle eşleşip eşleşmediği kontrol edilir. Eğer eşleşen herhangi bir hedef ön bellek yoksa IPv6 yönlendirme tablosuna göre bilgi sonraki yönlendiriciye gönderilir. Bu bilgi dönüşümüne dair veriler hedef ön bellekte kullanılmak üzere kaydedilir. Yönlendirme tablosu, direk eklenmiş ağ, uzak ağ, istemci ve varsayılan ağ yönlendirmelerini içerebilir [64].

4.1.1. IPv6 Yönlendirme Farklılıkları

IPv4 ve IPv6 yönlendirme işlemi uygulamada yaklaşık aynı olmasına rağmen, IPv6 yönlendirme işleminin çalışma prensibinde önemli farklılıklar vardır. Yönlendirme tablolarında yüz elli binden fazla IPv4 ağ öneki tutulurken, IPv6'da yaklaşık yedi yüz ağ öneki tutulması bu farklılıklardan bir tanesi olarak belirtilebilir. IPv6 yönlendirme işlemindeki farklılıklarda; IPv6 ağında bağlantı metriğinin geçişinin bozulması nedeniyle yönlendirme algoritması yanlış yola sevk edilebilmektedir [65].

4.1.2. Yönlendirme Metrik Parametreleri

Yönlendirme algoritmaları, en iyi yolu seçebilmek için yönlendirme tabloları içerisinde aşağıda belirtilen çeşitli metrik değer parametrelerini tutmaktadır [62].

- Yol uzunluğu
- Güvenlik
- Süre
- Bant genişliği
- Yoğunluk
- İletişim maliyeti

Yol uzunluğu, hedef ile kaynak yönlendiriciler arasındaki toplam uzaklık bilgisidir. Güvenlik, bağlantı noktalarındaki oluşabilecek bozukluklara karşın yön seçimidir.

Yönlendirme süresi ise paketin hedeften kaynak yönlendiriciye ulaşabilmesi için geçen zamandır. Bant genişliği, yönlendiriciler arasındaki yolda taşınabilecek paket miktarının kapasitesini göstermektedir. Yoğunluk, yönlendiricinin meşgul olma durumu olarak tanımlanabilir. Standart hatlar yerine özel hatlar üzerinden yönlendirme işleminin maliyeti, iletişim maliyeti performans parametresini göstermektedir [62].

4.2. Yönlendirme Algoritmaları

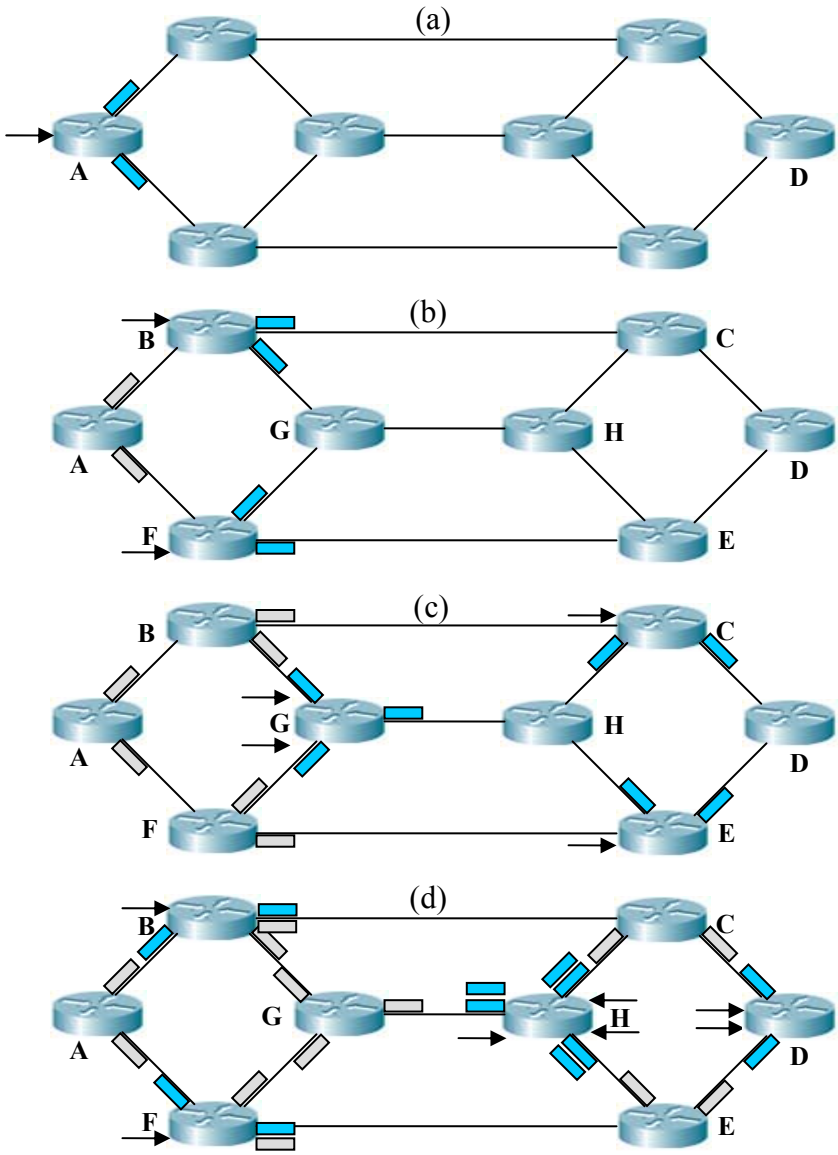
Literatürde bulunan en temel yönlendirme algoritmaları dinamik ve statik olarak iki gurupta incelenebilir [62,66]:

- Statik yönlendirme algoritmalarında yönlendirme, ağın trafiği ve yapısıyla ilgili bilgilere bağlı değildir. *Taşma (Flooding) Algoritması* ve *En Kısa Yol Algoritması (Dijkstra's Shortest Path Algorithm)* örnek olarak verilebilir.
- Dinamik yönlendirme algoritmalarında ise ağın trafiği ve topolojisiyle ilgili bilgilere dayanarak yönlendirme işlemine karar verilir. *Bağlantı Durum Algoritması (Link State Algorithm)*, *Uzaklık Vektörü Algoritması (Distance Vector Algorithm)* ve *Yol Vektörü Algoritması (Path Vector Algorithm)* örnek olarak verilebilir.

4.2.1. Taşma Algoritması

Bu teknikte yönlendirme için ağ topolojisi gibi herhangi bir ağ bilgisine gerek yoktur. Kaynak yönlendiriciden paketin kopyaları çıkarılır ve paket geldiği hat haricindeki diğer tüm hatlara gönderilir. Bu işlem, paketin hangi hatta yönlendirilmesine karar verilinceye kadar devam eder. Taşma tekniğinde, aynı paketin birden fazla kopyasının oluşturulması nedeniyle ağ trafiğini yoğunlaştırmaya sebep olmaktadır. Bu dezavantajı ortadan kaldırabilmek için paketlere yönlendirici sayacı eklenmiştir. Yönlendirici sayacına, kaynak ve hedef yönlendiricileri arasındaki yönlendirici sayısını gösteren maksimum bir değer atanmaktadır. Paket her bir yönlendiriciden geçtiğinde değeri bir azaltılmakta ve bu değer sıfır olduğunda paket hedef yönlendiriciye ulaşmamışsa atılmaktadır [66]. Paketlerin aynı yönlendiricide tekrar kopyalanmasını engellemek için diğer bir yöntem ise, paketlerin sürekli iletimi sonucu aynı kopyalar aynı yönlendiricilere çoktan ulaşmış olabileceği için, kopyası oluşmuş paket o yönlendiriciye

ulaştığında atılmaktadır [67]. Paketler en kısa yoldan varış noktasına ulaşmaktadır. Bu ulaşım sırasında paketin birçok kopyasının oluştuğunu ve birden fazla yönlendiriciye uğradığını gösteren yapı Şekil 4.1.'de gösterilmektedir [68]. Burada A, B, C, D, E, F, G ve H yönlendiriciyi, mavi renkteki kutucuklar orijinal paketi, griler ise paketlerin geçtiği düğümleri göstermektedir.



Şekil 4.1. Taşma tekniğinde paketlerin ağ içinde yayılması.

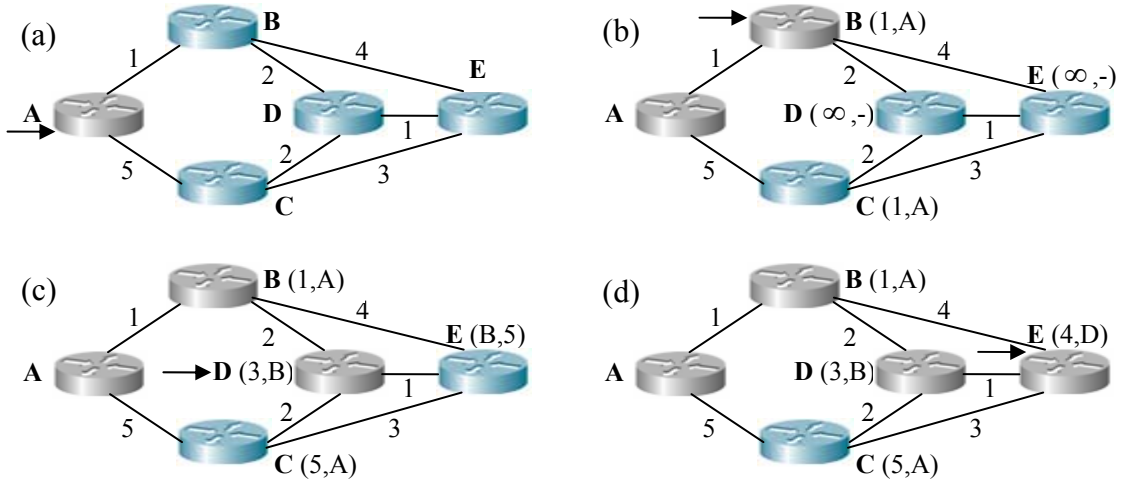
Şekil 4.1. A yönlendiricisinden D yönlendiricisine gönderilen paketin ulaştığı yönlendiricileri ve paketlerin kopyasının oluşturulmasını göstermektedir [68]. Taşma algoritması ağ uygulamalarında sıklıkla kullanılan bir teknik olmamakla birlikte askeri

amaçlar için kullanılabilmektedir. Özellikle askeri saha uygulamalarında yönlendiricilerin aniden devre dışı kalması durumunda, paketlerin hedef yönlendiriciye ulaşması mümkün olabilmektedir [68].

4.2.2. En Kısa Yol Algoritması

İki nokta arasındaki en kısa yol üzerinden paketleri gönderen ve Dijkstra tarafından geliştirilen bir tekniktir [68]. En kısa yol algoritması çalışma prensibi, farklı ölçütlerde kaynak ile hedef yönlendirici arasındaki en kısa yolu bulma olarak tanımlanabilir. Bu ölçütlerden bazıları aşağıda verilmektedir.

- Bağlantı noktaları arasındaki coğrafi uzaklık,
- Bağlantı noktaları arasındaki geçilen yönlendirici sayısı,
- Bağlantı noktalarında kuyrukta bekleme süresi,
- Her bağlantı için iletim süresi.



Şekil 4.2. En kısa yol algoritması için noktaların belirlenmesi.

Şekil 4.2.'de; A, B, C, D ve E yönlendiriciyi göstermektedir. A ve E yönlendiricileri arasında altı farklı (ABE, ACE, ABDE, ACDE, ABDCE, ACDBE) yol seçeneği vardır. Bunlardan ABDE seçeneği uzaklık bakımından en yakın yol olduğu için en iyi yönlendirme seçeneği olarak tanımlanabilir [66]. Şekil 4.2.'deki algoritmaya dair yönlendiricilerin belirlenmesi aşağıda açıklanmaktadır.

- (a) A'dan E'ye en kısa yolu hesaplamak için A noktası kalıcı olarak işaretlenip rengi değiştirilerek gri yapılmıştır.
- (b) A'ya göre B ve C noktaları kontrol edilmiş ve B'nin daha yakın olduğu tespit edilmiştir. Bu yüzden B sürekli nokta olarak işaretlenmiştir.
- (c) B'ye göre D ve E noktaları kontrol edilmiş ve D'nin daha yakın olduğu tespit edilmiştir. Bu yüzden D sürekli nokta olarak işaretlenmiştir.
- (d) Son olarak seçilecek herhangi bir nokta olmadığından, E sürekli nokta olarak işaretlenmiştir.

E hedef nokta olduğu için yönlendirme tamamlanmıştır. Yönlendirme işlemi A'dan B'ye, B'den D'ye, D'den E'ye şeklinde gerçekleşmiştir ve toplam uzaklık 4 (1+2+1) olarak bulunmuştur. Tablo 4.1.'de yönlendiriciler arası uzaklık değerleri gösterilmektedir [66].

Tablo 4.1. Yönlendiriciler arası uzaklık değerleri.

	A	B	C	D	E
A	0	1	5	∞	∞
B	1	0	∞	2	4
C	5	∞	0	2	3
D	∞	2	2	0	1
E	∞	4	3	1	0

En kısa yol algoritmasının çalışma prensibi aşağıda adım adım anlatılmıştır.

- Kaynak yönlendiriciden diğer tüm yönlendiricilere uzaklık hesaplanır.
- H yönlendirme kümesi ve s kaynak yönlendirici olarak varsayıldığında, ilk başta $H=\{s\}$ olmaktadır.
- Yönlendiriciler, en yakın olandan uzağa doğru H kümesine dâhil edilir.

Gerekli varsayımların atanması gerçekleştirildiğinde, kaynak yönlendiriciden diğer yönlendiricilere en kısa yol aşağıda belirtildiği şekilde bulunur.

for her i yönlendiricisi için

for diğer her yönlendirici için C(i,n) L(i,n) olarak belirlenecek

repeat

Geçici olarak bütün yönlendiriciler arasından en kısa olan C(i,w) uzaklığı ve w yönlendiricisi bulunur.

for i ve w haricindeki her yönlendirici için

do

if c(i,n)>c(i,w)+L(w,n) **then**

C(i,n)=C(i,w)+L(i,w)

Yol(i,n)=yol(i,w)+yol(w,n)

endif

end do

Burada, w yönlendiricisi kalıcı olarak işaretlenen yönlendiriciler kümesinin içerisine alınmaktadır.

until bütün yönlendiriciler kalıcı olarak işaretleninceye kadar döngüye devam edilmektedir [62].

Burada, C(i,n) i'den n'e kadar olan en kısa yol ve L(i,n) ise i ile n arasındaki uzaklık olarak atanmıştır.

4.2.3. Bağlantı Durum Algoritması

Bu algoritma, günümüzde yaygın olarak kullanılan ve uzaklık vektörü algoritmasının yerine kullanılmak üzere geliştirilen bir tekniktir. Bütün yönlendiriciler ağ topolojisi, yönlendiriciler arası uzaklık ve bağlantı bilgilerini tutan veritabanına sahiptir. Bu bilgi, gönderen yönlendiricinin dışında bütün yönlendiricilere ulaştırılır. Veritabanı bilgisini kullanarak ağda bulunan yönlendiriciler bağlantı durum bilgilerini almakta ve değişiklik olması durumunda güncelleme paketi yollamaktadır. Oluşan değişiklik sonucunda güncelleme paketi ağdaki yönlendiricilerin tamamına gönderildiğinden, yalnızca değişen bilgiler gönderilmiş olmaktadır. Bağlantı bilgilerini içeren LSP (Link State Packet - Bağlantı Durum Paketi) her bir yönlendiriciden alındıktan sonra ağın haritası oluşturulmaktadır. Bu ağ haritasıyla birlikte yönlendiriciler arasındaki en kısa uzaklık,

en kısa yol algoritması kullanılarak hesaplanmaktadır. Bütün yönlendiriciler, belirli bir süre içinde bağlı oldukları yönlendiricilere olan uzaklıklarını ölçmektedir [62,67].

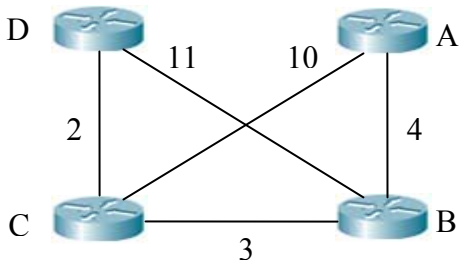
Yönlendiricinin ağdaki bütün bağlantı durum paketini aldığı düşünülerek aşağıdaki varsayımlar yapılırsa, bu tanımlamalara bağlı olarak algoritma [67],

M = {s}
N – {s} içindeki her bir n yönlendiricisi için
C(n)=L(s,n)
While (N ≠ M)
M=M ∪ {w} , C(w) (N-M) içindeki en kısa w yönlendiricisi
(N-M) içindeki her bir n yönlendiricisi için
C(n)=Min(C(n), C(w)+L(w,n))

şeklinde yazılabilir. Burada

- N: yönlendiriciler kümesini,
- L(i,j): i,j ∈ N olmak üzere yönlendiriciler arasındaki bağlantının değerini (i ve j arasında bağlantı yoksa L(ij)= ∞ değerini almaktadır),
- s: s∈N, N içersindeki diğer bütün yönlendiricilere olan en kısa yolu,
- M: kaynaktan hedefe doğru birleştirilmiş yönlendirici kümesini,
- C(n): s'den her bir n yönlendiricisine olan uzaklığı göstermektedir.

Her bir yönlendirici için onaylanmış ve kesin olmayan liste içeren bir yönlendirme tablosu oluşturulur. Her bir liste, giriş bilgisini içermektedir. Bunlar hedef, uzaklık ve sonraki yönlendirici bilgileri sırasında sayılabilir. Bu algoritmanın yönlendirme tablosunun nasıl oluşturulduğu Şekil 4.3'de gösterilmiştir [67].



Şekil 4.3. Bağlantı durum yönlendirme algoritması için örnek ağ topolojisi.

Şekil 4.3.'de A, B, C ve D yönlendiriciyi göstermektedir. Tablo 4.2.'de D yönlendiricisi için yönlendirme tablosu görülmektedir. Tablodaki her bir adımda görülen yollar hedef, uzaklık ve sonraki yönlendirici bilgileri sırasında yazılmıştır.

Tablo 4.2. D yönlendiricisi için yönlendirme tablosu.

