**T.C.**

**SOSYAL GÜVENLİK KURUMU BAŞKANLIĞI**

**SGK E-Hizmetlerinin sunumunda daha erişilebilir ve ekonomik bir çözüm olarak: SGK KIOSK**

**Sosyal Güvenlik Uzmanlığı Tezi**

**Hazırlayan**

**Yeliz GÜLTEKİN KÜÇÜKAĞAOĞLU**

**Tez Danışmanı**

**Uzman Fethullah EVLİYAOĞLU**

**Şubat 2016**

**Ankara**

Yeliz GÜÜLTEKİN KÜÇÜKAĞAOĞLU tarafından hazırlanan bu çalışmanın Sosyal Güvenlik Uzmanlığı Tezi olarak uygun olduğunu onaylarım. …./…./2016

Tez Danışmanının Adı SOYADI: Uzman Fethullah EVLİYAOĞLU

İmzası:

Bu çalışma, Kurulumuz tarafından oy birliği / oy çokluğu ile Sosyal Güvenlik Uzmanlığı Tezi olarak kabul edilmiştir.

|  |  |  |
| --- | --- | --- |
|  | **Adı Soyadı ve Unvanı** | **İmzası** |
| Başkan | : ………………………………………………… | …....………... |
| Üye | : …………………………………………………. | …....………... |
| Üye | : ………………………………………………… | …....………... |
| Üye | : …………………………………………………. | …....………... |
| Üye | : ………………………………………………… | …....………... |

Tarih: …./…./………

ÖNSÖZ

Bu çalışma sırasında tecrübe ve bilgisi ile beni yönlendiren tez danışmanım Yrd. Doç. Dr. Enis Karaarslan’a, ihtiyaç duyduğum konularda desteklerini esirgemeyen meslektaşlarım İbrahim ARSLAN, Celal DOĞAN ve Hüseyin KARAMAN’a, ayrıca her koşulda yanımda olan annem, babam ve eşime teşekkürü borç bilirim.

**Ankara 2014 Ahmet Furkan YENİCEOĞLU**

BEYAN

Bu tezin tasarımı, hazırlanması, yürütülmesi, araştırmalarının yapılması ve bulgularının analizlerinde akademik kurallara ve bilimsel etik davranış ilkelerine uyduğumu, ayrıca, bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi beyan ederim. …./…./……..

Adı ve SOYADI: Yeliz GÜLTEKİN KÜÇÜKAĞAOĞLU

İmzası:

ÖZET

**Sosyal Güvenlik Uzmanlığı Tezi**

**SGK E-Hizmetlerinin sunumunda daha erişilebilir ve ekonomik bir çözüm olarak: SGK KIOSK**

**Yeliz GÜLTEKİN KÜÜKAĞAOĞLU**

Bu çalışmanın amacı, Sosyal Güvenlik Kurumu hizmetlerine uzaktan ulaşabilmek için bir KIOSK sisteminin tasarlanmasıdır.

Tasarım öncesi e-SGK hizmetleri, insanların bilişim sistemlerine olan ilgileri ve bilişim alt yapıları incelenmiştir.

İncelemeler sonucunda neden KIOSK 'a ihtiyaç olduğu ve kazandıracakları üzerinde durulmuştur.

Tasarım için gerekli olabilecek donanım alternatifleri incelenmiştir. Ardından bu alternatifler arasında amaca en uygun olanı çeşitli kriterler ile belirlenmiştir.

Ardından işletim sistemi alternatifleri incelenmiştir. Aynı şekilde amaca en uygunu nedenleri ile birlikte açıklanmıştır.

Son olarak da kullanıcı yazılım arayüzü için aynı çalışmalar gerçekleştirilmiştir.

Tüm bu ön hazırlıkların ardından tasarıma başlanmıştır. Tasarımın test edilebilmesi için bir test veritabanı oluşturulmuş ve e-SGK hizmetlerinin bazıları benzetim yöntemi ile uygulamaya geçirilmiştir.

Tasarımın sonucunda bir KIOSK cihazı ortaya konulmuştur. Seçilen e-SGK uygulamalarında bazı denemeler gerçekleştirilmiştir. Bu denemelerde KIOSK 'un işlevleri denenmiştir. Bu sayede cihazın kolay kullanımlı, işlevsel ve ulaşılabilirliği görülmüştür.

**Anahtar Kelimeler:** KIOSK, e-SGK, SGK-KIOSK, e-SGK hizmetlerine ulaşım.

ABSTRACT

**Social Security Expertise Thesis**

**AS A MORE AVAILABLE AND ECONOMIC SOLUTION FOR SGK E-SERVICES : SGK KIOSK**

The purpose of this study is to design a KIOSK system to reach e-services of The Social Security Institution.

Before designing, information system infrastructures and interests of the people to information sytems have been analyzed.

As a result of analyzings they were focused why KIOSK is neccesary and the profits of it.

Hardware alternatives for designing have been investigated. Later, the most suitable one for the purpose determined among of them by various criterias.

After, operating systems have been investigated. In the same way, the most suitable one for the purpose has been described together with reasons.

Finally, for the user software interface, prgramming languages ang necessary tools have been investigated.

After all preliminary works, designing has been started. To test the design, a test database has been created and some services of the e-SGK have been applied by the simulation method.

As a result of design a KIOSK device has been revealed. Some tests have been executed for the selected e-SGK applications. During these tests the all functions of the KIOSK have been proven. Thus easy to useness, functionality and availability of the device have been observed.

Key Words: KIOSK, e-SGK, SGK-KIOSK, reach e-SGK services.

YÖNTEM

Hazırlanan çalışmanın amacı, Sosyal Güvenlik Kurumu bilgi işlem alt yapısı için IPv6’ya geçişin nasıl olabileceğinin açıklanmasıdır.

Yapılan çalışmada, konu ile ilgili teorik altyapıyı oluşturmak amacı ile kitap, makale, tez çalışmaları, süreli yayınlar, konferans ve seminer bildirileri vb. kaynaklardan yararlanılmıştır. Daha sonra Sosyal Güvenlik Kurumu bilgi işlem altyapısı üzerinde çalışılarak bu altyapıya uygun bir topoloji planı hazırlanmıştır. Hazırlanan topoloji planına uygun bir test ortamı kurulmuş ve bu test ortamında IPv6’ya geçiş için seçilen geçiş yöntemi kullanılarak uygulama çalışması yapılmıştır. Uygulama çalışmasında Sosyal Güvenlik Kurumu’nun internet üzerinden dışarıya verdiği hizmetlerin IPv6’ya geçirilmesi üzerinde yoğunlaşılmış, kurum iç ağı göz ardı edilmiştir.

**İÇİNDEKİLER**

[ÖNSÖZ i](#_Toc380153152)

[BEYAN i](#_Toc380153153)

[ÖZET ii](#_Toc380153154)

[ABSTRACT iii](#_Toc380153155)

[YÖNTEM iv](#_Toc380153156)

[GİRİŞ 1](#_Toc380153157)

[BİRİNCİ BÖLÜM 3](#_Toc380153158)

[TCP/IP YAPISI 3](#_Toc380153159)

[1.1 TCP/IP'ye Giriş 3](#_Toc380153160)

[1.2 OSI Referans Modeli 4](#_Toc380153161)

[1.3 TCP/IP (DOD) Referans Modeli 7](#_Toc380153162)

[1.3.1 TCP/IP Ağ Erişim Katmanı 9](#_Toc380153167)

[1.3.2 TCP/IP İnternet Katmanı 9](#_Toc380153168)

[1.3.2.1 Internet protocol 9](#_Toc380153169)

[1.3.2.2 Internet Control Message Protocol 11](#_Toc380153170)

[1.3.2.3 Adress Resolution Protocol (ARP) 12](#_Toc380153171)

[1.3.2.4 Reverse Address Resolution Protocol (RARP) 12](#_Toc380153172)

[1.3.3 TCP/IP İletim Katmanı 13](#_Toc380153173)

[1.3.4 TCP/IP Uygulama Katmanı 13](#_Toc380153174)

[1.4 IPV4 Adresleme, Alt ağlar ve Alt ağ maskesi 13](#_Toc380153175)

[1.4.1 IPV4 adres türleri 13](#_Toc380153177)

[1.4.2 Alt ağlar ve Alt ağ maskesi 16](#_Toc380153178)

[1.5 Network Address Translation (NAT) 18](#_Toc380153179)

[BÖLÜM 2 20](#_Toc380153180)

[INTERNET PROTOCOL VERSION 6 (IPV6) 20](#_Toc380153181)

[2.1 IPV6 Tarihçesi 20](#_Toc380153183)

[2.2 Yeni Nesil IP (IPV6) Gereksinimi 21](#_Toc380153184)

[2.3 IPV6 Adres Yapısı 25](#_Toc380153185)

[2.4 IPV6 Adres Öneki (Prefix) 27](#_Toc380153186)

[2.5 IPV6 Adres Türleri 27](#_Toc380153187)

[2.6 Unicast IPV6 Adres Türleri 28](#_Toc380153188)