Adım	Onaylanmış (En kısa yol)	Kesin Olmayan	Adım	Onaylanmış (En kısa yol)	Kesin Olmayan
1	D,0,-		**5**	D,0,- C,2,C B,5,B	A,12,C
2	D,0,-	B,11,B C,2,C	**6**	D,0,- C,2,C B,5,B	A,12,C
3	D,0,- C,2,C	B,11,B	**7**	D,0,- C,2,C B,5,B	A,9,C
4	D,0,- C,2,C	B,5,B A,12,C	**8**	D,0,- C,2,C B,5,B A,9,C	

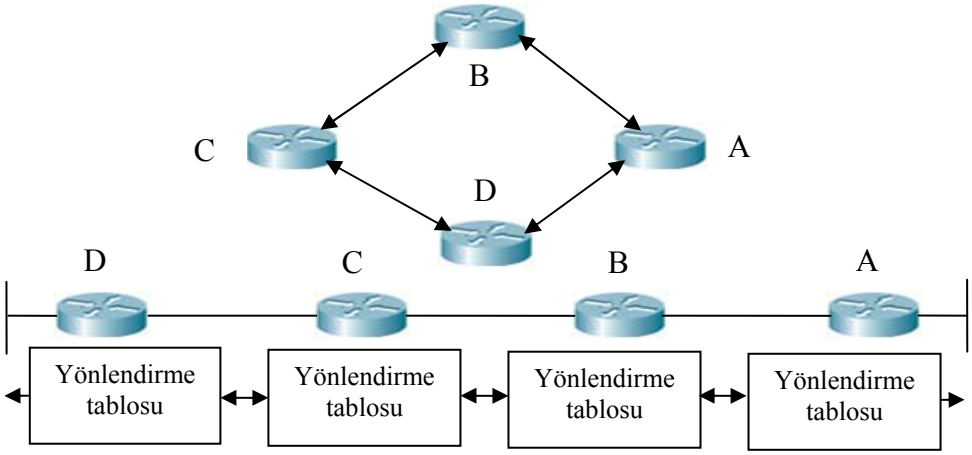
Bağlantı durum yönlendirme algoritması; çok fazla ağ trafiği oluşturmaz ve topolojideki değişikliği hızlı bir şekilde cevaplandırır. Her yönlendiricide geniş bir bilgi depolama gerektirmesi bu algoritmanın temel problemi olarak sayılabilir [67].

4.2.4. Uzaklık Vektörü Algoritması

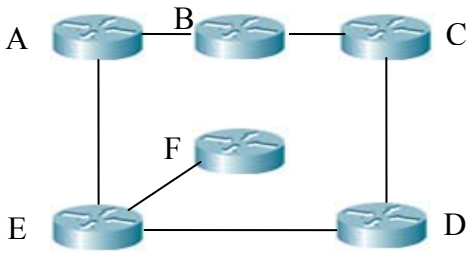
Bu algoritmanın geliştiricilerinden biri Bellman (1957) olduğu için Bellman-Ford yönlendirme algoritması olarak veya Ford ve Fulkerson (1962) tarafından geliştirildiği için Ford-Fulkerson algoritması olarak adlandırılabilir. Uzaklık vektörü algoritması ile yönlendirme tablosunda, bir yönlendiriciden diğer yönlendiricilere olan aradaki yönlendirici sayısı olarak en kısa uzaklık bilgisi ve bunu saptayabilmek için izlenmesi gereken yönlendirici sırası tutulmaktadır [62].

Her yönlendirici yalnızca bağlı olduğu yönlendiriciyi gördüğü için bütün ağ topolojisi hakkında bilgisi yoktur. Ağ topolojisinde bir değişiklik olduğu zaman yönlendirme tablosunda güncelleme yapılır ve herhangi bir yönlendirici, yönlendirme tablosunu direk bağlı olduğu yönlendiriciden alır. Örneğin Şekil 4.4.'deki B, A yönlendiricisinden

bilgileri uzaklık vektör numarasıyla birlikte alır. B yönlendiricisi gelen yeni yönlendirme tablosunu C'ye, C yönlendiricisi ise D yönlendiricisine bu bilgiyi göndermektedir [68].



Şekil 4.4. Yönlendiricilerin direk bağlı olduğu yönlendiriciden yönlendirme tablosunu alması.



Şekil 4.5. Örnek ağ topolojisi.

Tablo 4.3. Her bir yönlendiricideki başlangıç uzaklıkları.

Yönlendiricide Depolanan Bilgi	Yönlendiriciler arası uzaklık					
	A	B	C	D	E	F
A	0	1	∞	∞	1	∞
B	1	0	1	∞	∞	∞
C	∞	1	0	1	∞	∞
D	∞	∞	1	0	1	∞
E	1	∞	∞	1	0	1
F	∞	∞	∞	∞	1	0

Uzaklık vektör algoritmasının çalışma prensibi Şekil 4.5.'de bir örnek üzerinde açıklanmaktadır. Burada A, B, C, D, E ve F yönlendiriciyi göstermektedir. Ayrıca

birbirine direk bağlı olan bütün yönlendiriciler arasındaki maliyet değeri 1, bağlı olmayanlar ise ∞ olarak kabul edilmektedir. Her bir yönlendiricinin başlangıç uzaklıkları Tablo 4.3.'de, A yönlendiricisinin başlangıç yönlendirme tablosu ise Tablo 4.4.'de gösterilmektedir.

Tablo 4.4. A yönlendiricisinin başlangıç yönlendirme tablosu.

Hedef	Maliyet	Sonraki Yönlendirici
B	1	B
C	∞	-
D	∞	-
E	1	E
F	∞	-

Uzaklık vektör algoritmasının sonraki aşamasında, her bir yönlendirici direk bağlı olduğu komşu yönlendiricilere maliyet bilgilerini göndermektedir. Örneğin, E yönlendiricisi A'ya, D yönlendiricisine olan maliyetin 1 olduğu ve aynı zamanda da A ve E yönlendiricisine ulaşmanın maliyetinin de 1 olduğu bilgisini gönderir. Ayrıca D'ye E vasıtasıyla ulaşabileceği bilgisini de göndermektedir. Geçerli olan maliyet ∞ iken, aslında gerçek maliyet 2 olmaktadır. Bu yüzden A yönlendiricisi, maliyet değeri 2 olarak E vasıtasıyla D yönlendiricisine ulaşabilmektedir.

Tablo 4.5. Her bir yönlendiricideki son mesafeler.

Yönlendiricide Depolanan Bilgi	Yönlendiriciler arası uzaklık					
	A	B	C	D	E	F
A	0	1	2	2	1	2
B	1	0	1	2	2	3
C	2	1	0	1	2	3
D	2	2	1	0	1	2
E	1	2	2	1	0	1
F	2	3	3	2	1	0

Tablo 4.6. A yönlendiricisinin son yönlendirme tablosu.

Hedef	Maliyet	Sonraki yönlendirici
B	1	B
C	2	B
D	2	E
E	1	E
F	2	E

A, ağdaki bütün yönlendiriciler için yönlendirme tablosunu maliyet ve sonraki yönlendirici bilgileriyle birlikte güncelleyebilir. Yeni oluşturulan uzaklık bilgisi Tablo 4.5.'te, yönlendirme tablosu ise Tablo 4.6.'da gösterilmektedir.

Uzaklık vektörü algoritmasının yapısı için aşağıdaki varsayımlar yapılırsa [69]:

- $D_x[y]$: yönlendiricilerin ağırlığı,
- w(x; y): x ve y yönlendiricileri arasındaki bağlantı, (x ve y arasında doğrudan bağlantı yok ise $D_x[y]= \infty$ değerini almaktadır.)
- Cx[w]: x yönlendiricisinden w yönlendiricisine giderken hangi yönlendiriciden geçilmesi gerektiği,
- x: her bir yönlendiricinin bağlı oldukları yönlendiriciye olan uzaklık vektörü bilgisi olarak tanımlanabilir.

Her bir yönlendirici direk bağlı oldukları yönlendiricilere x bilgisini göndermekte ve her yönlendirici yönlendirme tablosundaki x bilgisini aşağıdaki hesaplama ile güncellemektedir. Buna göre algoritma:

for x'e bağlı her bir y yönlendiricisi için **do**
for birbirine bağlı w yönlendiricisi için **do**
if Dx[w] > w(x; y) + Dy[w] **then**
(w yönlendiricisine giderken y'den geçmek daha kısadır)
Dx[w] = w(x; y) + Dy[w]
Cx[w] = y
end if
end for
end for

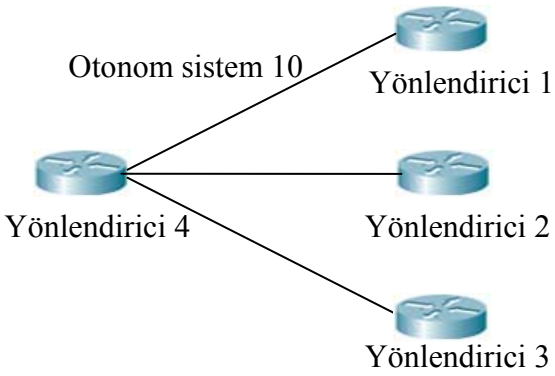
Her bir yönlendiricinin x uzaklık vektör bilgisi, komşu yönlendiricilere olan minimum uzaklık bilgisinin toplanmasıyla oluşturulur (w(x; y) + Dy[w]) [69].

En çok kullanılan yönlendirme algoritmalarından uzaklık vektör ve bağlantı durum algoritmaları kıyaslanacak olursa, uzaklık vektör algoritması sadece direk bağlı olduğu yönlendiriciler hakkında bilgi sahibiyken, bağlantı durum yönlendirme algoritması bütün ağ topolojisi hakkında bilgi sahibidir. Bu yüzden uzaklık vektörü algoritmasında

yönlendirme bilgisinin yayılımı daha yavaş olmakla beraber bağlantı durum algoritması daha fazla bilgi depolaması gerektirmektedir.

4.2.5. Yol Vektörü Algoritması

Aynı yönlendirme politikası içerisinde çalışan yönlendiricilerin oluşturduğu ağa otonom sistem (Autonomous System – AS) denir. Bu ağ bölgesi içerisinde tek bir yönlendirme protokolü kullanılır. Otonom sistemler benzeri olmayan bir numara atanmak üzere bölge numarasıyla tanımlanmaktadır [70]. Şekil 4.6.'da dört yönlendiriciden oluşan on kimlik numarasına sahip bir otonom sistem gösterilmektedir.



Şekil 4.6. Otonom sistem örneği.

Yol vektörü algoritması, yol bilgisini dinamik olarak güncelleyen yönlendirme algoritmasıdır. Bu algoritmanın yapısı uzaklık vektörüne çok benzemektedir. Bu algoritmada hedefe ulaşmak için otonom sistemler üzerinden yönlendirme gerçekleştirilir. Yönlendirme tablosunda hedefe ulaşma yolu ve sonraki yönlendirici bilgileri tutulmaktadır. Otonom sistem içerisindeki yönlendirme politikasına göre yol vektörü mesajları gönderilir. Eğer gelen mesaj bu politikaya uygun ise yönlendirme tablosu, hedefe ulaşma yolu ve sonraki yönlendirici bilgisiyle gönderilir. Bu mesaj otonom sistem numarasıyla birlikte sonraki yönlendiricinin girişi olarak değiştirilir [71].

4.3. Yönlendirme Protokolleri

Kullanılan yönlendirme tablosundaki bilgiler doğrultusunda hedef adrese IP paketlerinin gönderilebilmesi için yönlendirme işleminin gerçekleşmesini sağlayan

kurallar topluluğuna yönlendirme protokolü denir. Yönlendirme protokollerinin temel fonksiyonları aşağıdaki gibi sıralanabilir.

- Ağın topolojisi ve bağlantı durumu hakkında bilgi sahibi olmak,
- Ağda bulunan her yön için en kısa yolu hesaplamak,
- Kaynaktan hedef yönlendiriciye bilgileri yönlendirmek.

Bütün yönlendirme protokolleri belli metrik değerlere göre ağdaki en iyi yolu bulmaktadır. En uygun yolu nasıl hesapladıkları yönlendirme protokollerinin RFC standardında ayrıntılı bir şekilde tanımlanmıştır [72].

4.3.1. Yönlendirme Protokollerinin Gelişim Süreci

Dinamik yönlendirme protokolleri, 1960'lı yıllardan beri bilgisayar ağlarında kullanılmaktadır. RIP'in ilk versiyonu 1982'de yayımlanmasına karşın, protokol içerisindeki bazı basit algoritmalar 1969'lu yılların daha öncesinde ARPANET üzerinde kullanılmıştır. Yönlendirme protokollerinin tarihi gelişimi Tablo 4.7.'de verilmiştir [73]

Tablo 4.7. IP yönlendirme protokollerinin tarihi gelişimi.

EGP	IGRP	RIPv1	IS-IS	OSPFv2	EIGRP	RIPv2	BGP	RIPng	BGPv6 ve OSPFv3	IS-ISv6
1982	1985	1988	1990	1991	1992	1994	1995	1997	1999	2000

İlk yönlendirme protokolü RIP ve bu protokolün yeni versiyonu ise RIPv2'dir. RIPv2 versiyonu da geniş bilgisayar ağlarında yeterli değildir. Geniş ağların ihtiyaçlarını karşılamak için iki gelişmiş yönlendirme protokolü oluşturulmuştur. Bunlar, OSPF (Open Shortest Path First - İlk En Kısa Açık Yol) ve IS-IS (Intermediate System-to-Intermediate System – Ara Sistemden Ara Sisteme)'dir. Aynı zamanda Cisco tarafından geliştirilmiş olan IGRP (Interior Gateway Routing Protocol – İç Ağ Geçit Yönlendirme Protokolü) ve EIGRP (Enhanced IGRP – İyileştirilmiş IGRP) protokollerinden EIGRP, geniş bilgisayar ağlarında ihtiyaçları karşılayabilmektedir [73].

Bu protokollere ilaveten, farklı bilgisayar ağlarının birbirleri arasında yönlendirme işlemini gerçekleştirmesi gerekmektedir. BGP (Border Gateway Protocol – Sınır Geçit

Protokolü); ISP (Internet Service Provider – İnternet Servis Sağlayıcı) ve yönlendiriciler arasında, ISP ve istemciler arası yönlendirme bilgisi değişimi için kullanılmaktadır.

Birçok IP kullanıcısının oluşmasıyla birlikte IPv4 adres alanı kullanımı kısıtlanmıştır. Bu yüzden IPv6'ya ihtiyaç duyulmuştur. IPv6 tabanlı ağlarda iletişimi sağlamak için geliştirilen IP yönlendirme protokollerinin yeni versiyonları aşağıda listelenmiştir [73].

- RIPng (RIP next generation - RIP sonraki nesil)
- EIGRPv6 (EIGRP for IPv6 – IPv6 için EIGRP)
- OSPFv3 (OSPF version 3 – OSPF versiyon 3)
- IS-ISv6 (IS-IS for IPv6 – IPv6 için IS-IS)
- BGPv6 (BGPv4 for IPv6 – IPv6 için BGPv4)

4.3.2. Yönlendirme Protokollerinin Sınıflandırılması

Yönlendiriciler yönlendirme işlemini statik ve dinamik yönlendirme olarak iki farklı şekilde yapmaktadır [74]. Bu yönlendirme çeşitleri aşağıda açıklanmıştır.

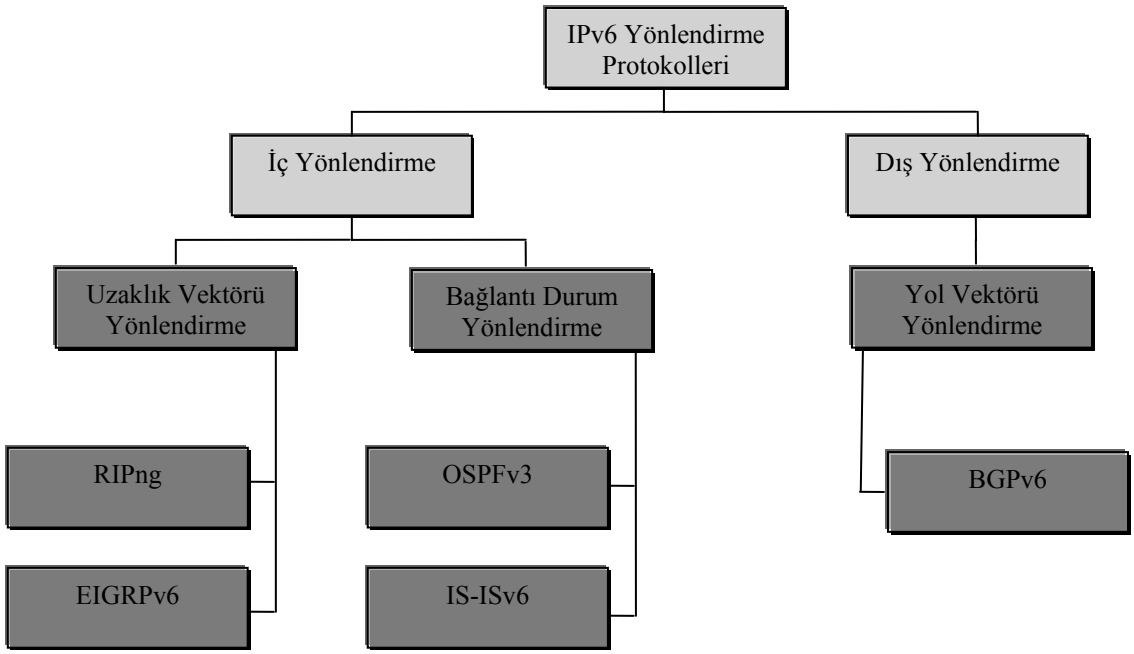
- **Statik yönlendirme:** Yönlendirme tablosu girişi el ile yapılandırılmış ve ağ topolojisindeki değişiklerden etkilenmeyen yönlendirmeye statik yönlendirme denir. Yönlendirme tablosundaki ağ topoloji bilgisi, yönlendirme giriş bilgileri ve değişiklikleri elle yapılandırılmaktadır. Bu yüzden statik yönlendirme küçük ağlar için iyi çalışabilmektedir.
- **Dinamik yönlendirme:** Ağ topolojisindeki değişiklilerde yönlendirme tablosu girişleri otomatik olarak güncellenebilen yönlendirmeye dinamik yönlendirme denir. Yönlendiriciler arasındaki iletişimde yönlendirici tabloları, yönlendirme protokolleriyle otomatik olarak güncellenmektedir. Dinamik yönlendirme daha az onarım istediğinden geniş ağlarda daha iyi sonuç verebilmekte ve ağ hataları daha kolay bulunabilmektedir.

Dinamik yönlendirmede kullanılan yönlendirme protokolleri, Şekil 4.7.'de gösterildiği gibi iç ve dış yönlendirme olarak iki ana gurupta sınıflandırılabilir [72,73,75]. İç yönlendirme protokolleri uzaklık vektörü ve bağlantı durum yönlendirme protokolleri olarak sınıflandırılmaktadır.

1. **İç Yönlendirme Protokolleri**: Yönlendirme işlemi bütün ağ içerisinde kendi aralarında gerçekleşir. İç yönlendirme protokolleri küçük internet içerisindeki yönlendiricilere, durum ve bağlantıları hakkında bilgi sağlar ve genellikle daha az karmaşık yönlendirme mimarisini destekler. Bu protokoller IGP (Interior Gateway Protocol – Dahili Geçit Protokol) olarak da adlandırılır. IGP protokollerinin IPv6 versiyonları aşağıdaki gibi listelenebilir.

    a. RIPng
    b. EIGRPv6
    c. OSPFv3
    d. IS-ISv6

2. **Dış Yönlendirme Protokolleri**: Yönlendirme işlemi bütün ağ ve geniş internet ağı arasında gerçekleşmektedir. Dış yönlendirme protokolleri, yönlendiricilerin durum ve bağlantıları hakkındaki değişiklikleri hızlı ve verimli bir şekilde haberleşen yönlendiricilere iletmek zorundadır. Bu protokoller EGP (Exterior Gateway Protocol – Harici Geçit Protokol) olarak da adlandırılır ve temel olarak kullanılan EGP protokolüdür. Bu protokol IPv6'da BGPv6 şeklinde adlandırılmaktadır.