[2.6.1 Global Unicast Adresler (Küresel tekil gönderim adresleri) 28](#_Toc380153196)

[2.6.2 Link-local adresler (Bağlantı yerel tekil gönderim adresleri) 28](#_Toc380153197)

[2.6.3 Unique local adresler (Eşsiz tekil gönderim adresleri) 29](#_Toc380153198)

[2.6.4 Multicast (Çoklu Gönderim Adresleri) 29](#_Toc380153199)

[2.7 IPV6 Başlık Yapısı 30](#_Toc380153200)

[2.8 IPV6 İle Gelen Yenilikler: 32](#_Toc380153201)

[2.8.1 Adres uzayının genişlemesi: 32](#_Toc380153204)

[2.8.2 Geliştirilmiş Güvenlik: 32](#_Toc380153205)

[2.8.3 Geliştirilmiş Servis Kalitesi (QOS) 32](#_Toc380153206)

[2.8.4 Multicast Dinleyici Keşfi (Multicast Listener Discovery, MLD) 32](#_Toc380153207)

[2.8.5 Internet Control Message Protocol Version 6 (ICMPv6) 33](#_Toc380153208)

[2.8.6 Komşu Keşfi (Neighbor Discovery) 33](#_Toc380153209)

[2.8.7 IPV6 Yönlendirme Protokolleri 34](#_Toc380153210)

[2.8.8 Otomatik Yapılandırma (Autoconfiguration) 34](#_Toc380153211)

[2.8.9 DHCPv6 35](#_Toc380153212)

[2.8.10 Dolaşılabilirlik (Mobility) 35](#_Toc380153213)

[2.9 IPV6 Geçişi 38](#_Toc380153214)

[2.9.1 İkili Yığın (Dual Stack) Yöntemi: 39](#_Toc380153216)

[2.9.2 Tünelleme Yöntemi: 40](#_Toc380153217)

[2.9.2.1 Elle Yapılandırılmış Tüneller 41](#_Toc380153218)

[2.9.2.2 6to4 Tüneli 41](#_Toc380153219)

[2.9.2.3 Isatap geçiş yöntemi 42](#_Toc380153220)

[2.9.2.4 Teredo Geçiş Yöntemi 43](#_Toc380153221)

[2.9.3 Çeviri Yöntemi 44](#_Toc380153222)

[BÖLÜM 3 45](#_Toc380153223)

[IPV6 GEÇİŞİ UYGULAMA ÇALIŞMASI 45](#_Toc380153224)

[3.1 Geçiş Hazırlığı 45](#_Toc380153226)

[3.2 Geçiş Çalışmaları 48](#_Toc380153227)

[3.2.1 Yönlendirici Yapılandırması 48](#_Toc380153231)

[3.2.2 Ateş Duvarı Yapılandırması 52](#_Toc380153232)

[3.2.3 Omurga Anahtar Yapılandırması 54](#_Toc380153233)

[3.2.4 Yük Dengeleyici Yapılandırması 56](#_Toc380153234)

[3.2.5 Uygulamanın Test Edilmesi 59](#_Toc380153235)

[DÖRDÜNCÜ BÖLÜM 61](#_Toc380153236)

[SONUÇ VE ÖNERİLER 61](#_Toc380153237)

[Şekil 1 OSI Referans Modeli Katmanları 10](#_Toc379967293)

[Şekil 2OSI Ve TCP/IP Referans Modelleri 13](#_Toc379967294)

[Şekil 3 TCP/IP protokolleri 14](#_Toc379967295)

[Şekil 4 IP Adres Başlığı 15](#_Toc379967296)

[Şekil 5 IP Adresi Gösterimi 18](#_Toc379967297)

[Şekil 6 A,B Ve C Sınıfı IP'ler 19](#_Toc379967298)

[Şekil 7 Rezerve IP Adresi Aralıkları 20](#_Toc379967299)

[Şekil 8 Alt Ağ Örneği 22](#_Toc379967300)

[Şekil 9 NAT Gösterimi 24](#_Toc379967301)

[Şekil 10 Bölgesel İnternet Kayıt Kuruluşları 28](#_Toc379967302)

[Şekil 11Dağıtılan IP Bloklarının Bir Kısmı 29](#_Toc379967303)

[Şekil 12 RIPE NCC IPv4 Havuzu 30](#_Toc379967304)

[Şekil 13IPv6 Adresi Tahsis Eden LIR Sayısının Zamanla Değişimi 31](#_Toc379967305)

[Şekil 14 IPv6 Adresi Gösterimi 32](#_Toc379967306)

[Şekil 15 IPv6 Adres Türleri 36](#_Toc379967307)

[Şekil 16 IPv4 Ve IPv6 Adres Başlıkları 37](#_Toc379967308)

[Şekil 17 IPv6 İle Birlikte Gelen Yenilikler 43](#_Toc379967309)

[Şekil 18 İkili Yığın Gösterimi 46](#_Toc379967310)

[Şekil 19 6to4 Tünel Gösterimi 48](#_Toc379967311)

[Şekil 20 ISATAP Tüneli 49](#_Toc379967312)

[Şekil 21SGK IPv6 bilgileri 52](#_Toc379967313)

[Şekil 22 Uygulama Topolojisi 53](#_Toc379967314)

[Şekil 23 Üçüncü Seviye Yönlendirme Ve Güvenlik Cihazları 54](#_Toc379967315)

[Şekil 24 Yönlendirici Arayüz Yapılandırması 57](#_Toc379967316)

[Şekil 25 Yönlendirici İçin Yönlendirme Yapılandırması 58](#_Toc379967317)

[Şekil 26 Yönlendiricinin IPv6 Rota Tablosu 59](#_Toc379967318)

[Şekil 27 Ateş Duvarı Arayüz Yapılandırması 60](#_Toc379967319)

[Şekil 28 Ateş Duvarı Rota Tablosu 60](#_Toc379967320)

[Şekil 29 Omurga Anahtar Vlan Arayüz IP Yapılandırması 61](#_Toc379967321)

[Şekil 30 Vlan Arayüz IP'leri 62](#_Toc379967322)

[Şekil 31 Omurga Anahtar IPv6 Yönlendirme Tablosu 63](#_Toc379967323)

[Şekil 32 Yük Dengeleyici Cihazın IPv6 Geçişinde Kullanılması 64](#_Toc379967324)

[Şekil 33Yük Dengeleyeci Self-IP Ataması 64](#_Toc379967325)

[Şekil 34 Yük Dengeleyici Sanal IP Ataması 65](#_Toc379967326)

[Şekil 35 Yük Dengeleyici Yönlendirme 65](#_Toc379967327)

[Şekil 36 Türk Telekom Tarafı Bağlantı Testi 66](#_Toc379967328)

[Şekil 37 Test Sunucusu Ekran Görüntüsü 67](#_Toc379967329)

**KISALTMALAR**

**IPV4 :** İnternet Protocol Version 4

**IPV6 :** İnternet Protocol Version 6

**DOD :** Department Of Defense

**ARPA :** Advanced Research Project Agency

**TCP/IP :** Transmission Control Protocol/Internet Protocol

**IAB :** Internet Activities Board

**IETF :** Internet Engineering Task Force

**RFC :** Request For Comments

**NCP :** Network Control Protocol

**WWW :** World Wide Web

**ISO :** International Organization for Standardization

**OSI :** Open Systems Interconnection

**MAC :** Media Access Control

**ICMP**  **:** Internet Control Message Protocol

**TCP :** Transmission Control Protocol

**UDP :** User Datagram Protocol

**HTTP :** Hyper-Text Transfer Protocol

**HTTPS :** Hyper-Text Transfer Protocol Secure

**FTP :** File Transfer Protocol

**SMTP :** Simple Mail Transfer Protocol

**STP :** Spanning Tree Protocol

**PPP :** Point to Point Protocol

**FDDI :** Fiber Distributed Data Interface

**ATM :** Asynchronous Transfer Mode

**SLIP :** Serial Line Internet Protocol

**ARP :** Adress Resolution Protocol

**RARP :** Reverse Address Resolution Protocol

**TFTP :** Trivial File Transfer Protocol

**NFS :** Network File System

**DNS :** Domain Name System

**DHCP :** Dynamic Host Configuration Protocol

**NAT :** Network Address Translation

**PAT :** Port Address Translation

**QOS :** Quality Of Service

**CIDR :** Classless Inter Domain Routing

**IANA :** Internet Assigned Numbers Authority

**IPSEC :** Internet Protocol Security

**MLD :** Mulicast Listener Discovery

**IGMP :** Internet Group Management Protocol

**ICMPv6 :** Internet Control Message Protocol Version 6

**RDISC :** Router Discovery

**RIPNG :** Routing Information Protocol Next Generation

**OSPFv3 :** Open Shortest Path Version 3

**EIGRP :** Enhanced Interior Gateway Routing Protocol

**BGP4+ :** Border Gateway Protocol 4+

**DHCPv6 :** Dynamic Host Configuration Protocol Version 6

**OECD :** [Organisation for Economic Co-operation and Development](https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&sqi=2&ved=0CCkQFjAA&url=http%3A%2F%2Fwww.oecd.org%2F&ei=WfH9UqOBJYiohAeVsIHgDw&usg=AFQjCNHOvha_Kgd0PZryx-7E0w8swGHlKA&sig2=7S5lkpfyCsvc50et8zB01g&bvm=bv.61190604,d.ZG4)

**NAT-PT :** Network Address Translation - Port Translation

GİRİŞ

İnternet kavramı 1980’lerde ortaya çıkmaya başlamıştır. İnternet çok fazla sayıda cihazın bir araya gelerek oluşturduğu ağı ifade eder. ilk olarak askeri ve bilimsel amaçlarla kullanılan internet, 1990’lı yıllarda kişisel bilgisayarların yaygınlaşması ile birlikte hayatın her alanında kullanılan bir yapı halini almıştır. Bu hızlı gelişimle birlikte internet bilgi edinme, eğlence, iletişim, e-ticaret, bankacılık ve finans hizmetleri, kamu hizmetleri gibi alanlarda vazgeçilmez hale gelerek yapılan birçok iş ve işlemin odak noktası haline gelmiştir.