Şekil 4.7. IPv6 yönlendirme protokolleri.

4.4. IPv6'da Kullanılan Yönlendirme Protokolleri

Yönlendirme işlemi IPv4 ve IPv6'da aynı mekanizma kullanılarak gerçekleştirilir. IPv6 yönlendirmede, yönlendirme protokolleri tarafından daha uzun adres satırı kullanılarak yönlendirme işlemi gerçekleştirilebilmektedir [75].

IPv4 için kullanılan yönlendirme protokollerinin yeni versiyonları geliştirilerek IPv6'da kullanılır hale getirilmiştir. RIP'in sonraki versiyonu olan RIPv2'den minimum değişiklikle geliştirilmiş RIPng, RIP'den daha farklı tasarlandığı için yeni protokol olarak da değerlendirilebilir [19]. RIP'in IPv6 versiyonu olan RIPng, RFC 2080 standardında tanımlanmıştır [76]. OSPF'nin IPv6 versiyonu olan OSPFv3, RFC 2740 standardında tanımlanmıştır [77]. IS-IS protokolünün IPv6'yı desteklemesi İnternet Taslak (Internet Draft) dokümanı içerisinde tanıtılmıştır [78]. İnternet Taslak dokümanı, IETF tarafından yayımlanan RFC niteliğindeki doküman olarak bilinmektedir [79].

BGP-4 (BGP versiyon 4) [80] yönlendirme protokolünün de IPv6'yı desteklemesi için RFC 2545 [81] standardındaki BGP-4 geliştirilmiş ve BGP-4+ olarak adlandırılmıştır [19]. BGP-4+ protokolü BGPv6 olarak da bilinmektedir [73].

Cisco tarafından geliştirilmiş EIGRPv6 [73] yönlendirme protokolü ve IETF tarafından tanımlanmış RIPng, OSPFv3, IS-ISv6 ve BGP-4+ [74] yönlendirme protokolleri IPv6'yı desteklemek için geliştirilmiş yeni protokoller olup detaylı bilgiler aşağıda verilmiştir.

4.4.1. RIPng

RIP, uzaklık vektör algoritması temelli 1988 yılında IETF tarafından standartlaştırılmış IPv4 ağları arasında yönlendirmeyi sağlamak amacıyla geliştirilmiş bir yönlendirme protokolüdür. Bu protokol, atlama sayısına (hop count) bakarak hedef ve kaynak arasında en az kaç yönlendiriciden atlanacaksa o yolu yönlendirme yolu olarak tercih etmektedir. RIP'in en önemli dezavantajı, diğer yollar arasındaki bant genişliği ve gecikme gibi faktörleri göz önünde bulundurmamasıdır. RIP'in IPv6 yönlendirmede kullanılmak için geliştirilmiş versiyonu RIPng'dir [10,72].

RIPng, Ocak 1997'de RFC 2080 [76] standardında tanımlanan ve uzaklık vektörü algoritması temelli yönlendirme algoritmasıdır. Bu protokol, RIPv1 ve RIPv2'den IPv6 yönlendirmeyi desteklemek için geliştirilmiştir. RIPng mesajlarını IPv6 adresi olan alıcı adresinin FF02::9 olduğu çoklu yayın adresine gönderir. Temel olarak bu protokolün nasıl çalıştığı aşağıda açıklanmıştır [10].

- Yönlendirici, yönlendirme bilgisini ve direk bağlı olduğu yönlendiricileri belirli zaman aralıklarında güncelleme mesajlarıyla göndermekte ve almaktadır.
- Yönlendirici direk bağlı olduğu yönlendiriciden güncelleme mesajı aldığında, bu bilgiler doğrultusunda yönlendirme tablosunu güncellemektedir.

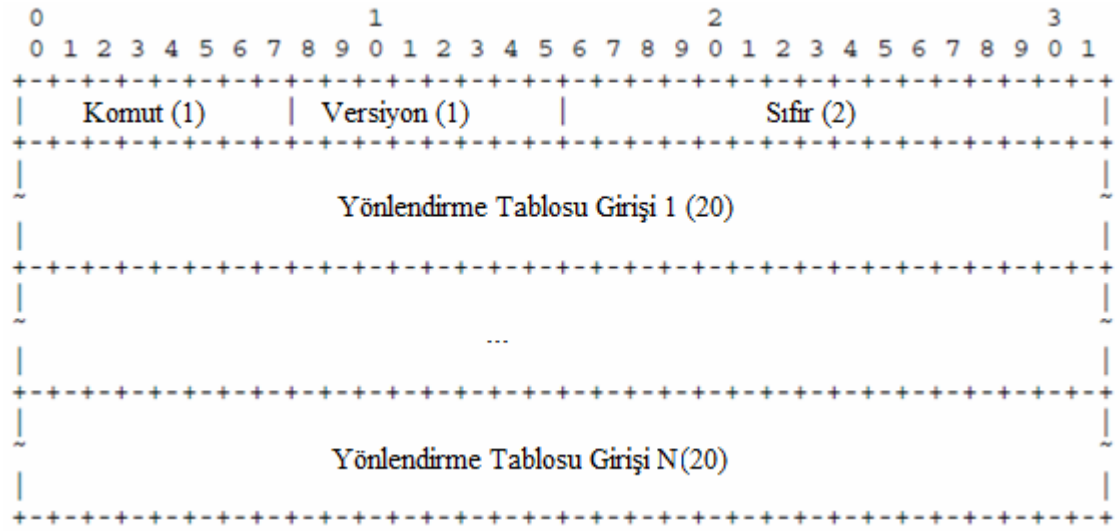
RIPng, en fazla 15 atlama yönlendiriciden ileriye yönlendirmeye izin verir. Sistem yöneticileri, her bir ağ için metrik değer 15 olacak şeklinde tanımlar. Bu metrik değere ilaveten her bir ağ için IPv6 hedef adres önek ve önek uzunluğu metrik değerle ilişkilendirilir. Bu işlem, RIPng'de belirlenmiş bir durum değil, sistem yöneticileri tarafından yapılan bir işlemdir [76].

RIPng yönlendirme tablosunda, ulaşılabilir hedefler için her bir giriş en azından aşağıdaki bilgileri içermelidir [75,76].

- Hedefin IPv6 öneki,
- Metrik değer: Hedef ile kaynak yönlendirici arasındaki maliyet bilgisi,
- Sonraki yönlendiricinin IPv6 adres bilgisi (sonraki atlama vb.). Eğer hedef ile kaynak yönlendirici direk bağlı ise bu bilgiye gerek yoktur,
- Yol değişim bayrağı: İzlenecek yolun değiştiğini gösteren bilgi,
- Zamanlayıcı: Yol bilgisinin gönderildiğini ve zaman aşımına uğrayıp uğramadığını gösteren bilgidir.

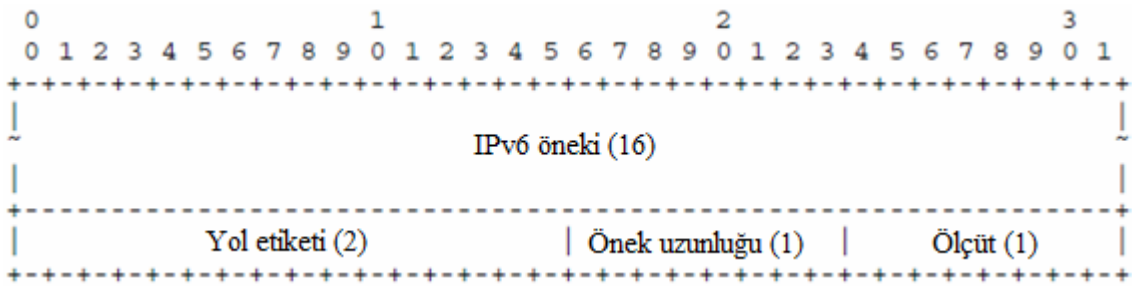
4.4.1.1. Mesaj Formatı

RIPng, UDP temelli bir protokoldür. Yönlendiriciler RIPng protokolünü kullanırken UDP 521 numaralı porttan UDP mesajlarını almakta ve göndermektedir. RIPng mesaj formatı Şekil 4.8.'de gösterilmektedir [76].



Şekil 4.8. RIPng mesaj formatı.

Buradaki her bir RTE (Route Table Entry – Yönlendirme Tablosu Girişi) formatı ise Şekil 4.9.'da gösterilmektedir.



Şekil 4.9. RIPng RTE formatı [76].

RTE'ler, 16 bayt uzunluğunda IPv6 öneki, 2 bayt uzunluğunda yol etiketi (route tag), 1 bayt uzunluğunda önek uzunluğu (prefix length) ve 1 bayt uzunluğunda yönlendirme ölçüt (routing metric) alanları üzerinde yönlendirme bilgilerini taşımaktadır. RIPng mesajı, yerel MTU'nun izin verdiği kadar birçok RTE'yi taşıyabilmektedir. MTU'ya özgü maksimum RTE sayısı aşağıdaki adımlarla hesaplanabilir [76,82].

- Sekizli MTU büyüklüğü alınır,
- O değerden; IPv6, UDP ve RIPng başlık büyüklükleri çıkarılır,
- Sonuç RTE'nin büyüklüğüne bölünür ve en yakın aşağı sayıya yuvarlanır.

Böylece standart başlığı oluşturup kullanmak için 40 bayt uzunluğundaki IPv6, 8 bayt uzunluğundaki UDP ve 4 bayt uzunluğundaki RIPng başlıklarının toplam büyüklüğü yerel MTU'dan çıkarılarak güvenli bir başlık elde edilir. RTE'nin uzunluğu 20 bayttır. Örneğin, MTU bağlantısı 1500 bayt olarak alındığında RTE hesaplaması aşağıdaki gibi yapılabilir.

1500 - 40 - 8 - 4 = 1448
1448 / 20 = 72.4

Sonuç olarak, her RIPng yönlendirme mesajında 72 RTE iletilebileceği görülmektedir [75,76].

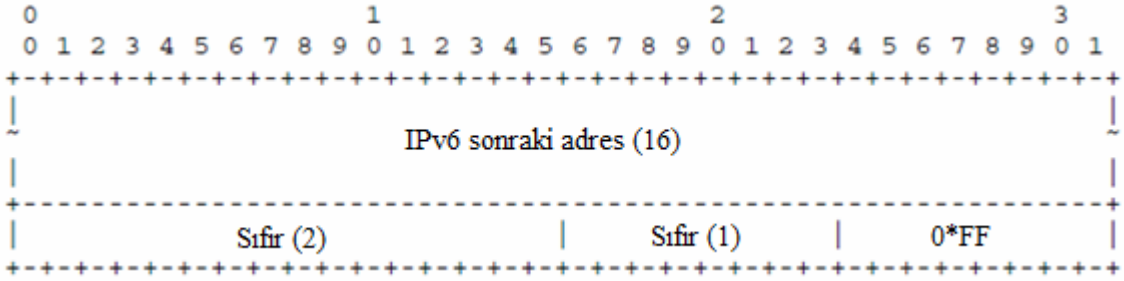
RIPng başlığındaki her mesaj, 1 bayt uzunluğunda komut (command) ve 1 bayt uzunluğunda versiyon bilgilerini içermektedir. Versiyon alanına 1 değeri atanmaktadır. Komut alanı, bu mesajın amacını açıkça belirtmek için kullanılmaktadır. Komut alanı, istek ve yanıt şeklinde iki farklı komut olarak tanımlanmıştır [76, 82]. Bu komutlar aşağıdaki gibi açıklanabilir.

- **İstek:** Yönlendiriciye, yönlendirme tablosunun tamamının mı yoksa belirli bir kısmının mı gönderileceğini sormak için kullanılır.
- **Yanıt:** Yönlendirme tablolarının tamamının mı yoksa belirli bir kısmının mı kullanılacağı bilgisini içerir. Bu mesaj, isteğe özgü yanıt veya yönlendirici tarafından düzenli bir şekilde gönderilen bir mesaj da olabilir.

Yol etiket alanı, RIPng için izlenecek yolun iç veya dış yönlendiriciden geldiğini saptamak için kullanılır. Önek uzunluk alanı, 0 ile 128 arasında bit olarak önekin uzunluğunu gösteren önemli bir kısımdır. Metrik, 1 ile 15 arasında değer içeren bir alandır. 16 değerini aldığında ise hedefi ulaşılamaz olarak gösterir [76].

4.4.1.2. Sonraki Yönlendirici

RIPng, RIPv2'ye birçok yönden benzer biçimde IPv6 adresinin sonraki yönlendirici adres bilgisini RTE şeklinde belirtir. Fakat RIPng protokolünde sonraki yönlendirici alanı her RTE için yaklaşık iki katı büyüklüğündedir. Sonraki yönlendirici RTE formatı Şekil 4.10.'da gösterilmektedir [76].



Şekil 4.10. RIPng sonraki yönlendirici RTE formatı.

Sonraki yönlendirici adres RTE'si, RIPng mesajının sonuna kadar veya diğer sonraki yönlendirici adres RTE'si ile karşılaşıncaya kadar bütün RTE'leri göstermektedir [75]. RTE'nin 0xFF değeri metrik alanıdır. IPv6 önek alanı sonraki yönlendiricinin adresini belirtir. Yol etiketi ve önek uzunluğu sonraki yönlendirici RTE'sinde sıfır (0:0:0:0:0:0:0:0) olarak atanmalıdır [76].

4.4.1.3. Zamanlayıcı

RIPng protokolünde yönlendirme bilgilerinin güncellenmesini kontrol etmek için güncelleme zamanlayıcısı (update timer), zaman aşımı zamanlayıcısı (timeout timer) ve atık yığın zamanlayıcısı (garbage-collection timer) vardır [82].

Güncelleme zamanlayıcısı, her 30 saniyede bir RIPng işleminde istenen yanıt mesajın komşu yönlendiricilere gönderilmesi için yönlendiriciyi uyarmaktadır. Zaman aşımı zamanlayıcısı, yolun artık geçerli olmadığını gösterir. Geçerli olmayan yol bilgisi komşu yönlendiricilere de ulaştığında artık tamamen yönlendirme tablosundan kaldırılır. Atık yığın zamanlayıcısı ise yolun geçerli olmadığı anda yönlendirme tablosundan kaldırılmasını sağlar [76].

4.4.1.4. İstek ve Yanıt Mesajı

İstek mesajı yönlendiriciye, yönlendirme tablosunun tamamının mı yoksa belirli bir kısmının mı gönderileceğini sormak için kullanılır. Genel ve özel olmak üzere iki tip istek mesajı vardır. Genel istek mesajı, yönlendirici tarafından direk bağlı olduğu komşu yönlendiricilere yönlendirme tablolarını göndermek için iletilen bir mesajdır. Komşu yönlendiriciler ise bu mesaja yanıt olarak yönlendirme tablolarını gönderir. Özel istek

mesajı, yönlendirme tablosunun tamamının gittiği yeri veya belirli bir kısmının gittiği yeri izlenmek için gönderilen bir mesajdır. Mesajı alan yönlendirici, istenen bilgileri yönlendirme tablosuyla birlikte yanıtlamaktadır. Genel istek mesajı IPv6 hedef adres olarak FF02::9 çoklu adresi kullanırken özel istek mesajı sorgulanan yönlendiricinin yerel veya küresel tekli adresini kullanmaktadır.

Yanıt mesajı yönlendiriciye, yönlendirme tablolarının tamamının mı yoksa belirli bir kısmının mı kullanılacağı bilgisini cevaplamak için gönderilir. İstenilmiş (solicited) ve istenilmemiş (unsolicited) olmak üzere iki tip yanıt mesajı vardır. İstenilmiş yanıt mesajı, istek mesajına karşı cevap olarak gönderilen mesaj olarak bilinmektedir. İstenilmemiş yanıt mesajı ise periyodik veya tetiklenmiş güncelleme işlemi yoluyla gönderilen bir mesajdır. Periyodik olarak gerçekleştirilen güncelleme işlemi, güncelleme zamanlayıcısının süresi bitmiş bütün yönlendirme tablosunu kontrol etmektedir. Tetiklenerek gerçekleştirilen güncelleme işlemi ise yol değişim bayrağı durumu değiştiği anda yapılmaktadır. İstenilmiş yanıt mesajı IPv6 hedef adres olarak istenilen mesajın kaynak IPv6 adresini kullanırken, istenilmemiş yanıt mesajı ise FF02::9 çoklu adresini kullanır [82].

4.4.2. OSPFv3

Yönlendirme protokolü olarak OSPF kullanan bütün yönlendiriciler kendi bağlantı durum bilgisini komşu yönlendiricilerine gönderir. Böylece yönlendiricilerin tamamı birbirleri hakkındaki bağlantı durum bilgisine ulaşmış olur. Yönlendiriciler, bağlantı durum bilgilerini aldıktan sonra yönlendirme veritabanını oluştururlar. Eğer ağın topolojisinde herhangi bir değişim olursa, sadece bu güncelleme bilgisi komşu yönlendiricilere gönderilir ve ağdaki tüm yönlendiriciler yönlendirme veritabanlarını günceller. Yönlendiriciler bu bilgiler doğrultusunda her hedef için en kısa yolu hesaplamaktadır. OSPF protokolü nispeten geniş ağlarda yönlendirme amacıyla tasarlanmış olup, ağ üzerinde alt ağların tanımlanmasına izin veren bir protokoldür [72].

RIP'in bazı eksikliklerine karşın geliştirilmiş olan OSPF, yönlendirme bilgisini RIP'den daha hızlı bir şekilde iletmekte ve çok daha fazla yönlendirme tablosunu barındırmaktadır. RFC 2328 standardında IPv4 için tanımlanan OSPFv2 (OSPF version 2 – OSPF versiyon 2), bağlantı durum algoritması kullanarak yönlendirme işleminin

gerçekleştiği OSPF protokolünün yeni bir versiyonudur. OSPF protokolünün IPv6 yönlendirmede kullanılmak için geliştirilmiş versiyonu "OSPF for IPv6" olarak da bilinen RFC 2740 standardındaki OSPFv3'dür [75,82].

OSPFv3 protokolünün, 32 yerine 128 bit IP yönlendirme işlemini uygunlaştırmasına ilaveten OSPFv2 versiyonundan farklı yanları aşağıdaki gibi sıralanabilir [74,75].

- Her alt ağ yerine her link kullanılması,
- IPv6 adreslerinde OSPF paket başlığı kullanılmamaktadır. Yönlendirici IP adresleri yerine yönlendirici ID'nin yönlendirici tanımlamasında kullanılması,
- Yerel-bağlantı, bölge ve otonom sistem şeklinde üç farklı taşma alanı oluşturulması,
- IPv4'e tabi olan paket formatının IPv6'ya uyarlanması,
- IPv6 adres ve önekini taşıması için LSA (Link State Advertisement - Bağlantı Durum Mesajı)'nın yeniden tanımlanması.