İnternetin altyapısını bir dizi protokol oluşturur. Bu protokoller haberleşme için kullanılacak kuralları belirler. İnternet protokolünün dördüncü versiyonu olan IPV4 (internet protocol version 4) Dünya’da geniş alana yayılmış ve genel kabul görmüş ilk versiyondur. İnternet alt yapısı ilk tasarlandığında günümüzdeki kadar yaygın kullanılacağı öngörülememişti. İnternet kullanımının artması ile birlikte IPV4 protokolü de zaman içerisinde günümüz ihtiyaçlarını karşılamakta yetersiz kalmıştır. Bu nedenle daha gelişmiş özelliklere sahip ve en önemlisi azalan IP adresi sorununu çözmek için yeni nesil bir İnternet Protokolü geliştirilmiştir. Bu protokolde internet protokolünün altıncı versiyonu IPV6 (internet protocol version 6) olarak adlandırılmıştır. Bu yeni nesil protokolle birlikte adres uzayı büyümüş, güvenlik ve servis kalitesi gibi özellikler geliştirilmiş, otomatik yapılandırma gibi yeni özellikler gelmiştir.

Sosyal Güvenlik Kurumu bir kamu kurumu olarak internet üzerinden vatandaşlara çeşitli hizmetler sunmaktadır. Bu hizmetlerin kalitesi ve sürekliliği açısından yeni nesil internet protokolü olan IPV6’ya geçişin çeşitli faydaları olacaktır.

Konu ile ilgili yapılan bu çalışma dört bölümden oluşmaktadır. Birinci bölümde TCP/IP yapısı üzerinde durulmuş ve IPV4 kavramı detaylı olarak incelenmiştir. İkinci bölümde ise yeni nesil internet protokolünün gerekliliği irdelenmiş, IPV6 kavramı açıklanmış, IPV6 ile birlikte gelen yenilikler anlatılmış, ve IPV6’ya geçiş için hangi yöntemlerin kullanılabileceği araştırılmıştır. Üçüncü bölümde ise Sosyal Güvenlik Kurumu alt yapı topolojisi örnek alınarak kurulan yapıda seçilen yöntemle IPV6’ya geçiş uygulaması yapılmıştır. Sonuç kısmında ise yapılan çalışma özetlenmiş ve öneriler sunulmuştur.

BİRİNCİ BÖLÜM

TCP/IP YAPISI

* 1. TCP/IP'ye Giriş

Birden daha fazla bilgisayarın bir araya gelerek iletişim kurabildiği yapıya bilgisayar ağı denir.Aynı ağ içerisinde bulunan cihazların birbiri ile iletişime geçebilmesi, aralarında veri aktarımı olabilmesi, birlikte çalışabilmeleri için konuşabilecekleri ortak bir dile ihtiyaçları vardır. Bu dile protokol adı verilir.

Birleşik Devletler ile Sovyetler Birliği arasında ikinci dünya savaşı sonrası başlayan soğuk savaş Sovyetler Birliği'nin uzaya uydu göndermesi ile yeni bir döneme girdi. Eğer Sovyetler Birliği uzaya uydu gönderebiliyorlarsa nükleer başlık taşıyan füzelerle Amerika'yı vurabilirlerdi. Bu uzay, teknoloji ve silahlanma yarışı sırasında Birleşik Devletler bilim ve teknoloji politikalarını yenilemeye başladı. Bu amaçla yapılan çalışmlardan biri de Birleşik Devletler Savunma Departmanına (DOD, Department Of Defense) bağlı İleri Düzey Araştırma Kurumu'nun (ARPA, Advanced Research Project Agency) kuruluşudur.[[1]](#footnote-2)

İnternet ARPA'nın 1969 yılında ARPANET adındaki ağı oluşturması ile ortaya çıkmaya başladı. ARPANET paket anahtarlamalı bir ağ olup ilk başlarda askeri amaçlarla kullanıldı. Üniversiteler ve çeşitli araştırma kurumlarının da bu ağı kullanmaya başlaması ile birlikte ARPANET büyümeye başladı. Birleşik Devletler Savunma Departmanı'nın olağan üstü koşullarda çalışabilecek hızlı bir ağa ihtiyacı vardı. Bu nedenle ARPA 1970'li yıllarda ise bu ağda kullanılmak için ARPA, TCP/IP'nin (İletim kontrolü protokolü/internet protokol) geliştirilmesine destek verdi ve TCP/IP protokolü geliştirilmeye başlandı.[[2]](#footnote-3)

"1983 yılında askeri birimlerin ARPANET’ten TCP/IP protokol mimarisine geçmesi ile birlikte artık TCP/IP haberleşmedeki birincil protokol olmuş, daha sonra "internet" kelimesi sıklıkla kullanılmaya başlanmıştır."[[3]](#footnote-4) Askeri amaçlar için geliştirilen internet teknolojisi zamanla üniversiteler, çeşitli araştırma kurumları, kamu kurumları tarafından da kullanılmaya başlandı. İnternette haberleşmek için DECnet, IPX, SNA, XNS gibi protokoller de bilgisayar üreticileri tarafından oluşturulmuştur. Fakat günümüzde tüm üreticilerin desteklediği TCP/IP protokolü internette kullanılan ortak protokol haline gelmiştir.

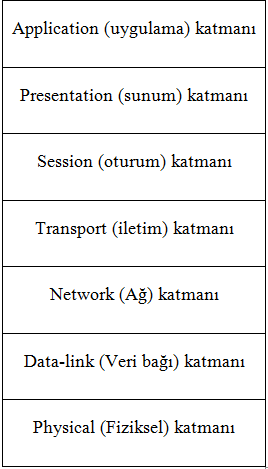
Şu anda internet üzerindeki geliştirmeler IAB (internet activities board) tarafından yönetilen IETF (Internet Engineering Task Force) adlı kuruluşun hazırladığı RFC'ler (Request For Comments) ile yapılmaktadır. RFC'ler internetle ilgili teknik geliştirmelerin yayınlandığı dökümanlardır.

RFC 2235’de internetin gelişimi ile ilgili çeşitli bilgiler verilmiştir. İnternetin gelişim süreci içerisinde, 1969’da “Steve Crocker” ilk RFC belgesini oluşturmuş, 1970 yılında ARPANET ağı için NCP (Network Control Protocol) kullanılmaya başlanmış, 1971 yılında ARPANET ağı 15 uç noktaya ve 23 kullanıcıya ulaşmış, 1973 yılında ARPANET ağına ilk yurtdışı bağlantısı İngiltere’den (The College Of London) yapılmış, 1976 yılında Kraliçe 2. Elizabeth ilk e-postayı göndermiş, 1983 yılında ARPANET ağında NCP yerine TCP/IP kullanılmaya başlanmış, 1987 yılında internet kullanıcısı sayısı 10.000’e 1988 yılında 60.000’e çıkmış, 1991 yılında WWW (World Wide Web) geliştirilmeye başlanmış, 1992 yılında kullanıcı sayısı 1.000.000’a çıkmış, 1994’de ilk internet üzerinden alışveriş yapılmış, 1997 yılında ise 2000. RFC yayınlanmıştır.[[4]](#footnote-5)

* 1. OSI Referans Modeli

Bilgisayar ağlarının ilk dönemlerinde farklı protokollere sahip ağlar bulunmaktaydı. Bu protokoller üreticiden üreticiye değişebiliyordu. Bu durum farklı protokollerde çalışan ağların iletişi açısından sorun oluşturabiliyordu. Bu sorunu giderebilmek için 1970'lerin sonunda International Organization for Standardization (ISO) tarafından Open Systems Interconnection (OSI) referans modeli oluşturuldu.[[5]](#footnote-6)

OSI referans modeli hiyerarşik olarak katmanlar oluşan bir yapıdır. Farklı üreticilerin cihazlarının birbirleri ile iletişim kurabilmeleri için aradaki haberleşmenin nasıl olacağını açıklar. OSI referans modelinin katmanları şekil 1'de gösterilmektedir.[[6]](#footnote-7)



Şekil 0 OSI Referans Modeli Katmanları

OSI referans modelinde 1. katman olan fiziksel katman (physcal), verinin elektriksel yada optik sinyallere çevrildiği katmandır. Fiziksel kablolar gibi ekipmanlar bu katmanda bulunur.