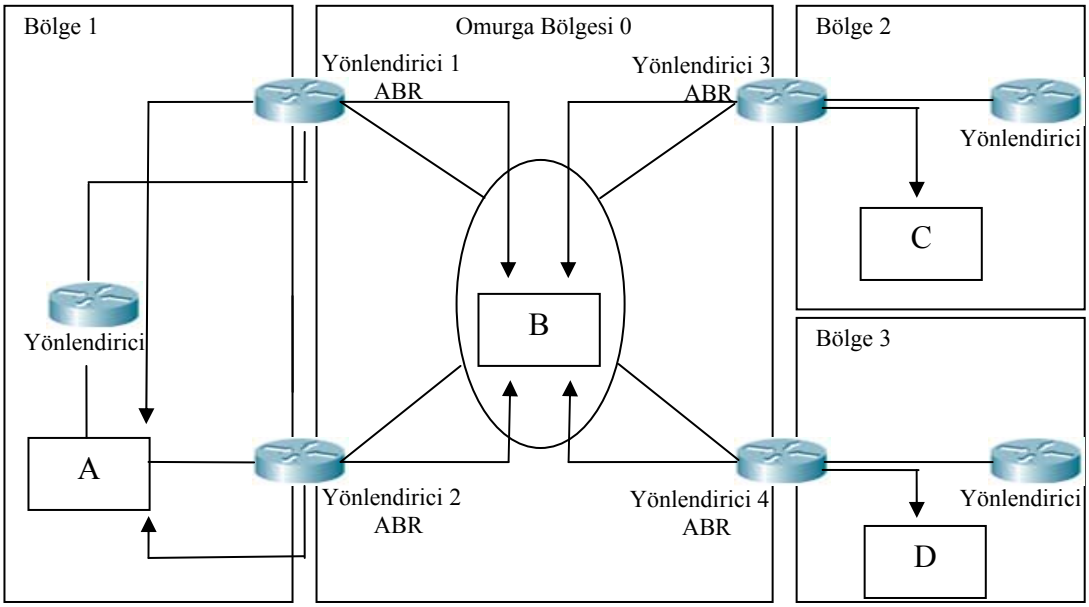
4.4.2.1. OSPF Bölgeleri ve Dış Yönlendirme

OSPF protokolü, oldukça geniş bir LSDB (Link State Database - Bağlantı Durum Veritabanı)'ye sahiptir. Geniş veritabanındaki işlem, işlemci ve hafızada yoğunluğa sebep olmaktadır. Otonom sistem içerisindeki her yönlendirici, veritabanı içerisinde değişiklikler yapar. OSPF, otonom sistemi bölgelere ayırarak işlem yükünü azaltır [82].

Bir bölgenin içerisindeki yönlendiricilerin hepsi otonom sistemi oluşturur. Bağlantı durum mesajları bölgenin dışına gönderilmez. Bu mesajlar bölgenin veri yapısını oluşturur ve bölge LSDB'si olarak ta bilinmektedir. Bağlantı durum veritabanı, yönlendirici-LSA ve ağ-LSA şeklinde iki kategoriden oluşur. Yönlendirici ve ağ, diğer bölgenin içerisindeki herhangi bir bölgeden oluşur. Bir bölge içerisindeki her yönlendirici, aynı bölge içerisindeki bütün yolların En Kısa Yol ağacını (Shortest Path First tree – SPF tree) oluşturur. Bu yollar iç bölge yolları olarak, tek bir bölge içerisindeki bütün yönlendiriciler de iç yönlendirici olarak adlandırılır. ABR (Area Border Routers - Sınır Bölgesi Yönlendiricileri) dış bölgenin yönlendirme yollarını bulmayı sağlar. Bütün bölgeler kendi aralarındaki bağlantıyı sağlamak için, omurga bölgesi (backbone area) olarak adlandırılan tek bir ortak bölgeye doğrudan

bağlanmalıdır. Bu işlem, omurga bölgesinde bir arabirim ve yerel bölgede bir arabirime sahip sınır bölgesi yönlendiricileri tarafından gerçekleştirilir. Sınır bölgesi yönlendiricileri, yerel bölgedeki bütün yolların omurga bölgesine bağlanacağını bildirir. Bu mesajın üzerine de omurga bölgesi yollarının yerel bölgeye bağlanacağı bildirilir. Bu işlem, otonom sistem içerisindeki bütün dağıtılmış yolların kesinleşmesini sağlar. Omurga bölgesi, bütün bölge yollarını toplamakta ve yeniden dağıtmaktadır.

Otonom sistem içerisindeki yönlendirme, iki seviye içerisinde gerçekleşmektedir. Eğer paketlerin kaynak ve hedef IP adresleri aynı bölge içerisinde ise paket yalnızca bölge LSDB'sinden elde edilen bilgiyle gönderilir. Buna iç bölge yönlendirmesi (intra area routing) adı verilir. Eğer hedef adres bölgenin dışındaysa paket yerel bölgenin ABR'si tarafından gönderilmek zorundadır. Buna ise gömülü bölge yönlendirmesi (inter area routing) denir. Şekil 4.11. üzerinde OSPFv3 bölgeleri ve yönlendirme güncellemeleri gösterilmektedir [82].



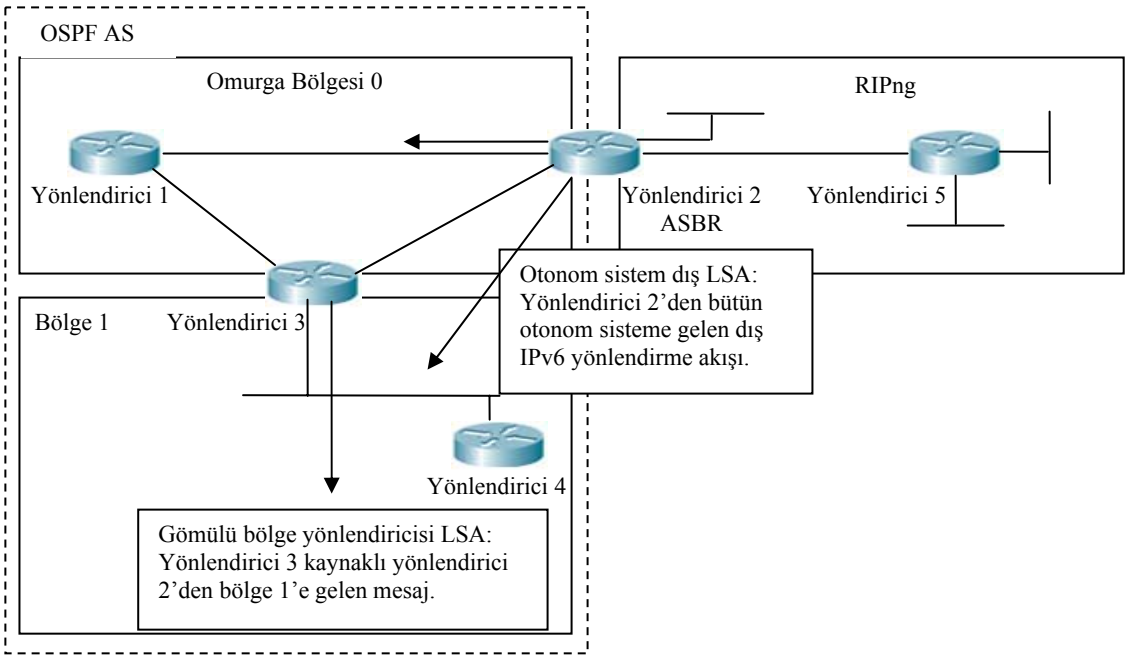
Şekil 4.11. OSPFv3 bölgeleri ve yönlendirme güncellemeleri.

Bu şekil üzerinden yönlendirme güncellemeleri aşağıda açıklanmıştır.

- (A) ABR 1 ve 2'den kaynaklanan omurga bölgesi, bölge 2 ve bölge 3'ün IPv6 yönlendirmesi için gömülü bölge bağlantı durum mesajını göstermektedir.

- (B) ABR 1, 2, 3 ve 4'ten kaynaklanan bölge 1, bölge 2 ve bölge 3'ün IPv6 yönlendirmesi için gömülü bölge bağlantı durum mesajını göstermektedir.
- (C) ABR 3'ten kaynaklanan omurga bölgesi, bölge 1 ve bölge 3'ün IPv6 yönlendirmesi için gömülü bölge bağlantı durum mesajını göstermektedir.
- (D) ABR 4'ten kaynaklanan omurga bölgesi, bölge 1 ve bölge 2'nin IPv6 yönlendirmesi için gömülü bölge bağlantı durum mesajını göstermektedir.

Yönlendirici, RIP ve BGP gibi farklı kaynaklardan gelen yönlendirme işlemini gerçekleştirebilir. OSPF kaynağından gelmeyen her yönlendirme, OSPF dış yönlendirmesi olarak düşünülür ve OSPF protokolüne eklenir. Dış yönlendirmeyi OSPF'ye eklemek için, yönlendiricinin en az bir arabirimini OSPF protokolüyle yapılandırılarak bu arabirimin OSPF olmayan ağları tanıması sağlanmaktadır. Bu yönlendirici, ASBR (Autonomous System Border Router - Otonom Sistem Sınır Yönlendiricisi) olarak isimlendirilir. Her dış yönlendirme için tek bir otonom sistem dış bağlantı durum mesajı kullanılarak dış yönlendirme gerçekleştirilir. Şekil 4.12.'de dış yönlendirmelerin OSPF protokolü yönlendirmesine eklendiği gösterilmektedir [82].

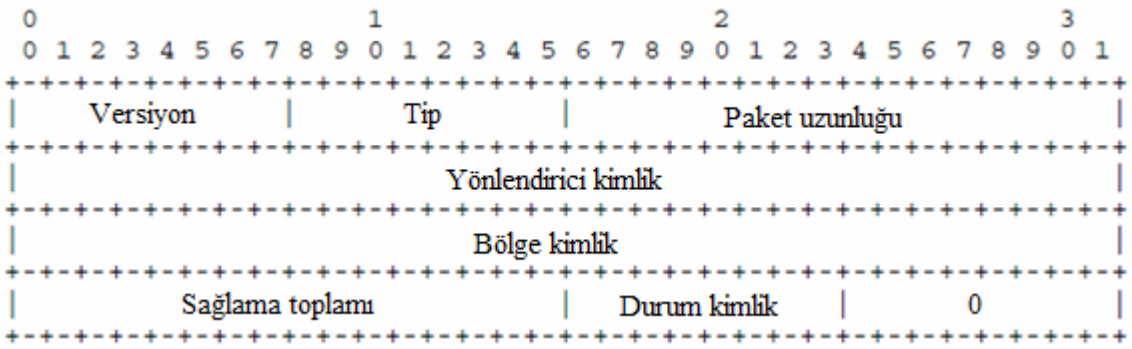


Şekil 4.12. OSPF'ye gelen dış yönlendirmeler.

4.4.2.2. Mesaj Formatı

OSPF paketleri, IPv6 başlığının sonraki başlık alanı için TCP veya UDP yerine direk olarak 89 numaralı port numarasını kullanır. IPv6 başlığı 40 bayt, OSPFv3 başlığı ise 16 bayt büyüklüğündedir. OSPFv3 mesaj formatı Şekil 4.13.'de, başlık formatı ise Şekil 4.14.'de gösterilmektedir [82].

Şekil 4.13. OSPFv3 mesaj formatı.



Şekil 4.14. OSPFv3 paket başlık formatı [77].

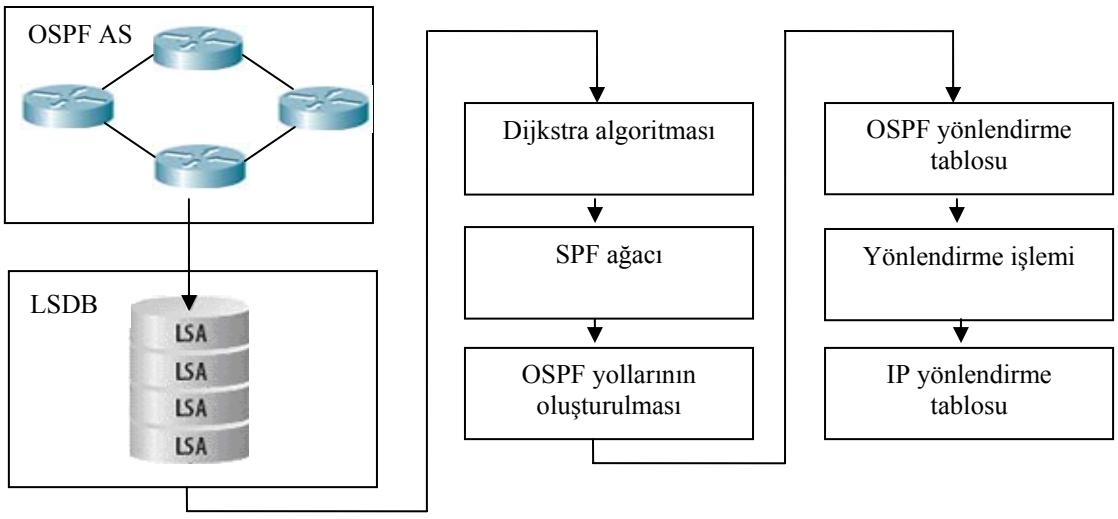
Tablo 4.8. OSPFv3 paket tipleri.

Paket Tipi	**İsmi**	**Açıklaması**
1	Merhaba (Hello)	Periyodik olarak komşu bağlantıları kurmak ve sürdürmek için bütün yönlendiricilere gönderilen pakettir.
2	Veritabanı Tanımlayıcısı (Database Description)	Bağlantı durum veritabanının içeriğini tanımlar.
3	Bağlantı Durum İsteği (Link State Request)	LSA değiştiği veya kaybolduğunda gönderilir.
4	Bağlantı Durum Güncellemesi (Link State Update)	LSA akışını yerine getirir. Kaynaktan diğer bir yönlendiriciye atlanırken bağlantı durum mesajlarını taşır.
5	LSA	Bağlantı durum mesajlarının alındığını bildirir.

OSPFv3 paket başlığında bulunan 1 bayt uzunluğundaki versiyon alanının değeri 3 ve versiyon numarasını, 2 bayt uzunluğundaki paket uzunluğu (packet length) alanı OSPF protokol paketinin uzunluğunu, 4 bayt uzunluğundaki yönlendirici kimlik (router id) alanı paketin kaynağını, 4 bayt uzunluğundaki bölge kimlik (area id) alanı OSPF paketlerinin ait olduğu bölgeyi, 2 bayt uzunluğundaki sağlama toplamı alanı 16 bit 1'e tamamlayıcı kullanarak bütün paketlerin toplamını, 1 bayt uzunluğundaki durum kimlik (instance id) alanı paketin ait olduğu durumu ve 1 bayt uzunluğundaki tip (type) alanı ise OSPF paketinin tipini belirtir. OSPFv3 paket tipleri Tablo 4.8.'de gösterilmektedir [77,82].

4.4.2.3. Bağlantı Durum Veritabanı

Bağlantı durum veritabanı, otonom sistem içerisindeki bağlantı durum mesajlarının değişiminden oluşur. Otonom sistem içerisindeki en kısa yollar Dijkstra Algoritması kullanılarak hesaplanıp her bir yönlendirici için SPF ağacı oluşturulur. Hedef kendi bölgesinde ise iç bölge ağacı, dış bölgede ise dış bölge ağacı oluşturulur. Ağaç şeklindeki bütün yollar OSPF yönlendirme tablosuna eklenir ve yönlendirme işlemi gerçekleştirilir. Bağlantı durum veritabanı OSPF protokolünün en önemli bileşenidir. Bağlantı durum veritabanının bileşenleri Şekil 4.15.'de gösterilmektedir [82].



Şekil 4.15. LSDB bileşenleri.

Bağlantı durum mesajları, bağlantı durum veritabanı öğesidir. LSA başlığı ve LSA gövdesinden oluşur. LSA başlığı, her bağlantı durum mesajı için eşsiz olan 20 bayt uzunluğundaki kısımdır [82].

4.4.3. IS-ISv6

Birleştirilmiş IS-IS, bağlantı durum yönlendirme algoritmasını kullanan, ISO 10589 dokümanında tanımlanmış ve OSPF protokolüne benzeyen bir yönlendirme protokolüdür. IS-IS hem IPv4 hem de OSI referans modeli network katmanı olan CLNP (Connectionless Network Protocol - Bağlantısız Network Protokolü)'yi desteklemektedir. IPv6 için birleştirilmiş IS-IS, İnternet Taslak dokümanında tanımlanmıştır [74]. Ayrıca IS-IS protokolünün nasıl kullanılabileceği ve protokol mimarisi RFC 1195'te tanımlanmıştır [19]. Yönlendirmedeki her bir yönlendirici, yönlendirici ile ilgili bilgileri içeren LSP'leri yayımlar. LSP, TLVs (type-length-values - tip-uzunluk-değerler) olarak gösterilen bilgilerini içerir [78].

OSPF ve IS-IS protokollerinin birçok yönden benzerlikleri vardır. OSPF otonom sistem içerisinde çalışırken, IS-IS ise yönlendirme alanı içerisinde çalışır. IS-IS yönlendirme alanı, merkez bölgeyle birlikte çoklu bölgelere ayrılabilir. Merkez bölge içerisindeki yönlendiriciler L2 (Level 2 - Seviye 2) yönlendiricileri olarak adlandırılmaktadır. Diğer bütün bölgelerdeki yönlendiriciler, L1 (Level 1 - Seviye 1) yönlendiricileri olarak adlandırılır. Çoğunlukla L2 yönlendirici, OSPF protokolündeki ABR olarak da düşünülebilir. Her bölge, yönlendiriciye atanan adresin ilk 13 baytı ile tanımlanır. Yönlendiriciler, IS-IS Merhaba paketleriyle birbirleriyle olan komşuluk ilişkilerini başlatır ve sürdürürler. Yönlendiriciler ancak aynı seviyedeyken komşu olabilirler ve bunu L1-LSP veya L2-LSP şeklinde bildirirler.

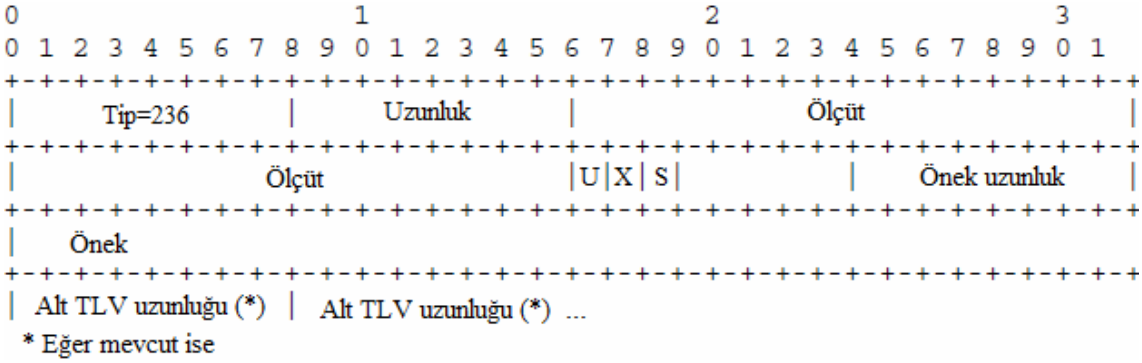
L1 yönlendiricileri yerel adreslerinin L1-LSP bildirilerinden oluşturulurken, L2 yönlendiricileri yerel adreslerinin L2-LSP bildirilerinden oluşturulmaktadır. Güzergâhlar direk olarak bağlı bölgelerden öğrenilir. Sadece L2 yönlendiricileri yönlendirme alanından dış güzergâhlarını bildirebilir ve bunlar OSPF protokolünde ASBR olarak adlandırılmaktadır. L1 yönlendirici, bölgesindeki L1 güzergâhlarını SPF ağacını oluşturarak bütün hedefleri bilir. L1 yönlendiricilerinin kendi bölgeleri dışındaki güzergâhlardan herhangi bir bilgisi yoktur. Dış bölgelere, en yakın L2 yönlendirici

vasıtasıyla ulaşılır. L2 yönlendirici, yönlendirme alanındaki bütün iç ve dış güzergâhları bilmektedir [82].