OSI referans modelinde 2. katman olan Veri bağı katmanı, ağ katmanından gelen paketleri çerçevelere (frame) böler. Bu katmanda adresleme MAC (Media Access Control) adresleri ile ile yapılır. MAC adresi üretici firma tarafından network kartına işlenen 48 bitlik eşsiz bir adrestir.[[7]](#footnote-8) Veri bağı katmanında aynı yerel ağ içerisindeki cihazlar anahtar (switch) aracılığı ile iletişim kurabilir. STP (spanning tree protocol), PPP (point to point protocol) gibi protokoller bu katmanda çalışırlar.

OSI referans modelinde 3. katman olan Ağ katmanı (network), kaynak ve hedefin aynı ağda mı farklı ağda mı olduğuna bakarak yönlendirme mi yada anahtarlama mı yapılacağına karar verir. 2. katmanda kullanılan MAC adresleri kaynak ve hedef farklı ağlarda ise çok anlamlı olmaz. Farklı ağlardaki hedeflerle iletişim kurmak için IP adresi adı verilen mantıksal adresler kullanılır. IP, ICMP (internet control message Protocol) gibi protokoller ağ katmanında çalışan protokollere örnek olarak gösterilebilirler.

OSI referans modelinde 4. katman olan iletim katmanı (transport), oturum katmanından gelen veriyi daha küçük parçalara bölerek ağ katmanından veriyi göndermeye hazır hale getirir. Ayrıca verinin güvenli bir şekilde karşı tarafa iletilip iletilmediğini kontrol eder. Bu katmanda TCP (Transmission Control Protocol) ve UDP (User Datagram Protocol) olmak üzere iki adet protokol kullanılır. Veri iletiminin karşı tarafa iletiminde oluşan kayıpların göz ardı edilebildiği, yüksek veri iletimi hızı gerektiren uygulamalarda (ses ve video iletimi gibi) UDP protokolü kullanılır veri iletilirken kayıp olup olmadığı kontrol edilmez. TCP protokolü ile veri iletiminde ise veriler parçalara bölünür (data segmentation), bölünen bu parçalar karşı tarafa sıra ile gönderilir. Karşı tarafın aldığı paketler içerisinde eksik olup olmadığı karşılıklı olarak haberleşerek kontrol edilir. Eksik paketler var ise tekrar gönderilir. Ve paketler geliş sırasına göre tekrar sıralanır.[[8]](#footnote-9) Ayrıca port numaralarının paketlere eklenip karşı tarafta tekrar değerlendirilmesi bu katman tarafından yapılır. Port numaraları ip adresi bilgisi bilgisine eklenir. Http (hyper-text transfer protocol): 80, Https (hyper-text transfer protocol secure): 443 gibi bazı servisler özel port numaraları kullanırlar.

OSI referans modelinde 5. katman olan oturum katmanı (session), haberleşme oturumlarını başlatan, yöneten ve sonlandırmaktan sorumlu olan katmandır. Ağa bağlı cihazlar arasında bir veya birden fazla oturum açılabilir. Bir sunucuya kullanıcılar çok fazla sayıda oturum açabilirler. Açılan bu oturumları yönetmek oturum katmanının görevidir.

OSI referans modelinde 6. katman olan sunum katmanı (presentation) uygulama katmanından gelen veriyi diğer cihazlarında anlayabileceği formata çevirme görevini üstlenmiştir. Sunum katmanın sağladığı hizmetler arasında veri şifreleme ve sıkıştırma işlemleri de sayılabilir. "Veri sıkıştırma işleminin sunum katmanında yapılması sayesinde, bu servisin uygulamalar tarafından geliştirilmesine gerek kalmaması ve iletim katmanının gerekli olmadığında bu servisi kullanmaması sağlanabilmektedir."[[9]](#footnote-10)

Osi referans modelinde 7. katman olan uygulama katmanı (application), OSI referans modelinin en üst katmanıdır. Bu katmanın protokolleri doğrudan son kullanıcılara hizmet verir. FTP (file transfer protocol), SMTP (simple mail transfer protocol), HTTP gibi uygulamalar bu katmanda çalışmaktadır.

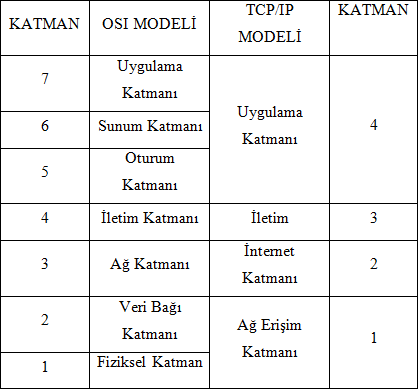
* 1. TCP/IP (DOD) Referans Modeli

TCP/IP modeli OSI modeline benzer şekilde hiyerarşik yapıda kurgulanmıştır. OSI modelindeki bazı katmanların birleştirilmesiyle oluşturulmuş bir modeldir. Yedi katman yerine dört katmandan oluşur. RFC 1122'de katmanlar açıklanmıştır.

Bu dört katman şunlardır:

* Ağ erişim katmanı (Network Access, link layer)
* İnternet katmanı
* Host-to-host katmanı (İletim, transport)
* Uygulama katmanı (Application)

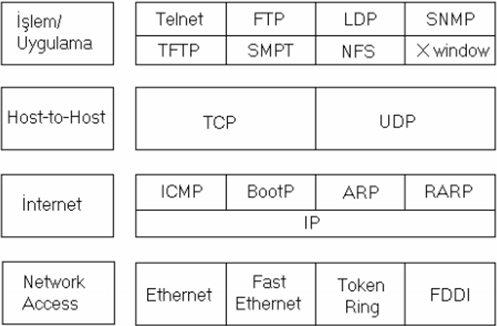
Şekil 2'de OSI modeli ve DOD modeli arasında bir karşılaştırma gösterilmektedir.[[10]](#footnote-11)



Şekil 0OSI Ve TCP/IP Referans Modelleri

Şekilde 2' de görüldüğü gibi OSI referans modelinin ilk iki katmanı olan Veri bağı katmanı ve fiziksel katman birleştirilerek DOD referans modelinin ilk katmanı olan Network access ( Ağ erişim katmanı) oluşturulmuştur. OSI modelinin üçüncü katmanı olan network katmanı, DOD modelinin ikinci katmanı olan internet katmanı haline gelmiştir. OSI modelinin dördüncü katmanı olan ulaşım katmanı, DOD modelinin üçüncü katmanı olan host-to-host (iletim) katmanı olmuştur. OSI referans modelinin son üç katmanı olan oturum, sunum ve uygulama katmanları da DOD modelinin dördüncü katmanı olan uygulama katmanı adı altında birleştirilmiştir.

TCP/IP ve OSI modelinde benzer katmanlar benzer görevleri yerine getirirler. Şekil 3'de TCP/IP referans modeli ve katmanlardaki protokoller gözükmektedir.[[11]](#footnote-12)



Şekil 0 TCP/IP protokolleri

1. 3. 1. TCP/IP Ağ Erişim Katmanı

TCP/IP modelinde ağ erişim katmanı OSI modelindeki fiziksel katman ve veri bağı katmanının birleştirilmesi ile oluşmuştur. Ethernet, Fast Ethernet, FDDI (fiber distributed data interface), ATM (asynchronous transfer mode), Frame Relay, SLIP (serial line internet protocol) ve PPP gibi protokoller bu katmanda çalışmaktadır. [[12]](#footnote-13)

* + 1. TCP/IP İnternet Katmanı

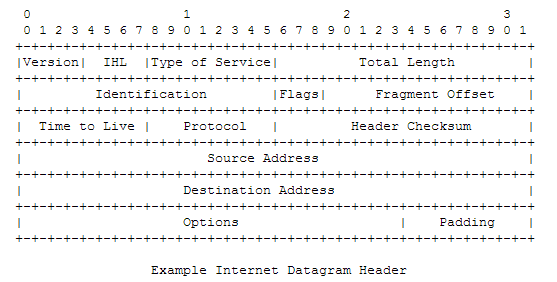
OSI modelindeki ağ katmanının görevleri benzer görevler yürütür. Yönlendirme işlemi bu katmanda yapılır. İnternet katmanındaki protokoller: IP, ICMP, ARP (Adress Resolution Protocol), RARP (Reverse Address Resolution Protocol), Proxy ARP olarak sıralanabilirler.

* + - 1. Internet protocol

Internet protokolü, internet katmanının en önemli bileşenidir. Bir ağdaki cihazın yerini herhangi bir evin adresine benzetilebilir. MAC adresleri evin kapı numarası ise ip adresi sokak ismidir. Ağ erişim katmanında MAC adresi bilgisi ile yalnızca aynı sokaktaki evler bulunabilirken daha geniş bir alanda adres aranıldığında yani yerel ağ dışına çıktığımızda mantıksal olarak cihazlara verilen ip adreslerine ihtiyaç duyulur.

İnternet Protokolü, İletim katmanından gelen segment’leri alarak paketlere böler. Daha sonra IP, alıcı tarafında, paketleri’leri tekrar segment’lere dönüştürür. Her pakete kaynak ve hedef IP adresleri tanımlanır. Bu paketleri alan yönlendiriciler hedef IP adreslerine bakarak yönlendirme kararlarını verir.[[13]](#footnote-14)

Şekil 4' de detayları RFC 791'de tanımlanan bir IP başlığı gösterilmektedir.



Şekil 0 IP Adres Başlığı

Version: İnternet protokolünün versiyonunu bildirir. 4 bitlik bir alandır.

Header length: 32 bitlik başlık uzunluğu alanıdır.

Priority and type of service: Servis kalitesi uygulaması için gereken parametreleri sağlayan 8 bitlik kısımdır.

Total length:Paketin uzunluğudur. Başlık ve verinin kendisi bu uzunluğa dahildir. 16 bitlik alandır.

İdentification:Parçalanma yapılan kısımları birleştirebilmek için gönderici tarafından atanan değer. 16 bitlik bir değerdir.

Flags:Pakette parçalanma olup olmadığını gösteren 3 bitlik kısımdır.

Fragments offset:Bir paket paçalanmışsa, o parçanın nereye ait olduğunu gösteren 13 bitlik alandır.

Time to live:Paketin ağ üzerinde ne kadar dolaşacağını gösteren değerdir. Her yönlendiriciden geçişte bir azaltılır. TTL süresi dolduğunda paket iptal edilir. Bu sayede paketin ağ içeresinde sonsuza kadar dolaşması engellenir. 8 bitlik alandır.

Protocol:Paketin hangi üst katma protokolüne ait olduğunu belirten 8 bitlik alandır.

Header checksum:Paketin başlık kısmının için hata kontrolü yapan 16 bitlik alandır.

Source ip address:Gönderen cihazın IP adresinin bulunduğu 32 bitlik alandır.

Destination ip address: Alıcı cihazın IP adresinin bulunduğu 32 bitlik kısımdır.

Options:istenildiği takdirde hata bulma, güvenlik vb.. gibi amaçlarla kullanılabilir.

Data:İletilen veriyi içerir.[[14]](#footnote-15)

* + - 1. Internet Control Message Protocol

ICMP (Internet Control Message Protocol) mesajları birkaç durumda gönderiler. Örneğin bir paket hedefine ulaşamadığında, ağ geçidi paketi iletebilmek yeterli ara bellek kapasitesine sahip olmadığında yada ağ geçidi trafiği daha kısa bir yoldan yönlendirdiğinde ICMP mesajları oluşur.

İnternet protokolü kesin olarak güvenliği sağlayacak şekilde dizayn edilmemiştir. ICMP mesajları iletişim ortamı sorunları ile ilgili geri bildirim sağlar. ICMP’nin bu şekilde çalışması İnternet protokolünü güvenli hale getirmez. Paketlerin teslim edilip edilmediği ile ilgili bir garanti sunmaz. Bazı paketler kayıplarına dair hiçbir mesaj olmadan teslim edilmeyebilir. Eğer güvenli bir iletişim gerekiyorsa kendi güvenli iletişim prosedürlerine sahip daha üst seviye bir protokol kullanılmalıdır.

Çeşitli ICMP mesajlarından bazıları şunlardır.

* Destination unreachable message (hedefe ulaşılamadı)
* Time exceeded message (zaman aşımı)
* Parameter problem message (parametre problemi)
* Source quench message (kaynak yetersizliği)
* Redirect message (yeniden yönlendirme)
* Echo, echo reply message (yankı, yankı cevabı mesajı)
* Timestamp, timestamp reply (zaman damgası, zaman damgası cevabı)
* Information request, information reply (bilgi isteği, bilgi cevabı)[[15]](#footnote-16)
  + - 1. Adress Resolution Protocol (ARP)

Bir ağ içerisinde kullanılan cihazların iletişime geçebilmeleri için birbirlerinin IP ve MAC adreslerini bilmeleri gerekir. IP adresi cihazlara sonradan atanan 32 bitlik mantıksal bir adrestir. MAC adresi ise üretici tarafından cihazların ağ arayüzüne işlenen 48 bitlik bir adrestir. Bir cihaz IP adresini bildiği bildiği başka bir cihazla iletişime geçmek MAC adresini de öğrenmek zorundadır. Bu işlem ARP sayesinde mümkün olmaktadır.

IP adresi bilinen bir cihazın MAC adresini öğrenmek isteyen cihaz öncelikle ağ üzerinde bir broadcast yayını yapar. Bu yayın ağ içerisindeki tüm cihazlara gönderilir. Yayında ARP isteği vardır. Yani iletişime geçilmek istenen cihazın MAC adresinin ne olduğu sorulur. Yayının ulaştığı cihazlardan sorulan IP’ye sahip olanı, isteği yapan cihaza kendi MAC adresini gönderir. Böylece IP adresinden MAC adresi öğrenilmiş olur.[[16]](#footnote-17)

* + - 1. Reverse Address Resolution Protocol (RARP)

Adress resolution protocol’ün tam tam tersi mantıkla çalışır. MAC adresi bilinen bir cihazın IP adresi öğrenilmek istendiğinde kullanılan protokoldür.

* + 1. TCP/IP İletim Katmanı

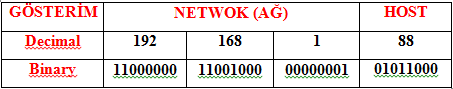
**“**iletim katmanı hedef ve kaynak cihaz arasındaki uçtan uca bağlantıyı sanal bir şekilde sağlamakla yükümlüdür”[[17]](#footnote-18) İletim katmanı protokolleri olan TCP ve UDP bir üst katmandan gelen veriyi alarak segmentlere ayırarak internet katmanına verirler. İletim katmanında sağlanamayan güvenlik bu katmanda sağlanır. TCP kullanan uygulamalarda paketlerin hedefe ulaşıp ulaşmadığı kontrol edilerek eksik paketler varsa tekrar gönderilir. Göndericinin belirlediği sıraya göre alıcı tarafında paketler sıralanarak verinin bütünlüğü korunur. Gönderilen paketlerin iletilip iletilmediğinin kontrol edilmek istenmediği durumlarda UDP kullanılır. IP adreslerine eklenen port numaraları da bu katmanda değerlendirilir.

* + 1. TCP/IP Uygulama Katmanı

Osi referans modelinde bahsedilen oturum, sunum ve uygulama katmanları TCP/IP modelinde birleştirilerek tek bir katman oluşturulmuş ve adına da uygulama katmanı denilmiştir. Bu katmanda kullanılan protokollere örnek olarak Telnet, FTP, TFTP (trivial file transfer protocol), NFS (network file system), SMTP, DNS (domain name system), DHCP (dynamic host configuration protocol) gibi protokoller örnek gösterilebilir.

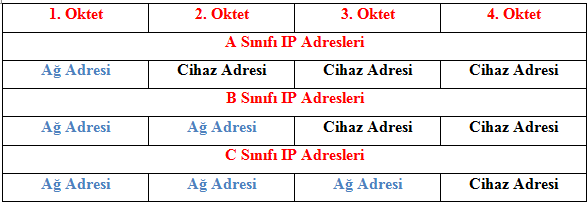
* 1. IPV4 Adresleme, Alt ağlar ve Alt ağ maskesi
  2. 1. IPV4 adres türleri

IPV4 adresleri 32 bitten oluşur. Bu 32 bitlik adres iki bölüme ayrılır. Bunlar Ağ (Network) adresi ve Cihaz (Host) adresidir. Network adresi cihazların bağlı bulunduğu ağı gösterirken Host adresi ise ağda bulunan cihazın numarasını göstermektedir IP adreslerini 2’lik sistemde (binary) göstermek zor olduğundan kullanım kolaylığı açısından 10'luk sistemde (decimal) gösterilirler.Şekil 5'de bir IP adresi gösterimi gösterilmektedir



Şekil 0 IP Adresi Gösterimi

IPV4 adresleri A,B,C,D,E olmak üzere beş sınıfa ayrılmıştır. D sınıfı IP adresleri multicast (çoklu gönderim) için ayrılmışken E sınıfı ise araştırmalar için ayrılmıştır ve ağda kullanılamazlar.[[18]](#footnote-19)



Şekil 0 A,B Ve C Sınıfı IP'ler

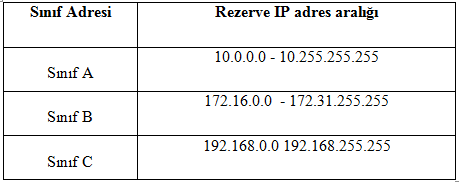
Şekil 6’da görüldüğü gibi birinci oktet (8 bit) ağ adresi geri kalan oktetler cihaz adresi olduğunda A sınıfı, birinci ve ikinci oktetler ağ adresi geri kalan oktetler cihaz adresi olduğunda B sınıfı, ilk üç oktet ağ adresi, son oktet cihaz adresi olduğunda C sınıfı IP adresleri oluşmaktadır. Buna göre:

* A sınıfı IP adresine sahip bir networkte 224-2= 16.777.214 cihaz ip adresi bulunmaktadır.
* B sınıfı IP adresine sahip bir networkte 216-2= 65.534 cihaz ip adresi bulunmaktadır.
* C sınıfı IP adresine sahip bir networkte 28-2=254 cihaz ip adresi bulunmaktadır.