Birleştirilmiş IS-IS üzerindeki küçük değişikliklerle IPv6 yönlendirme gerçekleştirilebilir. IPv6 yönlendirmede bilgileri taşıyabilmek için "IPv6 erişilebilirliği" ve "IPv6 arayüz adresi" alanları şeklinde iki yeni TLV tanımlanmıştır [78].

4.4.3.1. IPv6 Erişilebilirliği TLV

IPv6 erişilebilirlik TLV alanının tipi 236 değeriyle belirtilmektedir. RFC 1195'te tanımlanmış "IP dâhili erişilebilirlik bilgisi" ve "IP harici erişilebilirlik bilgisi" alanları yerine "IPv6 erişilebilirliği" alanı oluşturulmuştur. "IPv6 erişilebilirliği" TLV'nin yapısı Şekil 4.16.'da gösterilmektedir [78].



Şekil 4.16. IPv6 erişilebilirlik TLV.

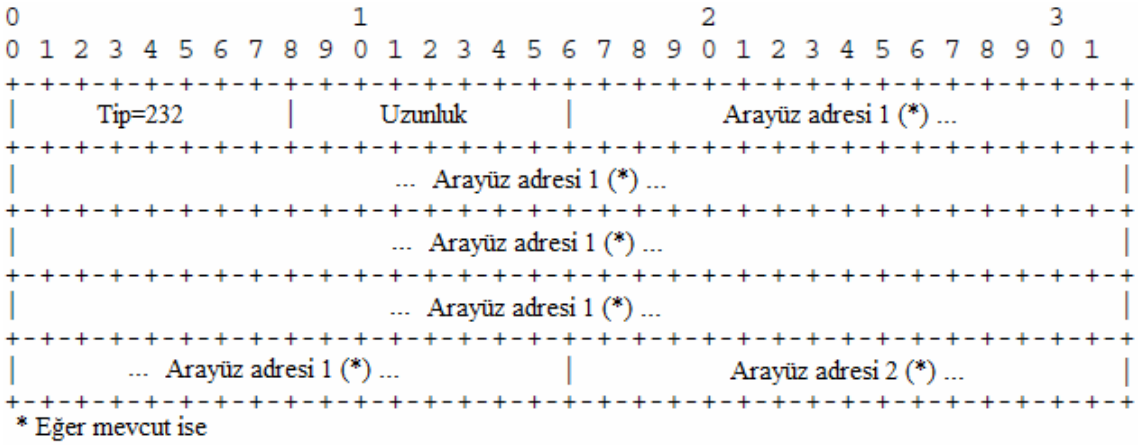
L1-LSP ve L2-LSP içerisinde IPv6 önek (prefix) tanımlanır. L2-LSP, yönlendirme alanının dışındaki IPv6 önekin bildirilmesi sonucu kontrol alanındaki X harici bit alanının ayarlanmasıyla kullanılabilir. IPv6 erişilebilirlik TLV'si; önek uzunluğu, IPv6 önek (IPv6 prefix), metrik (metric) ve kontrol (U,X,S) alanlarından oluşur [82].

32 bit uzunluğunda varsayılan metrik alanı mevcuttur. Önek uzunluk alanı, IPv6 adres önekinin uzunluğunu belirtir. S alanı eğer bir atanmış ise alt TLV'nin mevcut olduğunu belirtir [19]. U alanı, önek IS-IS protokolüne ilk enjekte edildiğinde sıfır değeri atanır. Eğer önek aynı seviyede bir bölgeden diğer bölgeye yeniden dağıtılırsa U alanı bir olarak atanır [78].

4.4.3.2. IPv6 Arayüz Adresi TLV

IPv6 arayüz adresi (IPv6 Interface Address) TLV, IP arayüz TLV ile doğrudan bağlantılıdır ve 128 bit IPv6 adresinden oluşmaktadır [19]. IPv6 arayüz adresi TLV alanının tipi 232 değeriyle belirtilmektedir [78].

Yönlendiriciler mesajlarını Merhaba paketleri içinde L1-LSP ve L2-LSP şeklinde bildirir. Merhaba paketleri, arayüze atanmış yerel IPv6 adresini içermek zorundadır. LSP içerisinde, yönlendiriciye atanmış küresel ve tekil yerel adresleri bulunur [82]. "IPv6 Arayüz Adresi" TLV'nin yapısı Şekil 4.17.'de gösterilmektedir.



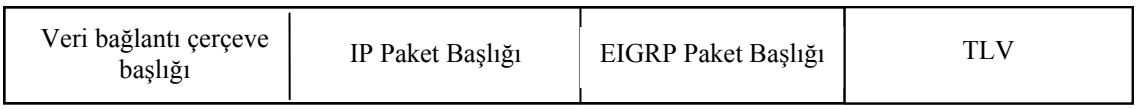
Şekil 4.17. IPv6 arayüz adresi TLV [78].

4.4.4. EIGRPv6

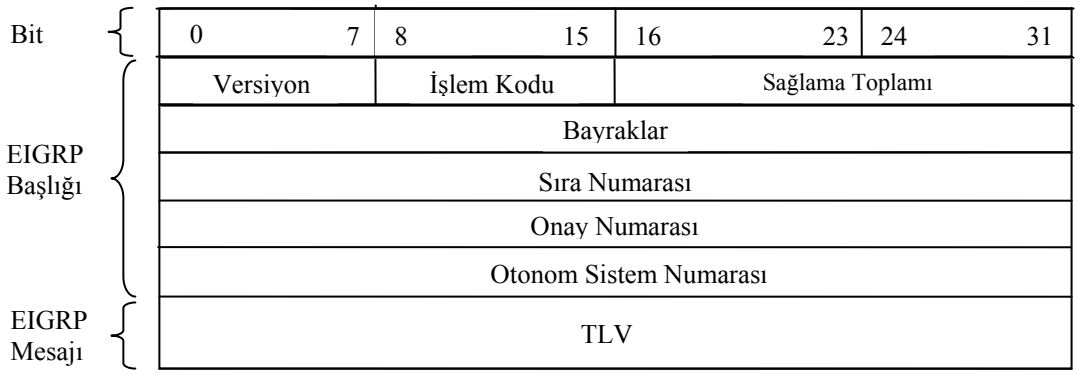
EIGRPv6, Cisco tarafından geliştirilmiş otonom sistem içerisinde çalışabilen iç yönlendirme protokollerindendir. Bu protokol, DUAL (Diffuse Update Algorithm – Yaygın Güncelleme Algoritması) kullanır. Bu protokolün temel amacı uzaklık vektör yönlendirmesinin sınırlamalarını ortadan kaldırmak ve bağlantı durum yönlendirmesinin yüksek işlemci ve performans hallerine çözüm olmak için geliştirilmiştir. Cisco, bu iki protokolün birleşimi olarak hibrit protokolünü geliştirmiştir [82]. Fakat temelde bu protokol, uzaklık vektör yönlendirme protokollerindendir. Metrik ölçüt olarak bant genişliği, gecikme, güvenilirlik ve yük değerleri kullanılmaktadır [83].

4.4.4.1. Mesaj Formatı

EIGRP mesajı dört alandan oluşur. Veri bağlantı çerçeve başlık (Data link frame header) alanı, kaynak ve hedef MAC adresini içerir. IP paket başlık (IP packet header) alanı, hedef ve kaynak IP adresini içerir. EIGRP paket başlık alanı, otonom sistem numarasını içerir. TLV alanı ise EIGRP mesaj veri kısmını gösterir. EIGRP mesajı Şekil 4.18.'de, EIGRP paket başlık alanları ise Şekil 4.19.'da gösterilmektedir [83].



Şekil 4.18. EIGRP mesajı.



Şekil 4.19. EIGRP paket başlığı.

Şekil 4.19.'da gösterilen EIGRP paket başlığı toplam 20 bayt uzunluğunda, 1 bayt versiyon alanı versiyon numarasını, 1 bayt uzunluğundaki işlem kodu alanı paket çeşitlerini tanımlamasını, 2 bayt uzunluğundaki sağlama toplamı alanı standart IP hesaplamasını, 4 bayt uzunluğundaki bayraklar alanı paketin ilave fonksiyonlarını, 4 bayt uzunluğundaki sıra numarası alanı paketin güncel sıra numarasını, 4 bayt uzunluğundaki onay numarası alanı alınan paketin sıra numarasını ve 4 bayt uzunluğundaki otonom sistem numarası ise EIGRP yönlendirme işlemi için kimlik numarası bilgisini içermektedir.

EIGRP başlığı aynı zamanda bir veya daha fazla TLV alanı içermektedir. Bunlar iki kategoride incelenebilir. İlk kategoride, güvenilir taşıma mekanizması için kullanılan genel EIGRP TLV alanı vardır. Diğer kategoride ise ağ katmanına özgü TLV alanı

vardır. IP, IPX, Appletalk ve IPv6 için TLV'ler mevcuttur. Bütün network katmanında en az iki tane TLV vardır. Biri iç EIGRP güzergâhlarını içerirken, diğeri dış güzergâhları içerir [82].

4.4.4.2. Güvenilir Taşıma Protokolü (Reliable Transport Protocol)

RTP (Reliable Transport Protocol - Güvenilir Taşıma Protokolü), EIGRP paketlerini göndermek ve almak için EIGRP tarafından kullanılır. Bu protokol EIGRP paketlerinin güvenilir ve güvenilmez teslimatlarını içerir. Güvenilir teslimat hedef tarafından onay gerektirir. Güvenilmez teslimat hedef tarafından onay gerektirmez. Paketler tekli veya çoklu olarak gönderilir.

PDM (Protocol Dependent Modules – Protokolden Bağımsız Modüller) EIGRP tarafından IP, IPX, AppleTalk ve IPv6 protokollerinin güzergâhları için kullanılır. PDM, her bir network katman protokolü için yönlendirme görevlerinden sorumludur [83].

4.4.4.3. Paket Çeşitleri

EIGRP, güvenilir paket iletimini sağlamak için uygun sırada EIGRP paketlerinin ulaşımını gerçekleştirir. EIGRP paket başlığı, güvenilir ulaşım mekanizmasını oluşturabilmek için sıra ve onay alanlarını içerir [82,83].

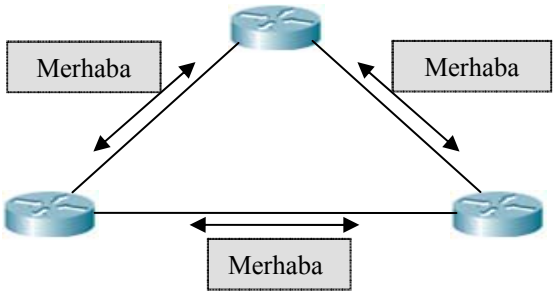
Şekil 4.20.'deki yönlendiriciler arası ilişkisi gösterilen EIGRP'deki beş farklı paket tipi aşağıdaki gibi açıklanabilir.

Merhaba paketleri: İki cihaz arası komşuluk kurulması ve keşfi için kullanılır. Güvenilir ulaşım için pek kullanılmamaktadır.

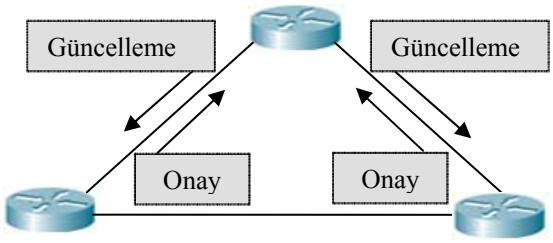
Onay paketleri: Bir paketin doğru olarak gönderildiğini onaylamak için kullanılır. Güvenilir ulaşım mekanizması için kullanılır.

Güncelleme (Update) paketleri: Rotaları tanıtmak için kullanılır. Güncelleme paketleri, yalnızca topolojilerde değişiklik olduğunda gönderilir. Genellikle güvenilir ulaşım mekanizması için kullanılır.

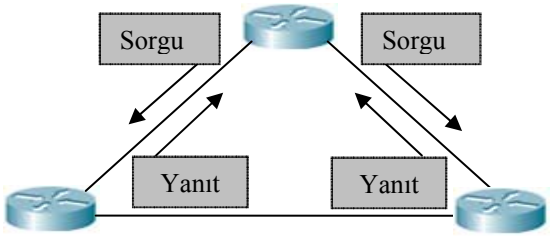
Sorgu (Query) ve yanıt (Reply) paketleri: Sorgu paketleri DUAL tarafından kullanılan ve ağa ulaşmak için gönderilen paketlerdir. Yanıt paketleri ise sorgu paketlerine cevap olarak gönderilen paketlerdir. Genellikle güvenilir ulaşım oluşturmada kullanılır.



(a) Merhaba paketleri.



(b) Onay ve güncelleme paketleri.



(c) Sorgu ve yanıt paketleri.

Şekil 4.20. EIGRP paket tipleri [83].

4.4.4.4. Yaygın Güncelleme Algoritması

DUAL, EIGRP içerisindeki bütün rotaların hesaplama işlemini yönetir. Temel amaç her bir rota için döngüye özgü yolların tablosunu oluşturmaktır. EIGRP'nin güvenilir taşıma mekanizması aşağıdaki prensipleri yerine getirmektedir [83].

- Yönlendirici, belirli zaman içerisinde kaybolan komşularını tespit etmelidir.
- Bütün mesajlar doğru ve düzgün sıra içinde teslim edilir.

- Bütün mesajlar belirli zaman içerisinde oluş sırasına göre işleme tabi tutulur.

DUAL, topoloji tablosu bulundurur. Topoloji tablosu, bir yönlendiriciden diğer bir yönlendiriciye olan bütün yolları gösteren bir haritayı tutan tablodur. En uygun maliyetli yol, yönlendirme işleminde kullanılmak için yönlendirme tablosuna kopyalanır [82]. Yönlendiriciye doğrudan bağlı olan yönlendirici listesi ise komşuluk tablosunda tutulmaktadır [83].

Bu algoritmanın düzgün bir şekilde çalışabilmesi için komşuluk bağlantılarının kurulması gerekir. Bu bağlantılar yönlendirme bilgilerinin karşılıklı değişimi için kullanılır. İlk komşuluk bağlantıları kurulduğunda, güncelleme paketleriyle bilinen tüm EIGRP güzergâhları birbirlerine geçer. Komşu yönlendiriciler tarafından yönlendirme bilgileri alındığında, her bir güzergâh için uzaklık ölçütü bildirilir. Bu ölçüt, komşu yönlendiriciden hedefe yol maliyetini göstermektedir. Yönlendirici her bir rota için bildirilen uzaklık ölçütünü de ekleyerek toplam mesafeyi hesaplar. Her bir rota için en uygun mesafe EIGRP topoloji tablosuna eklenir. En uygun rota birden fazla komşu yönlendiriciden alınmış ise, uygun mesafeden daha kısa olarak bildirilen uzaklık da topoloji tablosuna eklenir. Uygun şartlar döngüye özgü rota için test edilir. Eğer daha uygun şart ile karşılaşılırsa, komşu yönlendirici bu yönlendirici vasıtasıyla bildirilen uzaklığın hedef yola gidileceğini bildirir.

Topoloji tablosundaki her bir güzergâh; IPv6 önek ve önek uzunluğu, uygun mesafe, en uygun mesafe için komşu yönlendirici IPv6 adresi, en uygun mesafe listesi ve en uygun mesafe sayılarını içerir. Yönlendirici, herhangi bir değişiklik olması durumunda topoloji tablosunu yeniden hesaplar. DUAL en uygun mesafeyi bulur. En uygun mesafe var olan ile değiştirilerek bütün komşulara bu bilgi gönderilir [82]. Bu algoritma döngüye özgü yedek rota listesini tuttuğu için hızlı yakınsama zamanı sağlamaktadır [83].

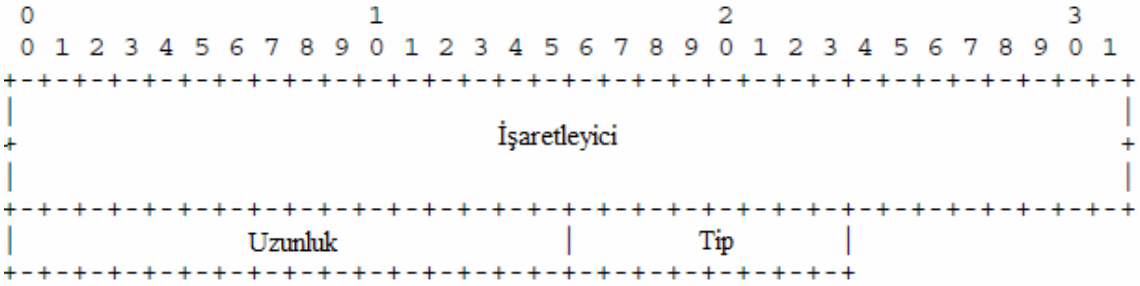
4.4.5. BGPv6

BGP RFC 4271 belgesinde tanımlanmış yol vektör yönlendirme protokolüdür. Otonom sistemler içerisinde kullanılan RIPng ve OSPFv3 protokollerinden farklı olarak BGP–4, otonom sistemler arasındaki bilgi iletimi için tasarlanmıştır. BGP–4 yönlendirme bilgisi, otonom sistemler arasındaki bütün bağlantıları tanımlayan mantıksal yol ağacıyla

oluşturulur. BGP-4 yönlendiricilerinin sanal rotaları belirlenip bu yollara göre yönlendirme tablolarının içerisinde yol ağacı bilgisi oluşturulur. BGP-4 mesajları TCP 179 numaralı port kullanılarak gönderilir. BGP-4 IPv4 için kullanılan yönlendirme protokolüdür. IPv6 için BGP-4 genişletilerek IPv6 adres önekini desteklemesi sağlanmış ve BGPv6 adını alarak RFC 2545 belgesinde tanımlanmıştır [74].

4.4.5.1. Mesaj Başlığı

BGP mesaj başlığı toplam 19 bayt uzunluğunda üç farklı alandan oluşur. 16 bayt uzunluğundaki işaretleyici (marker) alanı, iki otonom sistem çifti arasında doğrulama verisini içerir. 2 bayt uzunluğundaki uzunluk alanı, BGP mesajının toplam boyutunu gösterir. Uzunluk alanı 19 ile 4096 bayt arasında olabilir. 1 baytlık tip alanı ise mesajın tipini göstermektedir [82]. BGP mesaj başlık formatı Şekil 4.21.'de, BGP mesaj tipleri ise Tablo 4.9.'da gösterilmektedir.



Şekil 4.21. BGP mesaj başlık formatı [80].

Tablo 4.9. BGP mesaj tipleri [82].

Tipi	**İsmi**	**Açıklaması**
1	(Açık) Open	İki otonom sistem arasında BGP komşuluğunu başlatmak için yönlendirici tarafından gönderilen mesajdır.
2	Güncelleme	BGP güzergâhlarının durum bilgisini ve yönlendirme bilgisini içerir.
3	Tebliğ (Notification)	Hata veya sona eren BGP bağlantılarını rapor etmek için gönderilir.
4	Canlı tutma (Keepalive)	Zaman aşımına uğramış BGP bağlantılarını engellemede kullanılır.