Yukarıdaki hesaplama yapılırken bulunan sonuçlardan iki çıkarılmasının sebebi, IP adreslerinden birinin ağın broadcast IP'si, diğerinin de network IP’si olmasıdır. Belirli aralıktaki IP'ler, IP sınıflarına dahil edilmiştir. Buna göre

* A sınıfı IP adresleri 0.0.0.0'den 127.255.255.255'e kadar olan IP'lerden oluşturulmuştur.
* B sınıfı IP adresleri 128.0.0.0'den 191.255.255.255'e kadar olan IP'lerden oluşturulmuştur.
* C sınıfı IP adresleri 192.0.0.0'den 223.255.255.255'e kadar olan IP'lerden oluşturulmuştur.

Gerektiği durumlarda LAN'da kullanılmak üzere rezerve özel (private) IP'ler de tahsis edilmiştir. Bu IP'ler internete yönlendirilemezler. Sadece iç ağda kullanılabilirler. İnternete yönlendirileceği zamanlarda NAT (network address translation) adı verilen işlemle genel (public) IP'ye çevrilerek gönderilir. NAT işleminin çeşitli faydaları vardır. Networkler kendi içlerinde aynı özel IP blokları kullanmalarına rağmen internete daha az sayıda genel IP ile çıkabilmektedir. Bu işlem sayesinde IPV4 adresleri çok daha önce bitmemiştir. Rezerve özel IP blokları şu şekilde oluşturulmuştur.[[19]](#footnote-20)



Şekil 0 Rezerve IP Adresi Aralıkları

IPv4 adres çeşitlerinden bahsederken yayın türlerini de açıklamak önemlidir. IPv4' de üç çeşit yayın vardır. bu yayınlar:

* Unicast: Tek bir cihaza gönderilir.
* Multicast: Bir cihaz tarafından belirli bir grup cihaza gönderilir.
* Broadcast: Bir cihazdan ağ içerisindeki tüm cihazlara gönderilirler.[[20]](#footnote-21)
  + 1. Alt ağlar ve Alt ağ maskesi

Bir ağ tasarlanırken IP adresleri bazı kurallara göre atanmalıdır. Yönlendirme işleminin verimli olabilmesi için IP adresleme kuralları adresleri alt ağ (subnet) adı verilen gruplara ayırırlar. Bu kurallara göre:

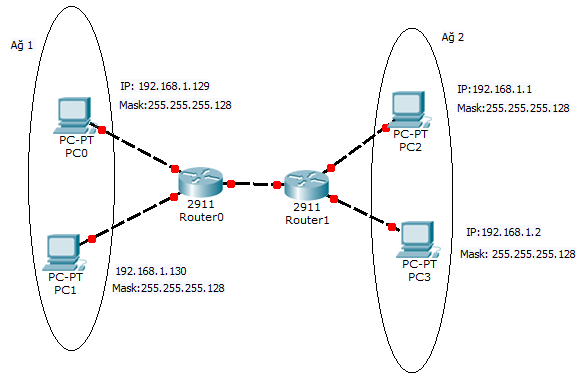
* Bir yönlendirici tarafından ayrılmayan adresler aynı alt ağdadır.
* En az bir yönlendirici tarafından ayrılan adresler farklı alt ağlardadır. [[21]](#footnote-22)

Ağları ayırma işleminin bazı nedenleri vardır. Bunlardan en önemlileri:

* Düşük network trafiği: Ağlar yönlendiricilerle parçalara ayrılmaz ise broadcast trafiği nedeni ile ağlar çalışamaz hale gelir. Bölünmüş bir ağda broadcast trafiği yönlendiriciden geçemeyeceği için yerel ağ içesinde kalır.
* Ağlar küçüldükçe yerel ağ içerisinde oluşan bir problemi bulmak kolaylaşacaktır. Bir ağ ne kadar büyürse sorun giderme o kadar zorlaşır.[[22]](#footnote-23)

1.4.1 bölümünde kullanılabilecek ip adreslerinin A,B ve C sınıfı olmak üzere üç sınıfa ayrıldığından bahsedilmişti. A sınıfı bir ip adresinde 16.777.214 host adresi, B sınıfı bir IP adresinde 65.534 host adresi ve C sınıfı bir IP adresinde 254 bulunmaktadır. Birkaç yüz host bulunacak bir networkte A sınıfı bir IP adresi kullanılacağı zaman milyonlarca IP adresi boşta kalacaktır. Bu da ciddi bir IP adresi israfı anlamına gelmektedir. Bu IP adresi israfını engellemek için Alt ağ maskesi (subnet mask) kavramı ortaya çıkmıştır. Alt ağ maskeleri kullanılarak herhangi bir IP adresini istenildiği kadar alt ağa bölmek mümkündür.

Alt ağ maskesi 32 bitlik bir değerdir. IP adresi ve Alt ağ maskesinin lojik and (ve) işlemi ağ adresini verir. Eğer iki host’un ağ adresi aynı ise aynı alt ağda, farklı ise farklı bir alt ağdadır. Bu durumda iletişim arada bir yönlendirici olması gerekecektir.



Şekil 0 Alt Ağ Örneği

Şekil 8'de alt ağlar ile ilgili bir örnek gözükmektedir. 192.168.1.0 ağ adresi C sınıfıdır. Bu sınıfta 254 host bulunabilir. Fakat şekilde alt ağ maskesi ile bu ağ bölünerek iki farklı ağda kullanılabilmiştir. 192.168.1.129 host’u için:

* 192.168.1.129 ip'si binary: 11000000. 10101000.00000001.10000001
* 255.255.255.128 maskesi binary: 11111111.11111111.11111111.10000000

Bu iki değer and işlemine tabi tutulduğunda:

11000000.10101000.00000001.10000000 sonucu çıkar. Bu sonuçta decimal olarak 192.168.1.128'dir yani network adresi bu host için 192.168.1.128 olur.

192.168.1.1 hostu için:

* 192.168.1.1 ip'si binary: 11000000. 10101000.00000001.00000001
* 255.255.255.128 maskesi binary: 11111111.11111111.11111111.10000000

Bu iki değere and işlemi uygulandığında:

11000000.10101000.00000001.10000000 sonucu çıkar. Bu sonuç ise decimal olarak 192.168.1.0'dır. Yani 192.168.1.1 host’unun network adresi 192.168.1.0 olacaktır. Görüldüğü iki host aynı C sınıfı IP bloğu içerisinde olmalarına rağmen alt ağ maskesi kullanılarak ağ bölünmüş ve host’lar farklı alt ağlarda konumlandırılmıştır.

* 1. Network Address Translation (NAT)

Nat, RFC 3022 dökümanında tanımlanmakta olup, internette yönlendirilebilir genel bir IP adresi olmayan bilgisayarın internet üzerindeki diğer bilgisayarlar ile haberleşmesini sağlamaktadır. Bu durumda iç ağda private IP adresleri veya İnternet üzerinde başka bir kurum adına kayıtlı genel IP adresleri de kullanılabilir.[[23]](#footnote-24)

İnternete yönlendirilebilen IPV4 adresleri sınırsız olmadığı için, yerel ağlarında çok fazla IP adresi atanmış cihaz olan kurumlar için NAT işlemi çok faydalıdır. Bu işlemle iç ağlarında özel bir IP bloğu kullanarak dışarıya istenildiği takdirde daha az sayıda IP adresi ile çıkış yapabilirler. Şekil 9'da NAT yapısı gösterilmektedir.[[24]](#footnote-25) NAT işleminin üç türü vardır. Bunlar:

* Statik NAT
* Dinamik NAT
* PAT (Port address translation, port adresi çevrimi)

olarak sıralanabilirler.