4.4.5.2. BGP Yol Özellikleri

Yol özellikleri, NLRI (Network Layer Reachability Information - Network Katman Ulaşılabilirlik Bilgisi) mesajları hakkında ek bilgi sağlar. Yol özelliğinde tip, uzunluk ve değer alanları vardır. Yol bilgisinin tip alanının ismine göre fonksiyonu vardır. Tip alanı çeşitleri Tablo 4.10.'da gösterilmektedir [82].

Tablo 4.10. BGP tip alanları.

Tipi	**İsmi**	**Açıklaması**
1	Orijin (Origin)	Yol bilgisiyle bütün yolların kaynakları tanımlanabilir.
2	Otonom sistem yol (As_Path)	En az atlanacak otonom sistem sayısını belirtir.
3	Sonraki düğüm (Next_Hop)	Sonraki yönlendirici adresini gösterir. IPv6 için kullanılamaz.
4	Med	İki otonom sistem arasındaki tercih edilen en iyi yol bilgisidir.
5	Yerel_Öncelik (Local_Pref)	Rotanın yerel öncelik sırasını belirtir.
6	Atomik_Toplam (Atomic_Aggregate)	Daha karmaşık yoldan daha basit yol seçimini bildirir.
7	Toplayıcı (Aggregator)	Güzergâh bilgisinin yönlendirici tarafından toplanmasıdır.
8	Topluluk (Community)	Güzergâh seçimi için kullanılır.
14	Erişilebilen NLRI (Mp_Reach_NLRI)	Çoklu protokol NLRI'yı bildirir. IPv6 öneki için kullanılır.
15	Erişilemeyen NLRI Mp_Unreach_NLRI	Geçerli olmayan çoklu protokol NLRI'yı bildirir. IPv6 öneki için kullanılır.

4.4.5.3. IPv6 İçin Çoklu BGP Protokolü

BGP-4 tamamen IPv4'e özgü üç bilgi taşımaktadır. Bunlar aşağıda sıralanmıştır.

- Güncelleme mesajı içerisindeki uygun ve geçerli olmayan NLRI IPv4 öneki içerir.
- Güncelleme mesajı içerisindeki Sonraki düğüm yol özelliği IPv4 adresini içerir.
- Açık mesajı ve Toplayıcı yol bilgisinin içerisindeki BGP belirteci olarak bilinir.

BGP-4 protokolünün IPv6 desteğini sağlayabilmesi için çoklu protokol NLRI ve sonraki adres bilgileri eklenmelidir. BGP-4'e iki yeni özellik Erişilebilen NLRI ve Erişilemeyen NLRI eklenir. BGP-4 yönlendiricileri, IPv6 ilavesi olsa bile yerel IPv4 adresine gereksinim duymaktadır. Komşu otonom sistem yönlendiricileri, IPv6 desteğini gösterebilmesi için isteğe bağlı BGP parametrelerini bildirmesi gerekir. BGP bağlantısı ve rota seçimi değişmeden kalmaktadır. Rota seçiminde sonraki yönlendirici bilgisi ve IPv6 NLRI dikkate alınması gerekmektedir. Güncelleme mesajları sadece IPv6 NLRI mesajlarını bildirir. Bütün bildirilmiş veya geçerli olmayan IPv6 rotaları Erişilebilen NLRI ve Erişilemeyen NLRI içerisinde taşınır. Güncelleme mesajı, aynı yol özelliğinde hem IPv6 NLRI hem de IPv4 NLRI bildirebilmektedir. Bu durumda bütün alanlar kullanılabilir. IPv4 ve IPv6 NLRI ilgili yönlendirme bilgisine bağlı olarak ayırt edilebilir.

Erişilebilen NLRI yol özelliği, iki komşu otonom sistem arasında sonraki yönlendirici IPv6 adresiyle birlikte uygun IPv6 NLRI'ların değişimini sağlamaktadır. Erişilemeyen NLRI yol özelliği ise iki komşu otonom sistem arasında artık geçerli olmayan çoklu IPv6 güzergâhlarını gönderir [82].

5. BÖLÜM

IPv6'YA ENTEGRASYON ve IPv6'DA FARKLI YÖNLENDİRME PROTOKOLLERİNİN BAŞARIMI

5.1. Benzetim Ortamı

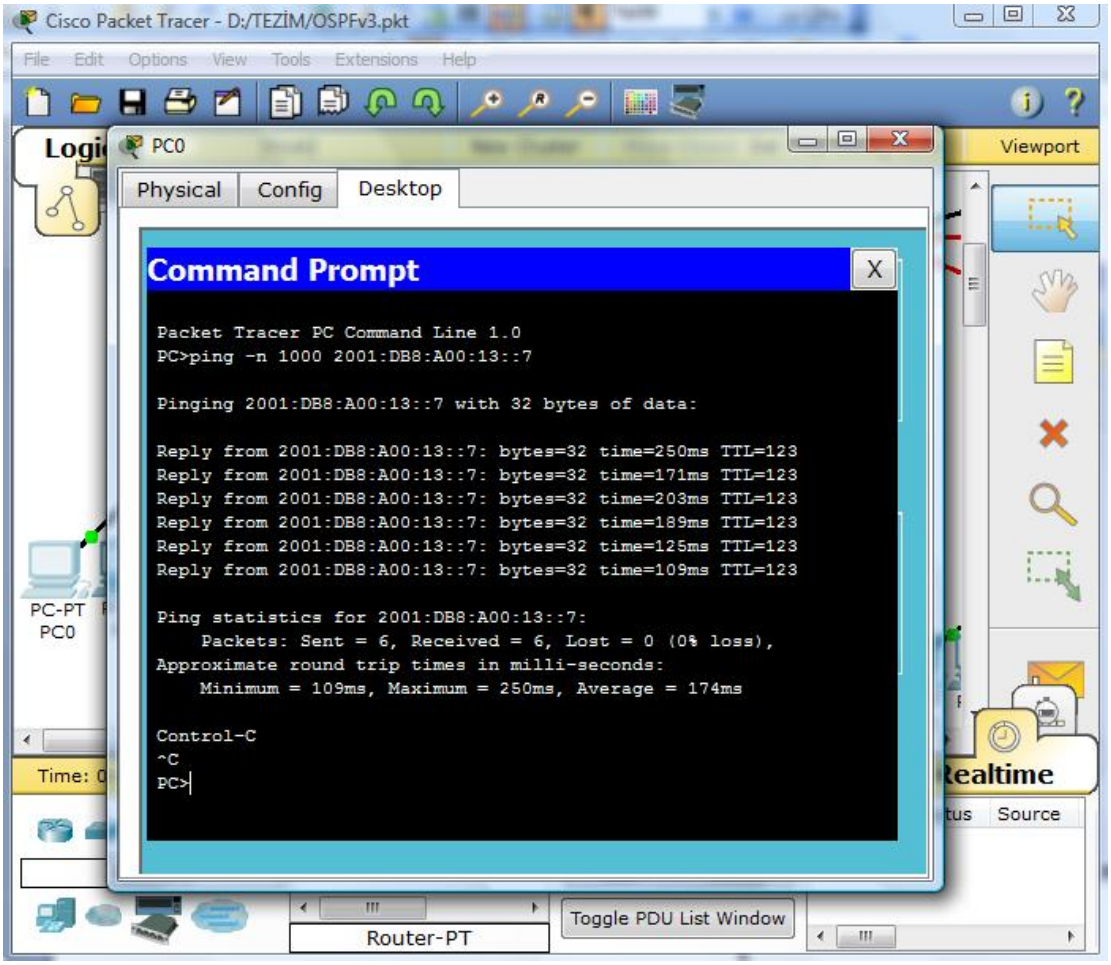
IPv4'ten IPv6'ya geçiş yöntemlerinden olan çift yığın tekniği ve IPv6'daki farklı yönlendirme protokollerinin benzetimi, CPT 5.2 benzetim programı aracılığıyla gerçekleştirilmiştir. IPv6 paketlerinin IPv6 yönlendirme protokolleri kullanarak farklı ağ yapıları üzerindeki akışının benzetimi gerçekleştirilerek bu protokoller üzerine bazı testler yapılmıştır. CPT, IPv6 yönlendirme protokollerinden bazılarını desteklemektedir [84,85]. Desteklenen protokoller kullanılarak benzetim çalışmaları yapılmıştır. Bu protokoller aşağıda listelenmiştir.

- RIPng
- OSPF
- EIGRP
- Statik yönlendirme

Benzetim ortamının örnek bir ekran görüntüsü verilen Şekil 5.1., benzetim işleminin gerçekleştirildiği CPT programının ve modellenen ağdaki bir bilgisayar ile diğer bir bilgisayarın haberleşmesi için yapılan işlemi belirten süreci göstermektedir. Bu çalışma için Intel Core 2 Duo 2.1 GHz işlemci, 4 GB Ram ve 160 GB hard disk özelliklerine sahip Acer TravelMate6593 dizüstü bilgisayar kullanılmıştır.

Yayın (broadcast) adresi üzerinden tüm ağın adresi gönderildiği için ağ üzerindeki cihaz sayısının fazla olması, yayın trafiğini artırmakta [86] ve benzetim ortamının performans analizinde gereksiz yoğunluğa neden olabilmektedir. Ayrıca, yayın adresi üzerinden yapılan güvenlik saldırısının azaltılması için yayın adres sınırlamasının yapılması

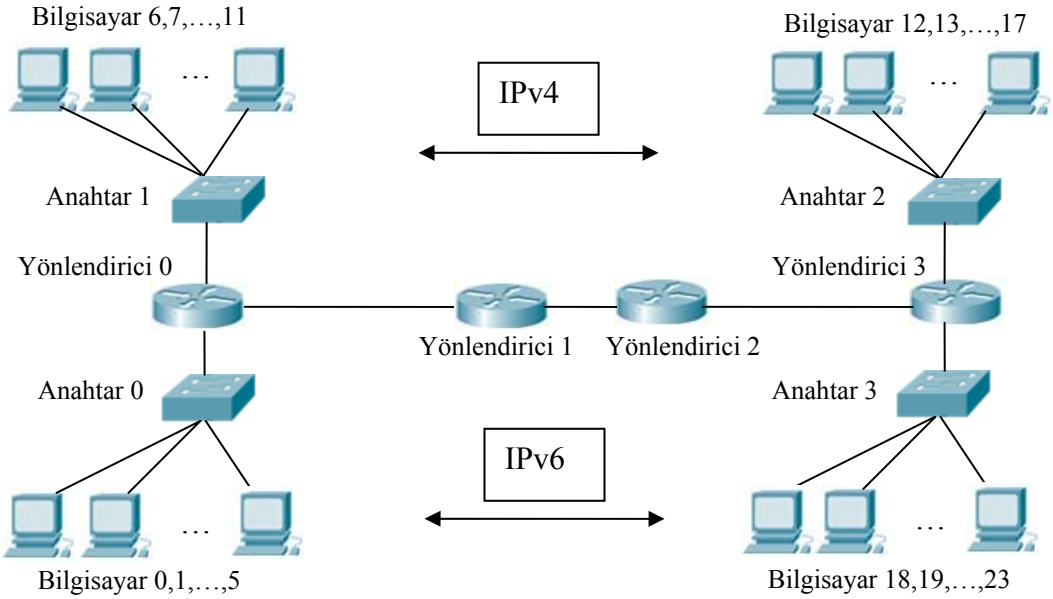
gerekmektedir [87]. Bu yüzden benzetim modellerinde kullanılan bilgisayar, anahtar (switch) ve yönlendirici cihazları belirli sayıyı aşmamıştır.



Şekil 5.1. Benzetim ortamı.

5.2. IPv4'ten IPv6'ya Entegrasyonda Çift Yığın Yönteminin Benzetimi

Çift yığın yönteminin benzetimi, Şekil 5.2.'de gösterilen modele göre gerçekleştirilmiştir. Bu modelde, bilgisayarlar sırasıyla numaralandırılıp bilgisayar 0-23 şeklinde adlandırılmış, anahtarlar sırasıyla numaralandırılıp anahtar 0-3 şeklinde adlandırılmış ve yönlendiriciler de sırasıyla numaralandırılıp yönlendirici 0-3 şeklinde adlandırılmıştır. Toplamda 24 bilgisayar, 4 anahtar ve 4 yönlendirici kullanılarak oluşturulmuş bir ağ modeli için benzetim gerçekleştirilmiştir.



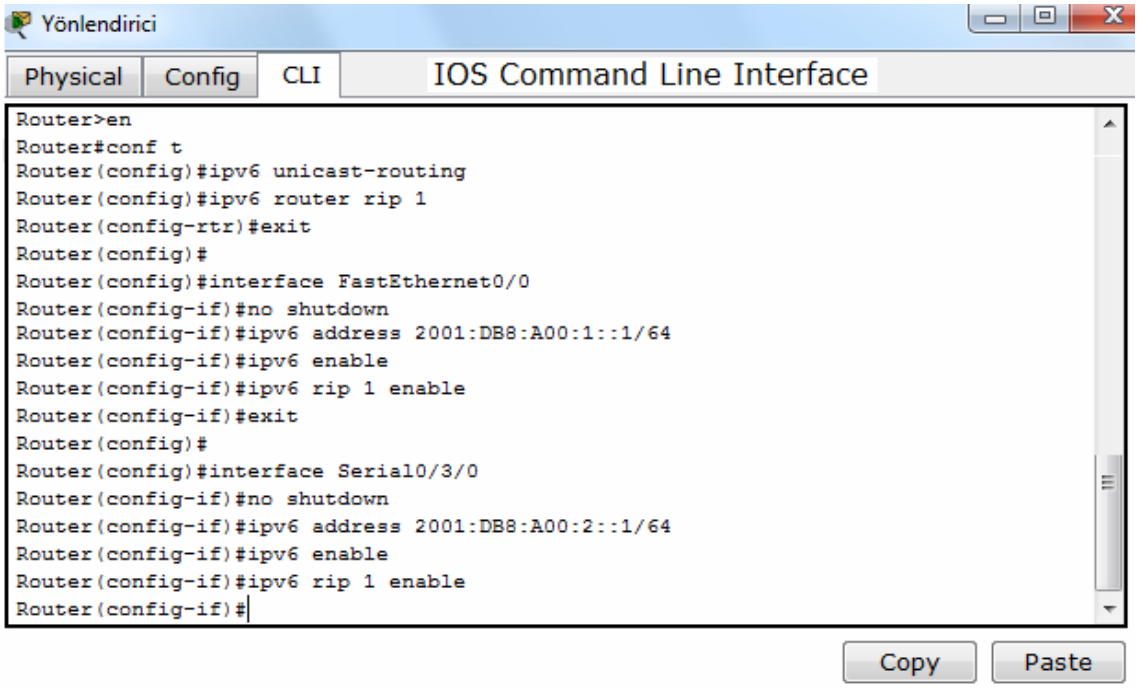
Şekil 5.2. Çift yığın yöntemi için modellenen benzetim ağ modeli.

Şekil 5.2.'de; anahtar 0 ve anahtar 3'e bağlı bilgisayarlar IPv6, anahtar 1 ve anahtar 2'ye bağlı bilgisayarlar da IPv4 olarak yapılandırılmıştır. Yönlendiricilerde ise hem IPv4 hem de IPv6 yapılandırmaları uygulanmıştır. Böylece yönlendirici 1 ve yönlendirici 2 üzerinden IPv4 olarak yapılandırılan bilgisayar 6-11 ile bilgisayar 12-17, IPv6 olarak yapılandırılan bilgisayar 0-5 ile bilgisayar 18-23 arasında çift yığın yöntemi ile bağlantı kurulması sağlanmıştır.

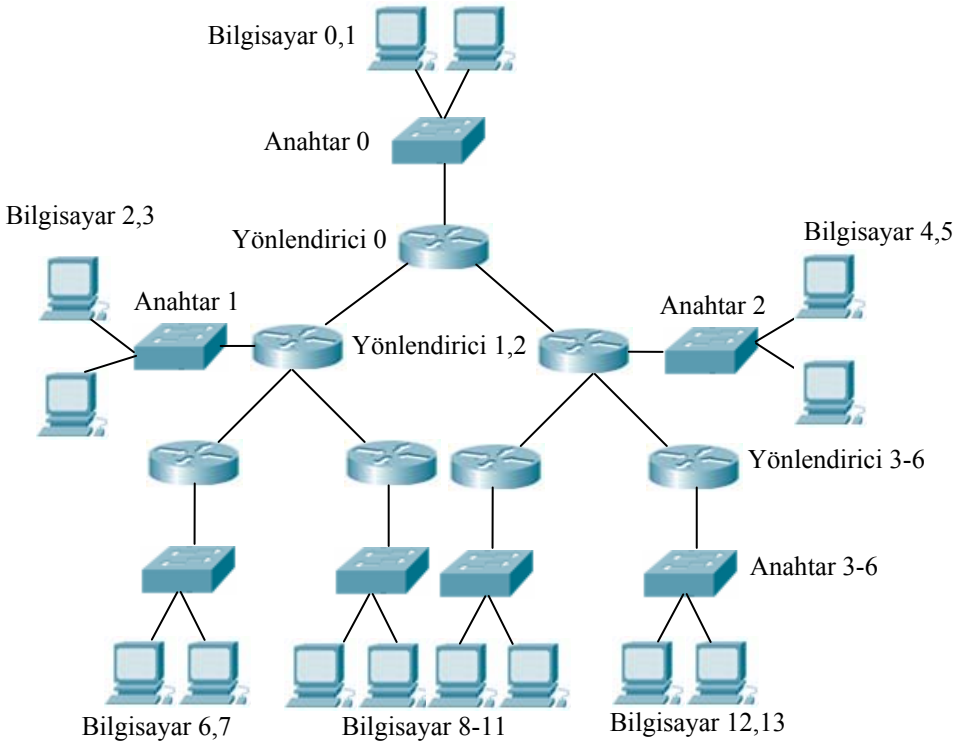
5.3. IPv6'daki Farklı Yönlendirme Protokollerinin Benzetimi

Bu çalışmada, IPv6 statik yönlendirme ve dinamik yönlendirme protokolleri kullanılmıştır. Statik yönlendirmeye ilaveten dinamik yönlendirme protokollerinden olan RIPng, OSPFv3, EIGRPv6 protokolleri, ağdaki paket gecikmeleri ve veri transfer hızları açısından karşılaştırılmıştır. CPT programı ile benzetim ağ modellerinde gerçekleştirilen yönlendirme protokollerinden RIPng örnek yapılandırma ayarları Şekil 5.3.'de gösterilmektedir.