Şekil 0 NAT Gösterimi

BÖLÜM 2

INTERNET PROTOCOL VERSION 6 (IPV6)

1. 1. IPV6 Tarihçesi

IPV4'ün kullanım olarak tüm Dünya'da yaygınlaşmaya başlaması ile birlikte 32 bitlik IP adreslerinin zaman içinde yetersiz kalacağı anlaşıldı. IP adreslerinin yetersiz kalmasında IPv4 adreslerinin belirli bir hiyerarşiye göre dağıtılmaması da etkili olmuştur. Ayrıca hiyerarşik bir yapıya sahip olmayan ve zamanla artan IP adresleri internetin omurga yönlendiricileri üzerinde çok büyük yönlendirme tabloları oluşturmaya başladı. 1990’lı yılların başlarında IP adreslerinin yetersiz kalması sorununu çözmek ve zamanın şartlarına göre ihtiyaçları daha iyi karşılayabilmek için “IETF IPv6 Workgroup” yeni bir yapı geliştirmeye başladı.[[25]](#footnote-26)

IETF tarafından yapılan çalışmalar sonucunda 1995 yılında RFC 1883 ile yeni nesil internet protokolünün özellikleri tanıtılmıştır. Bu yeni nesil protokol 128 bitlik bir adrese sahip olup IP adreslerinin tükenmesi çok zordur. IPV4 protokolünden sonra gelen protokolün IPV6 olarak adlandırılmasının sebebi RFC 1190 olarak yayınlanan "Experimental Internet Stream Protocol, Version 2" adlı çalışmanın daha önceden IPV5 olarak adlandırılmış olmasıdır. Bu çalışma deneysel bir çalışma olmasına rağmen karışıklığa sebebiyet vermemesi için geliştirilen yeni protokol IPV6 olarak isimlendirilmiştir.

IPV6 ile birlikte sadece adres sayısı değil IPV4' ün bazı özellikleri geliştirilmiş ve eksiklikleri giderilmiştir. Güvenlik, servis kalitesi (quality of service, QoS), mobilite gibi hizmetler geliştirilmiştir. Otomatik yapılandırma ve IPV4 adres başlığı optimizasyonu gibi yeni özellikler eklenmiştir.

Günümüzde IPV6'nın kullanım oranı artmaya başlanmıştır. Özellikle internetteki kullanıcılara hizmet sağlayan kamu ve özel sektör kuruluşlarının internete IPV6 ile bağlanan kullanıcılar ortaya çıkmaya başladığında, bu kullanıcılara da hizmet vermek için alt yapılarını IPV6 hazır hale getirmeleri gerekmektedir. Zaruri olarak aniden geçmek yerine geçiş çalışmalarına başlamak ve hazırlıklı olmak için tüm Dünya'da ve ülkemizde geçiş ile ilgili çeşitli çalışmalar yapılmaktadır. Donanım ve yazılım olarak artık bir çok ürün de IPV6 desteği sunmaktadır.

* 1. Yeni Nesil IP (IPV6) Gereksinimi

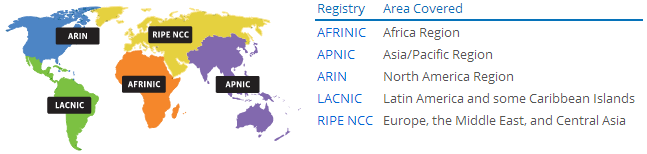
İnternetin kullanımının yaygınlaşması ile birlikte mevcut IPv4 adresleri sayısı yetersi kalmaya başlamıştır. Günümüzde Dünya nüfusu 7 milyarı geçmiş İnternet kullanıcıları sayısı ise 2,5 milyara yaklaşmıştır.[[26]](#footnote-27) Tüm Dünya’da internet kullanımı bu kadar hızlı artışı aşağıdaki sebeplerle açıklanabilir.

* Mobil şebekelerin yaygınlaşması
* Yüksek hızlı erişim
* İnternet bağlantılı elektronik ve haberleşme cihazları
* Ev otomasyon uygulamaları ve algılama şebekeleri[[27]](#footnote-28)

32 bitlik IPv4 adres havuzu yaklaşık olarak 4 milyar IP adresi içerir. IP adresleri azalmasına çözüm olarak zaman içersinde CIDR (classless inter domain routing) ve NAT gibi çözümler ortaya çıkmış ama nihai olarak yeni bir internet protokolü kaçınılmaz hale gelmiştir.[[28]](#footnote-29)

Adres sayısının yetersiz kalması dışında yeni bir IP versiyonunun geliştirilme sebepleri olarak performans yönetimi, güvenlik ve otomatik adres atama konuları gösterilebilir. Performans yönetimi konusu IP adreslerindeki hiyerarşik seviye eksiliğinden dolayı yönlendiricilerin yönlendirme tablosu üzerinde yönetimi zor olan çok fazla yönlendirme bilgisi olmasını ifade eder. İnternet kullanımın son yıllarda artışı, finans sektörü gibi alanlarda kullanılması ise güvenliğin IP protokolü tarafından desteklenmesini gerektirmiştir. Ayrıca IPv4'de ip ataması karmaşık ve insanlar tarafından ayarlanması gereken bir süreçtir. Ama kullanıcılar genel olarak tak ve kullan cihazları tercih ederler. Bu gibi nedenler de yeni bir IP protokolü geliştirilmesini gerekli kılmıştır.[[29]](#footnote-30)

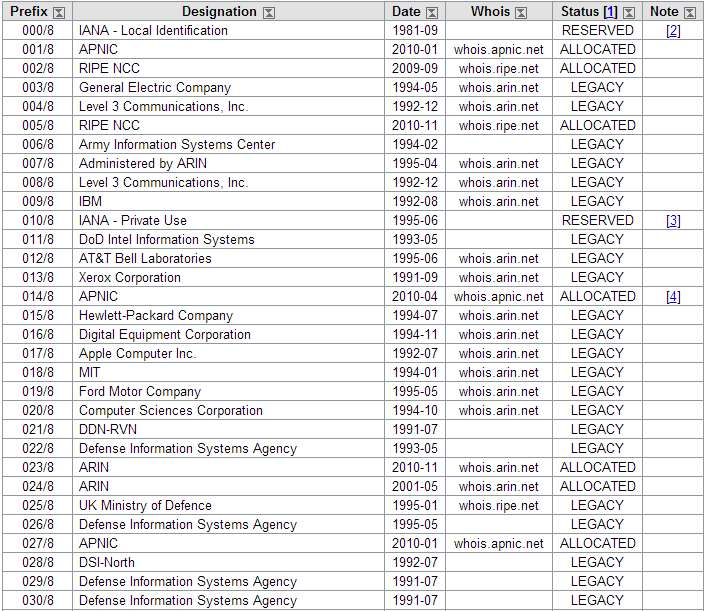
IP adreslerinin koordinasyonundan, IANA (Internet Assigned Numbers Authority) adlı kuruluş sorumludur. Servis sağlayıcıları IP adreslerini IANA altındaki  Regional Internet Registry (Bölgesel İnternet Kayıt Kuruluşu, RIR) adındaki bölgesel internet kayıt kuruluşlardan alırlar. Şekil 10'da bölgesel internet kayıt kuruluşları gözükmektedir.[[30]](#footnote-31)



Şekil 0 Bölgesel İnternet Kayıt Kuruluşları

Türkiye'nin de içinde bulunduğu Avrupa, Ortadoğu ve Asya'nın bir kısmına IP adresleri dağıtımından RIPE NCC adlı kuruluş sorumludur.

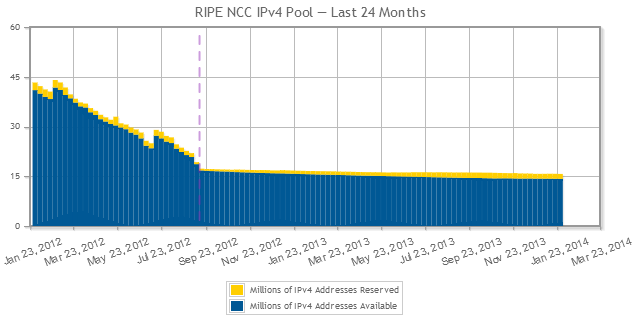
IP adreslerinin tükenmesinin en önemli nedenlerinden birisi IP'lerin kullanımdan dolayı azalması değildir. IP adreslerinin verimli tahsis edilmemesi de adres uzayının tükenmesini hızlandıran nedenlerdendir.[[31]](#footnote-32) Şekil 11'de /8 IP bloklarının bazılarının dağıtımı gözükmektedir. Şekil 11'de görüldüğü gibi bazı şirketlere /8 IP bloklarından tahsis edilmiştir.[[32]](#footnote-33) Bu bloklar tüm IP adreslerinin 256'da 1'idir.