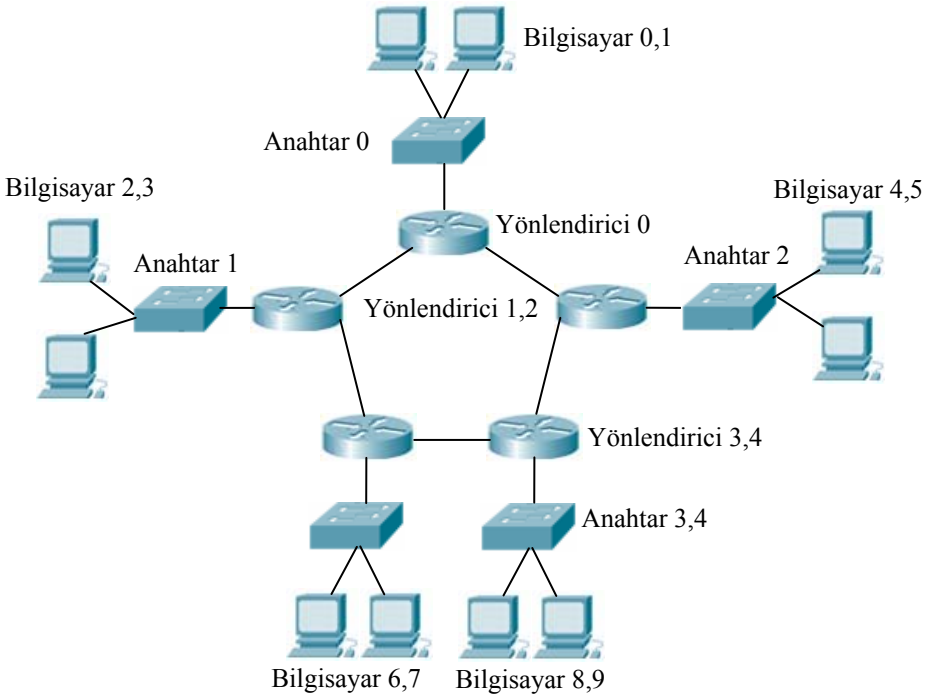
Benzetim için dört farklı ağ modellenmiştir. Şekil 5.4. ağaç topolojisi modelini, Şekil 5.5. halka topolojisini, Şekil 5.6. yıldız topolojisini ve Şekil 5.7. veri yolu (bus) ağ topolojisine benzer şekilde 48 bilgisayar (PC), 8 anahtar (switch), 6 yönlendirici (router) kullanılarak oluşturulmuş modellenen karmaşık bir ağ modelini göstermektedir.



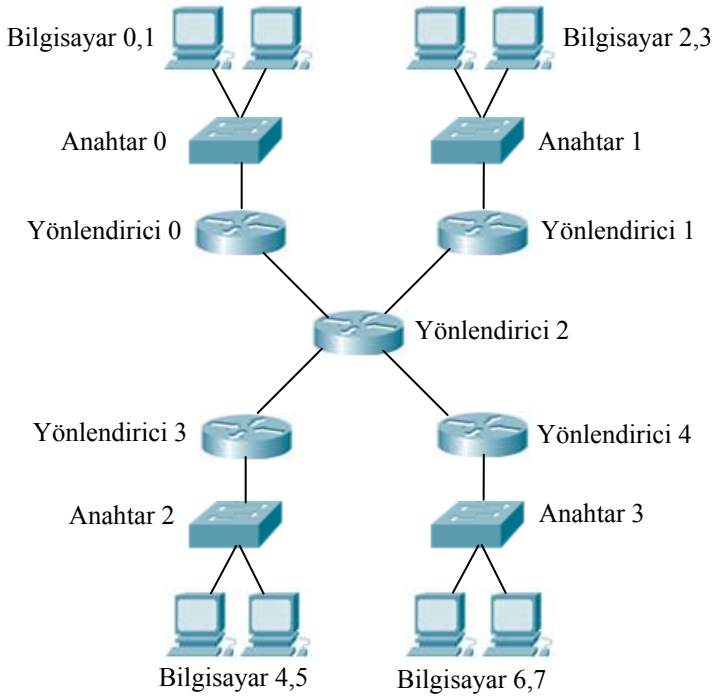
Şekil 5.3. RIPng örnek yönlendirici yapılandırması.



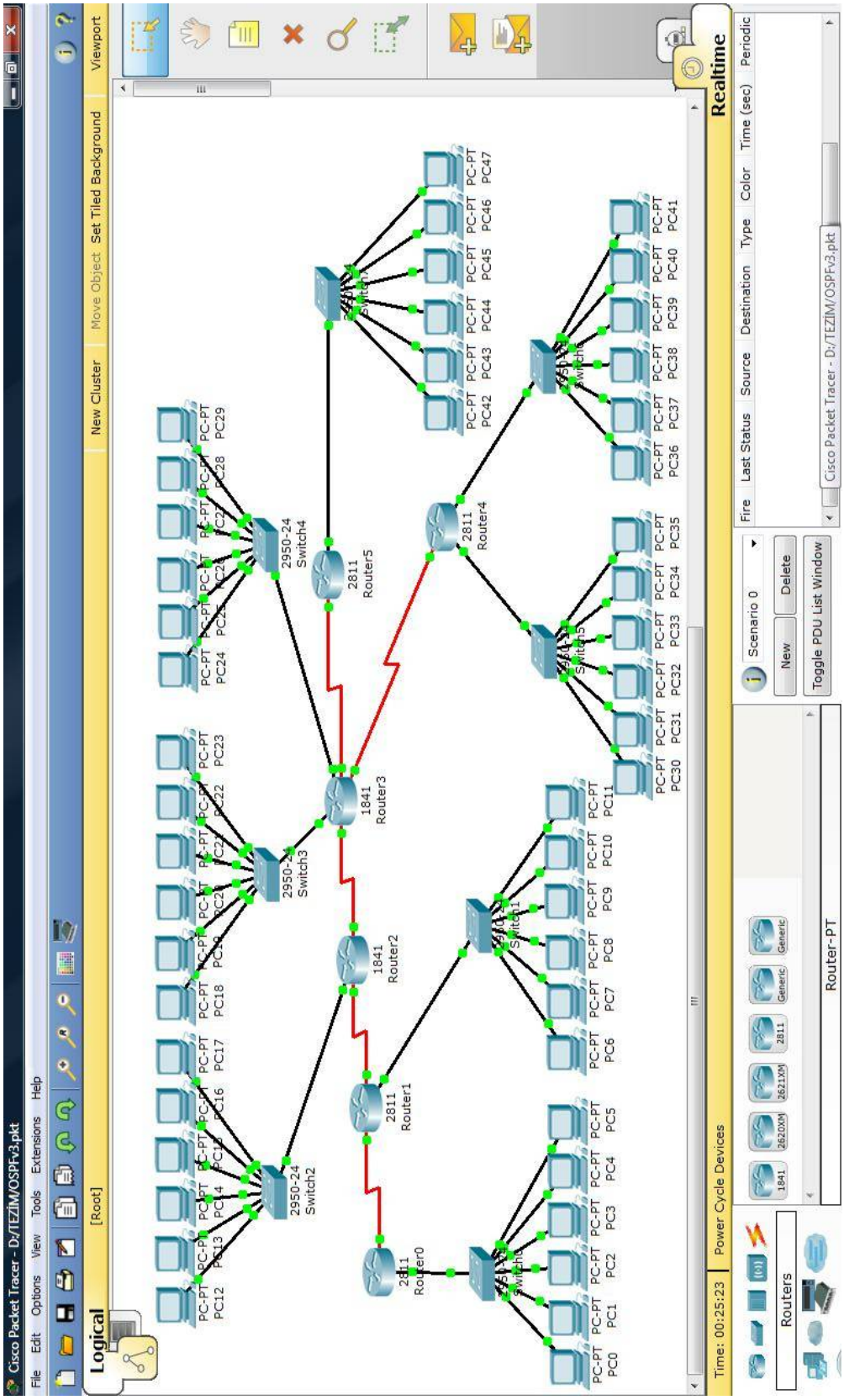
Şekil 5.4. Ağaç topolojisine göre oluşturulan ağ modeli.



Şekil 5.5. Halka topolojisine göre oluşturulan ağ modeli.



Şekil 5.6. Yıldız topolojisine göre oluşturulan ağ modeli.



Şekil 5.7. Karmaşık ağ modeli.

5.3.1. Paket Gecikmesi ve Veri Transfer Hızı (Throughput) Karşılaştırması

Şekil 5.4-7.'deki benzetim modelleri kullanılarak ağdaki bilgisayarlar ve yönlendiriciler arasında ping komutu gönderilmiştir. Bu komut, paketin yönlendiriciler üzerindeki iletimini ve kaynak düğüm ile hedef düğüm arasındaki bağlantı durumunu göstermektedir. Bir ağ cihazı ping komutu ile ağdaki diğer cihaza ICMP paketlerini gönderir ve ağ cihazı da ICMP paketleriyle cevap verir [88].

Veri transfer hızı ölçümü, toplam veri miktarının ortalama süreye bölünmesiyle bayt cinsinden bulunan sonuç sekiz ile çarpılarak bit cinsinden aşağıdaki gibi hesaplanmıştır.

Veri transfer hızı = {Toplam veri miktarı / Ortalama süre } * 8

Benzetim çalışmalarında, CPT 5.2 programındaki kısıtlamalardan dolayı bilgisayarlar arasında 32 bayt boyutunda, yönlendirici bilgisayar arasında ise 1472 bayta kadar paket gönderilmiştir.

5.3.1.1. Ağaç Topoloji Modeli Benzetim Sonuçları

Şekil 5.4.'de modellenen ağaç topoloji ağında, PC-PC ve yönlendirici-PC arasındaki erişim zamanları ve veri transfer hızları Tablo 5.1.'de gösterilmektedir.

Tablo 5.1. Ağaç topolojisinde 1000 defa paket gönderim sonucu erişim zamanları ve veri transfer hızları ölçümü.

Yönlendirme Protokolü	**Veri Miktarı (bayt)**	**Test Verileri**			
		Minimum Süre(ms)	**Maksimum Süre(ms)**	**Ortalama Süre(ms)**	**Throughput (kbps)**
PC 0 ile PC 13 arasındaki sonuçlar					
OSPFv3	32	63	188	148	1,73
RIPng	32	56	202	155	1,65
EIGRPv6	32	62	203	153	1,67
Statik yönlendirme	32	63	203	154	1,66
PC 0 ile PC 13 arasındaki sonuçlar					
OSPFv3	1472	62	141	110	107,05
RIPng	1472	72	141	112	105,14
EIGRPv6	1472	62	141	111	106,09
Statik yönlendirme	1472	70	141	113	104,21

OSPFv3 yönlendirme protokolünde paket gecikme süresi PC 0 – PC 13 arasında 32 bayt ICMP paketi gönderiminde 148 ms iken test edilen diğer üç yönlendirme protokolünde ortalama 154 ms, yönlendirici 0 ile PC 13 arasında 1472 bayt ICMP paketi gönderiminde ise OSPFv3'de ortalama süre 110 ms iken diğerlerinde ortalama süre 112 ms olarak ölçülmüş, OSPFv3'teki paket gecikmesinin daha kısa olduğu görülmüştür.

Diğer bir performans kriteri olarak da veri transfer hızları test edilmiştir. Veri transfer hızı OSPFv3 için PC 0 – PC 13 arasında 32 bayt ICMP paketi gönderiminde 1,73 kbps iken test edilen diğer üç yönlendirme protokolünde ortalama 1,66 kbps, yönlendirici 0 ile PC 13 arasında 1472 bayt ICMP paketi gönderiminde ise OSPFv3 için 107,05 kbps iken diğerlerinde ortalama 105,15 kbps olarak ölçülmüş, OSPFv3'teki veri transferinin daha yüksek bir verim sağladığı görülmüştür.

5.3.1.2. Halka Topoloji Modeli Benzetim Sonuçları

Şekil 5.5.'de modellenen halka topoloji ağında, PC-PC ve yönlendirici-PC arasındaki erişim zamanları ve veri transfer hızları Tablo 5.2.'de gösterilmektedir.

Tablo 5.2. Halka topolojisinde 1000 defa paket gönderim sonucu erişim zamanları ve veri transfer hızları ölçümü.

Yönlendirme Protokolü	**Veri Miktarı (bayt)**	**Test Verileri**			
		Minimum Süre(ms)	**Maksimum Süre(ms)**	**Ortalama Süre(ms)**	**Throughput (kbps)**
PC 0 ile PC 9 arasındaki sonuçlar					
OSPFv3	32	77	188	157	1,63
RIPng	32	82	203	163	1,57
EIGRPv6	32	78	188	162	1,58
Statik yönlendirme	32	80	203	175	1,46
Yönlendirici 0 ile PC 9 arasındaki sonuçlar					
OSPFv3	1472	63	141	114	103,3
RIPng	1472	62	141	115	102,4
EIGRPv6	1472	78	141	116	101,5
Statik yönlendirme	1472	78	140	115	102,4

OSPFv3 yönlendirme protokolünde paket gecikme süresi PC 0 ile PC 9 arasında 32 bayt ICMP paketi gönderiminde 157 ms iken test edilen diğer üç yönlendirme protokolünde ortalama 167 ms, yönlendirici 0 ile PC 9 arasında 1472 bayt ICMP paketi gönderiminde

ise OSPFv3'de ortalama süre 114 ms iken diğerlerinde ortalama süre 115 ms olarak ölçülmüş, OSPFv3'teki paket gecikmesinin daha kısa olduğu görülmüştür.

Diğer bir performans kriteri olarak da veri transfer hızları test edilmiştir. Veri transfer hızı OSPFv3 için PC 0 ile PC 9 arasında 32 bayt ICMP paketi gönderiminde 1,63 kbps iken test edilen diğer üç yönlendirme protokolünde ortalama 1,54 kbps, yönlendirici 0 ile PC 9 arasında 1472 bayt ICMP paketi gönderiminde ise OSPFv3 için 103,3 kbps iken diğerlerinde ortalama 102,1 kbps olarak ölçülmüş, OSPFv3'teki veri transferinin daha yüksek bir verim sağladığı görülmüştür.

5.3.1.3. Yıldız Topoloji Modeli Benzetim Sonuçları

Şekil 5.6.'da modellenen yıldız topoloji ağında, PC-PC ve yönlendirici-PC arasındaki erişim zamanları ve veri transfer hızları Tablo 5.3.'de gösterilmektedir.

Tablo 5.3. Yıldız topolojisinde 1000 defa paket gönderim sonucu erişim zamanları ve veri transfer hızları ölçümü.

Yönlendirme Protokolü	Veri Miktarı (bayt)	Test Verileri			
		Minimum Süre(ms)	Maksimum Süre(ms)	Ortalama Süre(ms)	Throughput (kbps)
PC 0 ile PC 7 arasındaki sonuçlar					
OSPFv3	32	65	203	161	1,59
RIPng	32	90	201	166	1,54
EIGRPv6	32	93	203	165	1,55
Statik yönlendirme	32	66	203	166	1,54
Yönlendirici 0 ile PC 7 arasındaki sonuçlar					
OSPFv3	1472	63	171	115	102,4
RIPng	1472	63	172	117	100,65
EIGRPv6	1472	62	171	116	101,52
Statik yönlendirme	1472	62	141	117	100,65

OSPFv3 yönlendirme protokolünde paket gecikme süresi PC 0 ile PC 7 arasında 32 bayt ICMP paketi gönderiminde 161 ms iken test edilen diğer üç yönlendirme protokolünde ortalama 166 ms, yönlendirici 0 ile PC 7 arasında 1472 bayt ICMP paketi gönderiminde ise OSPFv3'de ortalama süre 115 ms iken diğerlerinde ortalama süre 117 ms olarak ölçülmüş, OSPFv3'teki paket gecikmesinin daha kısa olduğu görülmüştür.

Diğer bir performans kriteri olarak da veri transfer hızları test edilmiştir. Veri transfer hızı OSPFv3 için PC 0 ile PC 7 arasında 32 bayt ICMP paketi gönderiminde 1,59 kbps iken test edilen diğer üç yönlendirme protokolünde ortalama 1,54 kbps, yönlendirici 0 ile PC 7 arasında 1472 bayt ICMP paketi gönderiminde ise OSPFv3 için 102,4 kbps iken diğerlerinde ortalama 100,94 kbps olarak ölçülmüş, OSPFv3'teki veri transferinin daha yüksek bir verim sağladığı görülmüştür.

5.3.1.4. Karmaşık Bir Ağ Modeli Benzetim Sonuçları

Şekil 5.7.'de modellenen karmaşık bir ağda; PC-PC arasındaki erişim zamanları ve veri transfer hızları Tablo 5.4.'de, yönlendirici-PC arasındaki 1472 bayt veri için erişim zamanları ve veri transfer hızları Tablo 5.5.'de gösterilmektedir.

Tablo 5.4. Karmaşık modelde PC 0 - PC 47 arasındaki erişim zamanları ve veri transfer hızları ölçümü.

Yönlendirme Protokolü	**Veri Miktarı (bayt)**	**Test Verileri**			
		Minimum Süre(ms)	**Maksimum Süre(ms)**	**Ortalama Süre(ms)**	**Throughput (kbps)**
1000 defa paket gönderim sonuçları					
OSPFv3	32	21	250	161	1,59
RIPng	32	59	250	169	1,51
EIGRPv6	32	38	265	166	1,54
Statik yönlendirme	32	52	250	168	1,52
5000 defa paket gönderim sonuçları					
OSPFv3	32	16	250	160	1,6
RIPng	32	24	250	169	1,51
EIGRPv6	32	50	250	166	1,54
Statik yönlendirme	32	37	250	168	1,52

OSPFv3 yönlendirme protokolünde paket gecikme süresi Tablo 5.4.'den PC 0 ile PC 47 arasında 32 bayt ICMP paketi gönderiminde 161 ms iken test edilen diğer üç yönlendirme protokolünde ortalama 168 ms, yönlendirici 0 ile PC 47 arasında veri boyutu 1472 bayt olarak test edildiğinde Tablo 5.5.'de OSPFv3'de ortalama süre gönderilen paket sayısına göre (1000, 5000) 159 ms, 160 ms iken diğerlerinde ortalama süre 161 ms olarak ölçülmüş, 1000 ve 5000 defa ICMP paketi gönderim sonuçlarında

belirgin bir değişikliğin olmadığı ve her ikisinde de OSPFv3'teki paket gecikmesinin daha kısa olduğu görülmüştür.

Tablo 5.5. Karmaşık modelde yönlendirici 0 - PC 47 arasındaki erişim zamanları ve veri transfer hızları ölçümü.

Yönlendirme Protokolü	**Veri Miktarı (bayt)**	**Test Verileri**			
		Minimum Süre(ms)	**Maksimum Süre(ms)**	**Ortalama Süre(ms)**	**Throughput (kbps)**
1000 defa paket gönderim sonuçları					
OSPFv3	1472	109	203	159	74,06
RIPng	1472	101	203	161	73,14
EIGRPv6	1472	94	203	161	73,14
Statik yönlendirme	1472	101	203	162	72,69
5000 defa paket gönderim sonuçları					
OSPFv3	1472	96	203	160	73,6
RIPng	1472	93	203	162	72,69
EIGRPv6	1472	97	212	161	73,14
Statik yönlendirme	1472	102	209	161	73,14

Diğer bir performans kriteri olarak da veri transfer hızları test edilmiştir. Veri transfer hızı OSPFv3 için Tablo 5.4.'den PC 0 ile PC 47 arasında 32 bayt ICMP paketi gönderiminde 1,59 kbps iken test edilen diğer üç yönlendirme protokolünde ortalama 1,52 kbps, yönlendirici 0 ile PC 47 arasında 1472 bayt ICMP paketi gönderiminde Tablo 5.5.'de OSPFv3 için gönderilen paket sayısına göre (1000, 5000) 74,06 kbps ve 73,6 kbps iken diğerlerinde ortalama 72,99 kbps olarak ölçülmüş, OSPFv3'teki veri transferinin daha yüksek bir verim sağladığı görülmüştür.

Tablo 5.6. Karmaşık modelde 1000 defa paket gönderim sonucu OSPFv3 yönlendirme protokolünün erişim zamanı ölçümü.

	Veri Miktarı (bayt)	**Test Verileri**		
		Minimum Süre (ms)	**Maksimum Süre (ms)**	**Ortalama Süre (ms)**
PC 0 – PC 11	32	25	156	101
PC 0 – PC 47	32	21	250	161

Tablo 5.6.'da gösterildiği gibi, Şekil 5.7.'de gösterilen karmaşık bir ağ yapısı modelinde PC 0 – PC 11 arasındaki 2 anahtar ve 2 yönlendiriciden geçen veri trafiği gecikme

süreleri ile PC 0- PC 47 arasındaki 2 anahtar ve 5 yönlendiriciden geçen veri trafiği gecikme süreleri karşılaştırıldığında; yönlendirici sayısındaki 3 adet artış, ortalama 60 ms olarak etki etmiştir. Buradan anlaşıldığı gibi yönlendirici sayısındaki artış paket gecikme sürelerini doğrudan etkilemektedir.

5.3.1.5. Genel Değerlendirme

Tablo 5.1-5.'deki sonuçlar değerlendirildiğinde, uçtan uca iki bilgisayar arasında modellenen bir ağda OSPFv3 yönlendirme protokolü veri transfer hızının RIPng, EIGRPv6 ve statik yönlendirmeye göre daha hızlı olduğu, ortalama paket gecikmesinin de daha kısa olduğu görülmüştür. Buna göre OSPFv3 yönlendirme protokolünün diğer üç yönlendirme protokolünden daha yüksek bir verim sağladığı anlaşılmaktadır. Fakat diğer yönlendirme protokolleri ile arasında çok az farklılıkların olduğu tespit edilmiştir.

6. BÖLÜM

SONUÇLAR

Bu tez çalışmasında, IPv6'nın genel özellikleri, IPv4'ten IPv6'ya entegrasyon için geçiş yöntemleri ve IPv6 ağlarda haberleşmede kullanılan yönlendirme protokolleri incelenerek, bilgisayar ortamında modellenen bazı ağ yapıları üzerinde farklı IPv6 yönlendirme protokollerinin performans analizleri yapılması amaçlanmıştır. Yakın gelecekte kullanılması zorunluluk haline gelecek olan IPv6'nın geçiş sürecinde, IPv4 ve IPv6 altyapısı belirli bir süre birlikte kullanılacağından, IPv4'ten IPv6'ya geçiş entegrasyonu için kullanılabilecek yöntemler olan çift yığın, tünelleme vb. hakkında bilgiler verilerek, çift yığın tekniğinin CPT 5.2 programında modellenen örnek bir ağ üzerinde benzetimi gerçekleştirilmiştir. Türkiye'de ULAKBİM tarafından yürütülmekte olan IPv6'ya geçiş çalışmalarında, birkaç yıl boyunca omurga ve uç birimlerde çift yığın yönteminin kullanılması uygun olup, IPv6'ya geçiş belirli bir süre alacağı için IPv6 ağlarının IPv4 ağları ile haberleşmesinde sadece aynı ağda değil internet üzerinden de haberleşebilen IPv6 bağlantısı amaçlayan 6to4 tünelleme tekniğinin kullanımının daha uygun olacağı öngörülmektedir.

IPv6 için yönlendirme algoritmaları ve bu algoritmaları kullanarak yönlendirme işlemini gerçekleştiren yönlendirme protokolleri incelenmiştir. Performans analizi için kullanılan CPT 5.2 benzetim programı ile modellenen ağaç, halka, yıldız topolojileri ve karmaşık bir ağ yapısı üzerinde, bütün bilgisayar ve anahtar cihazlarının gerekli yapılandırma ayarları yapılmıştır. Yönlendiriciler için kullanılacak olan OSPFv3, RIPng, EIGRPv6 ve statik yönlendirme protokollerine göre farklı yönlendirici yapılandırma ayarları başarıyla gerçekleştirilerek farklı boyuttaki veri paketleri için benzetim yapılmıştır. Modellenen ağ üzerindeki benzetim sonuçları doğrultusunda karşılaştırılan yönlendirme protokollerinin paket gecikmesi ve veri transfer hızı

performans kriteri olarak değerlendirildiğinde en uygun IPv6 yönlendirme protokolü olan OSPFv3 önerilmiştir.

İleriki çalışmalarda, IS-ISv6 ve BGPv6 yönlendirme protokolleri de dâhil edilerek farklı benzetim programları kullanılıp daha büyük boyuttaki paketlerle yönlendirme protokollerinin performans analizlerinin yapılması, IPv6 yönlendirme protokollerinin güvenlik açısından araştırılarak kıyaslanması ve gerçek ağ ortamında daha gelişmiş farklı yönlendirici cihazları kullanarak bu performans analizlerinin daha iyi sonuçlarının elde edilmesi hedeflenebilir.

Ayrıca, IPv6 yönlendirme protokollerinin yeni sezgisel optimizasyon algoritmaları kullanarak iyileştirilip IPv6 uygulamaları geliştirilmesi ve mobil cihazlarda IPv6 kullanımının yaygınlaştırılması amaçlanabilir.

KAYNAKLAR

1. Buckhanan, B., Handbook of Data Communication and Networks 1999 ed., Kluwer Academic Publishers, Boston, 211-212, 1999.
2. Krose, J.F., Ross, K.W., Computer Networking A top-down Approach Featuring The Internet 2nd ed., Addison Wesley, Pearson, 369-375, 334-33, 2003.
3. Huitema, C., Routing in the Internet, Prentic-Hall, New Jersey, 1995.
4. Huitema, C., IPv6: The New Internet Protocol, Prentice-Hall: Upper Saddle River, NJ, 247 pp, 1998.
5. RFC 2460; Deering, S., Hinden, R., Internet Protocol Version 6 (IPv6) Specification, 1998.
6. Cisco Systems IOS Learning Services, The ABCs of IP Version 6, Understanding the Essentials Series, 2002.
7. Cisco Systems, IPv6 Tutorial, South Asian Network Operators Group, http://www.sanog.org/resources/sanog5-pfs-ipv6-tutorial.pdf, 2005.
8. Li, C., et al, IPv6 Development in China, China Education and Research Network (CERNET) Center, 2002.
9. RFC 1819; Delgrossi L., Berger, L., Internet Stream Protocol Version 2 (ST2), 1995.
10. Süslü, A., PC Temelli Çift IP Destekli (IPv4-IPv6) Yönlendirici Benzetimi, Yüksek Lisans Tezi, Beykent Üniversitesi, İstanbul, 2005.
11. Erdoğan, K., IPv4'ten IPv6'ya Geçiş Süreci İçin IPv6 Tünel ve Sanal Hedef IP Teknikleri, Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara, 2007.
12. Şahin, M., IPv6 Sistem Geçişi, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006.
13. Chan, C., et al, High-Performance IP Forwarding With Efficient Routing-Table Update, Computer Communications,26, 1681-1692, 2003.
14. Warkhede, P., Suri, S., Varghese, G., Multiway Range Trees: Scalable IP Lookup With Fast Updates, Computer Networks, 44, 289–303, 2004.
15. Lampson, B., Srinivasan, V., Varghese, G., IP Lookups Using Multiway and Multicolumn Search, IEEE/ACM Transactions on Networking, Vol. 7, No. 3, 1999.

16. Dicle, Z., et al, IPv6 ve IPv4 İçin Karşılaştıralı Bilgisayar Benzetimi, Elektrik Elektronik Bilgisayar Mühendisliği 11. Ulusal Kongresi ve Fuarı, İstanbul, 2005.
17. Blaga, T., Dobrota, V., Testing IPv4/IPv6-Based Unicast/Multicast Routing Protocols Using Linux and FreeBSD, COST290, 1st Management Committee Meeting, Malta, 2004.
18. Ustundag, D.T., Comperative Routing Performance Analysis of IPv4 and IPv6, Master Thesis, Atilim University, Ankara, 2009.
19. Saaristo, S., Implementation of IS-IS Routing Protocol for IP versions 4 and 6, Master of Science Thesis, Tampere University, Helsinki, 2002.
20. Hua, L., et al, Conformance Test Research on OSPFv3 Based on XML, Computer Science, 2007.
21. Honkola, J., OSPF and IS-IS Evolution, HUT T-110.551 Seminar on Internetworking, 2004.
22. Ziring, N., Router Security Configuration Guide Supplement - Security for IPv6 Routers, National Security Agency, 2006.
23. Xue-qian, Z., Jia-qi, C., Analysis and Comparison of RIPng and OSPFv3 in IPv6 Network,Communications Technology, 2008.
24. Xing, Y., et al, Research and Practice on Conformance Test of RIPng Protocol of IPv6, Computer Engineering, Vol 32, No 20, 2006.
25. Wang, J., et al, OSPFv3 Protocol Simulation with Colored Petri Nets, IEEE, 2003.
26. Convery, S., Miller, D., IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation, Cisco Systems Paper, 2004.
27. RFC 791; Information Sciences Institute University of Southern California, Internet Protocol Darpa Iternet Program Protocol Specification, 1981.
28. Peterson, S., Extension Of A Network Scanning Tool With IPv6 Features (Nmap), End of Studies Dissertation, Liege University, Embourg, 2002.
29. RFC 1519; Fuller, V., et al, Classless Inter-Domain Routing (CIDR), 1993.
30. RFC 3027; Holdrege, M., Srisuresh, P., Protocol Complications with the IP Network Address Translator, 2001.
31. Can, E., IPv6 Üzerinden Ses Uygulaması ve Paket Analizi, Yüksek Lisans Tezi, Beykent Üniversitesi, İstanbul, 2006.

32. Microsoft Corporation, Introduction to IP Version 6, 2004.
33. RFC 3775; Johnson, D., Perkins, C., Arkko, J., Mobility Support in IPv6, 2004.
34. Altuğ, R.O., Ev Ağlarında Otomatik IPv6 Yönlendirici Yapılandırılması, Yüksek Lisans Tezi, Anadolu Üniversitesi, Eskişehir, 2006.
35. Efe, A., Yeni Nesil Internet Protokolü IPv6'da Güvenlik Riskleri ve Olası Çözüm Önerileri, Yüksek Lisans Tezi, Beykent Üniversitesi, İstanbul, 2006.
36. Gai, S., Internetworking IPv6 with Cisco Routers, McGraw-Hill, 1998.
37. RFC 3513; Deering, S., Hinden, R., Internet Protocol Version 6 (IPv6) Addressing Architecture, 2003.
38. RFC 4193; Hinden, R., Haberman, B., Unique Local IPv6 Unicast Addresses, 2005.
39. RFC 2461; Narten, T., Nordmark, E., Simpson, W., Neighbor Discovery for IP Version 6 (IPv6), 1998.
40. Huang, C.Y., A New Mechanism using IPv6 for Smooth Handoff in an Integrated Ad Hoc and Cellular Network under High Speed Movement, Master Thesis, National Dong Hwa University, Hualien, 2002.
41. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, Ankara, http://www.tubitak.gov.tr , Kasım 2009.
42. Ulusal Akademik Ağ ve Bilgi Merkezi, Ankara, http://www.ulakbim.gov.tr, Kasım 2009.
43. Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçiş Projesi, Ankara, http://www.ipv6.net.tr, Temmuz 2010.
44. Bilgi Teknolojileri ve İletişim Kurumu, Ankara, http://www.tk.gov.tr/Yayin/Is_Planlari/2007_is_plani.pdf, Kasım 2009.
45. Bilgi Teknolojileri ve İletişim Kurumu, Ankara, http://www.tk.gov.tr/Etkinlikler/Ulusal_Etkinlikler/protokoller/2007/ulakbim_protokol.htm, Kasım 2009.
46. IPv6 Promotion Council, Japan, http://www.v6pc.jp/en/index.phtml, Nov. 2009.
47. u-Japan Policy, Japan, http://www.soumu.go.jp/menu_02/ict/u-japan_en/index.html, Nov. 2009.
48. China-Japan IPv6 into Operation, Romania, http://www.fmprc.gov.cn/ce/cero/rom/kjwh/t197050.htm, Nov. 2009.

49. Orcan, S., et al., Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi, TBD 25. Bilişim Kurultayı, Sheraton Convention Center, Ankara, 2008.
50. Free Online Encyclopedia, Wikipedia Foundation Inc, USA, http://tr.wikipedia.org/wiki/IPv6_Yayılımı#ABD, Dec. 2009.
51. Chown, T., Palet, J., IPv6 R&D and Commerical Activities in Europa, Proceedings of the 2004 International Symposium on Applications and the Internet Workshops (SAINTW'04), IEEE 2004.
52. Bolat, A., et al., Ulusal IPv6'ya Geçiş ve Stratejiler, Bilgi Güvenliği Kriptoloji Konferansı 08, ODTÜ, Ankara, 2008.
53. Samad, M., et al., Deploying Internet Protocol Version 6 (IPv6) Over Internet Protocol Version 4 (IPv4) Tunnel, IEEE CNF, Research and Development, 109 – 112, 2002.
54. Kadayıf, İ., Kabal, O., IPv4 Ağlarının IPv6 Ağlarına Entegrasyonu, Çanakkale Onsekiz Mart Üniversitesi Bilimsel Araştırma Projeleri Komisyonu, Çanakkale, 2006.
55. RFC 2893; Gilligan, R., Nordmark, E., Transition Mechanisms for IPv6 Hosts and Routers, 2000.
56. Wang, K., Yeo, A.K., Ananda, A.L., DTTS: A Transparent and Scalable Solution for IPv4 to IPv6 Transition, IEEE CNF, Computer Communications and Networks, 248 – 253, 2001.
57. Ayumu, Y.H., Takao, K., Yamazaki, H.K., Open 6to4 Relay Router Operation, IEEE CNF, Applications and the Internet Workshops, 266 – 269, 2003.
58. Chown, T., IPv6 Campus Transition Experiences, IEEE CNF, Applications and the InternetWorkshops, 46 – 49, 2005.
59. Lee, S.D., Shin, M.K., Kim, H.J., The Implementaion of ISATAP Router, IEEE CNF, Advanced Communication Technology, Volume 2, 3, 2006.
60. RFC 3056; Carpenter, B., Moore, K., Connection of IPv6 Domains via IPv4 Clouds, 2001.
61. Waddington, D.G., Chang, F., Realizing the Transition to IPv6, IEEE JNL, Communications Magazine, 40:138 – 147, 2002.
62. Bozkurt, B., Bilgisayar Ağlarında Yönlendirici Algoritmaları için Simülatör, Yüksek Lisans Tezi, Marmara Üniversitesi, İstanbul, 2001.
63. Beijnum, I.V., Running IPv6, Apress Press, New York, 2006.

64. Schuh, S., Migrating Small Business Networks To IPv6, Vienna University, Master Thesis, Wien, 2006.
65. Dunmore, M., An IPv6 Deployment Guide, 6NET, 2005.
66. Narayanan, S., Simulation of Dijkstra Routing Algorithm**,** BE- Electronics, 2003.
67. Musa, A.S.S., Routing Algorithm Based On Optical Multi-Protocol Label Switching Using Wavelength and Code Division Multiplexing**,** Ph.D. Thesis, Texas University, El Paso, 2005.
68. MEGEP, Yönlendirme Temelleri, Milli Eğitim Bakanlığı, Ankara, 2008.
69. Goodrich, M.T., Efficient and Secure Network Routing Algorithms, Johns Hopkins University, Baltimore, 2001.
70. Cisco Systems, Introduction to BGP, Cisco ISP Workshops, http://map.twnic.net.tw/ip93/doc/k/bgp.pdf, 2003.
71. Free Online Encyclopedia, Wikipedia Foundation Inc, USA, http://en.wikipedia.org/wiki/Path_vector_protocol, Aug. 2009.
72. Özbilen, A., Genetik Algoritma ile İletişim Ağlarında Yönlendirme Optimizasyonu, Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara, 2006.
73. Graziani, R., Johnson, A., Routing Protocols and Concepts CCNA Exploration Companion Guide, Cisco Press, 2007.
74. Davies, J., Understanding IPv6, Microsoft Press Second Edition, Washington, 2008.
75. Loshin, P., IPv6 Theory Protocol and Practice, Elsevier Inc., USA, 2004.
76. RFC 2080; Malkin, G., Minnear, R., RIPng for IPv6, 1997.
77. RFC 2740; Coltun, R., Ferguson, D., Moy, J., OSPF for IPv6, 1999.
78. Hopps, C., Routing IPv6 with IS-IS, Internet-Draft, 2007.
79. Free Online Encyclopedia, Wikipedia Foundation Inc, USA, http://en.wikipedia.org/wiki/Internet_draft, Aug. 2009.
80. RFC 1771; Rekhter, Y., Li, T., A Border Gateway Protocol 4 (BGP-4), 1995.
81. RFC 2545; Marques, P., Dupont, F., Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing, 1999.
82. Hagen, S., IPv6 Essentials, Chapter 8, O'Reilly, USA, 2006.
83. Cisco Systems, CCNA Exploration Routing Protocols and Concepts, Chapter 9 (EIGRP), Cisco Networking Academy, 2007.

84. Cisco Systems, Cisco Packet Tracer, Cisco Packet Tracer Data Sheet, 2009.
85. Cisco Systems, Packet Tracer 5.0, Cisco Packet Tracer 5.0 Data Sheet, 2008.
86. Emre, B., Trafik Analizinin Belirlenmesi ve Engellenmesi, Ender UNIX Yazılım Geliştirme Takımı, 2007.
87. Karaarslan, E., Akın, G., Demir, H., Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Yöntemleri, Akademik Bilişim 2008, Çanakkale 18 Mart Üniversitesi, Çanakkale, 2008.
88. MEGEP, Alt Ağlar, Milli Eğitim Bakanlığı, Ankara, 2008.

ÖZGEÇMİŞ

Mevlüt Doğru, 1985 yılında Ürgüp'te doğdu. İlköğrenimini Ürgüp'te, orta öğrenimini Kayseri'de tamamladı. 1999 yılında Kayseri Özel Hisarcıklıoğlu Fen Lisesini kazandı. 2002 yılında Erciyes Üniversitesi'nde bir yıl yabancı dil hazırlık eğitimi aldıktan sonra aynı üniversitenin Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nden 2007 yılında mezun oldu. Aynı yıl Erciyes Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda Yüksek Lisans eğitimine başladı. 2008/2009 eğitim öğretim yılında Erciyes Üniversitesi Develi Hüseyin Şahin Meslek Yüksekokulu'nda ücretli öğretim görevliliği yapan Mevlüt Doğru, Aralık 2009'dan itibaren Sosyal Güvenlik Kurumu Yazılım Geliştirme ve Sistem Daire Başkanlığı'nda bilgisayar mühendisi olarak görevini sürdürmektedir.

Tel : 0 535 878 1206
E-posta : mdogru50@yahoo.com
Adres : Sosyal Güvenlik Kurumu Yazılım Geliştirme ve Sistem Daire Başk.
Mamak Cad. No:213/C 06620 Mamak/ANKARA