Şekil 0Dağıtılan IP Bloklarının Bir Kısmı

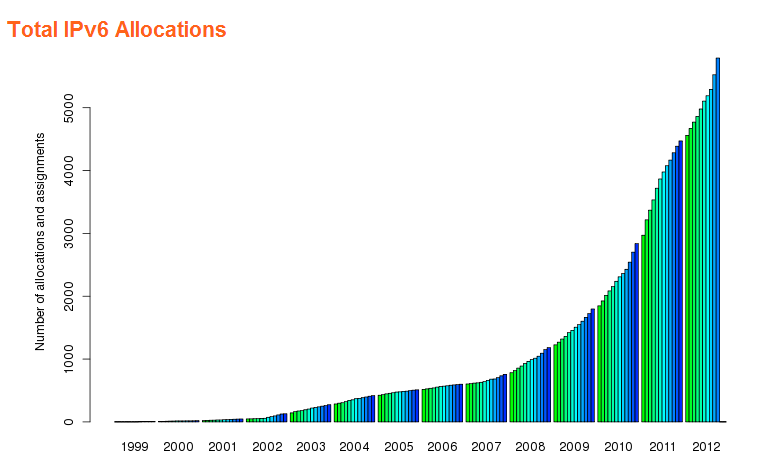
Eylül 2012'de Avrupa, Ortadoğu ve Asya'nın bir kısmına IP dağıtan RIPE NCC son /8 bloğunun ayrıldığını belirtti. Bu dağıtımında Local Internet Registries (LIRs) kuruluşlarına bazı kurallara göre olacağı açıklandı. Buna göre bir LIR sadece /22 (1024 IP) bloğu olarak IP adresi alabilir. Bu dağıtımda daha önceden IPV6 adresi almışlarsa yapılacaktır.[[33]](#footnote-34)

Şekil 12'de görüldüğü gibi RIPE NCC artık IP dağıtımını oldukça sınırlandırmıştır.[[34]](#footnote-35)



Şekil 0 RIPE NCC IPv4 Havuzu

IPV4 adresleri dağıtımdaki bu azalmaya rağmen IPV6 adresi tahsis edilen LIR (Local Internet Registry, Yerel İnternet Kayıt Kuruluşları) sayısı hızla artmaktadır. Şekil 13'de RIPE NCC verilerine göre IPV6 adresi tahsis eden yerel internet kayıt kuruluşları sayısındaki artış gözükmektedir.[[35]](#footnote-36) Görüldüğü gibi son birkaç yılda IPV6 adresi tahsis eden yerel internet kayıt kuruluşu sayısı hızla artmıştır.



Şekil 0IPv6 Adresi Tahsis Eden LIR Sayısının Zamanla Değişimi

Ayrıca IPV4 ticari olmayan kullanım için tasarlanmış olup günümüzde beklenilen servis kalitesi işlemini, modern ticari hayat için temel olan çoklu yayın fonksiyonlarını veya güvenlik için gerekli yapılanmayı sağlamak amacı ile tasarlanmıştır.[[36]](#footnote-37)  Genişletilmiş IP adres havuzuna ek olarak IPV6 ile güvenlik, servis kalitesi (Qos , quality of service) desteği, mobility desteği gibi özellikleri geliştirilmiş ve çeşitli optimizasyonlar yapılarak IPV4'ün gereksiz özellikleri çıkarılmıştır.[[37]](#footnote-38)

Ülkemizde de bu konu ile ilgili, başbakanlık tarafından Kamu Kurum ve Kuruluşları için IPv6’ya Geçiş Planı adlı genelge çıkarılmıştır. Bu genelge ile:

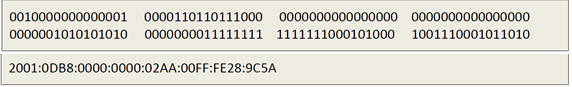
* IPv4 adresleri tükendiğinde ortaya çıkacak yalın IPv6 kullanan kullanıcıların da kamu kurum ve kuruluşlarının internet üzerinden sunduğu hizmetlerden faydalanabilmeleri,
* IPv6 ile birlikte gelen güvenlik, servis kalitesi, verimlilik gibi yeniliklerden kamu kurum kuruluşlarının sunduğu hizmetlerde faydalanması,
* Bilişim sektöründe araştırma ve geliştirme faaliyetlerinde bulunan kurum ve kuruluşların IPv6’ya geçişinin teşvik edilerek bu alanda da ülkemizin teknoloji üreten bir ülke konumuna gelmesi[[38]](#footnote-39)

amaçları ile kamu kurumlarının internet üzerinden verdiği hizmetleri genelgede belirtilen aşama ve zaman planı doğrultusunda IPV6'ya geçirmeleri gerekmektedir.

* 1. IPV6 Adres Yapısı

IPV4 adresleri 8 bitlik 4 kısımdan oluşan toplam 32 bir adres olarak düşünülmüştür. Gösterim olarak ise onluk sistem tercih edilmiştir. 192.168.1.1 gibi ip adresi şeklinde gösterilir. IPV6 adreslerinde ise 128 bitlik adresler kullanılmaktadır. IPv4 adres havuzunda 232 adet IP adresi vardı. IPV6 adreslerinde ise bu sayı 2128 adete çıkmıştır. “Bu sayı ise yaklaşık olarak 1038'e tam olarak da 340.282.366.920.938.463.463.374.607.431.768.211.456' a denk gelmektedir.”[[39]](#footnote-40)

Gösterim olarak da IPV6 adresleri 16 bitlik sekiz kısma ayrılmış. Bu kısımlar da onluk sistem yerine onaltılık sistemde gösterilmeye başlanmıştır. Şekil 14'te IPV6 adres yapısı gösterilmektedir.[[40]](#footnote-41)



Şekil 0 IPv6 Adresi Gösterimi

Şekil 14'de gözüktüğü gibi IPV6 adresleri 16 bitlik sekiz kısma ayrıldıktan sonra 16'lık sistemde yazılmıştır, IPV4 adreslerinden farklı olarak nokta ile değil de iki nokta ile ayrılmaya başlanmıştır.

IPv6 adresleri IPV4 adreslerine göre oldukça uzun oldukları için gösterim sırasında kolaylık olması açısından çeşitli kısaltmalar yapılabilirler. Örnek olarak şekil 17'deki IPV6 adresini ele alınırsa:

2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A

IPV6 adresleri gösteriminde 16 bitlik kısımların solundaki 0'lar atılabilir. Bu sıfırlar atıldıktan sonra aşağıdaki şekle gelecektir.

2001:DB8:0000:0000:2AA:FF:FE28:9C5A

Ayrıca tamamı 0000 olan bir blok yada yan yana olan birden fazla blok atılabilir. burada dikkat edilmesi gereken nokta bu işlemin sadece bir kez yapılabilmesidir. Eğer adresin içinde yan yana olmayan başka bir kısımda 0000 şeklinde ise, atılma işlemi daha önceden yapıldığı için yapılamaz. 0000 olan bloklar atıldıktan sonra fazladan ":" işareti araya koyulur. Ve IP adresi aşağıdaki hale gelir.

2001:DB8::02AA:00FF:FE28:9C5A

Bu şekilde kısaltmalarla adreslerin yazımı biraz daha kolay hale gelebilir.

* 1. IPV6 Adres Öneki (Prefix)

**“**IPv6 adreslerinde IPv4 adreslerinde olan A,B,C gibi sınıflar bulunmamaktadır.”[[41]](#footnote-42)Bunların yerine IPv4 adreslerinde olan CIDR gösterimi IPv6 adreslerinde de bulunmaktadır.

2001:067c:1558:0000:0000:0000:0000:0000 /48 ip bloğunu ele alalım.

/48 önekini alan bu ip adresinde ilk 48 bitlik kısım (altı çizili kısım) network adresini belirtir. Kalan kısım ise host adresleridir. Kısaltma kurallarına göre bu ip bloğunu tekrar yazarsak

2001:67c:1558:: /48 şeklinde network adresini göstermiş oluruz.

Bu ip bloğunun ilk IP'si için bir host adresi tanımlayacak olursak:

2001:67c:1558::1/48 şeklinde gösterebiliriz. bu gösterimle host IP'si ve o host’un hangi ağa ait olduğu açıkça belli olmaktadır.

IPv4'te kullanılan bazı özel IP adreslerinin IPv6'da gösterimi şu şekildedir:

0::0 adresi IPV4'teki 0.0.0.0 adresine eşittir.

0::1 adresi IPV4'teki 127.0.0.1 (loopback ip adresi) adresine eşittir.

* 1. IPV6 Adres Türleri

IPV6' da üç temel adres türü vardır. Bunlar:

* Unicast
* Anycast
* Muticast adresleridir.[[42]](#footnote-43)

IPV6 adreslerinde IPV4 adreslerinden farklı olarak broadcast adresleri bulunmamaktadır. Ayrıca IPV4 adreslerinden farklı bir yön olarak IPV6 adreslerinde anycast adı verilen yeni bir adres türü ortaya çıkmıştır.

Unicast adresleri tek ağ arayüzünü tanımlar. Paketler doğrudan tekil hedef IP adresine gönderilir. Anycast IP’leri bir grup içerisindeki bir adet arayüzünü ifade eder. Gönderilen paketler grup içerisinde bir cihaza iletilir. Bu yapılarından dolayı anycast adresleri yük dağıtımı (load balancing) uygulamalarında kullanılabilirler. Multicast adresleri ise yine farklı arayüzlerden oluşan bir grubu tanımlar. Multicast bir hedef IP’sine sahip paketler grup içerisindeki tüm cihazlara gönderilirler.[[43]](#footnote-44)

* 1. Unicast IPV6 Adres Türleri

1. 6. 1. Global Unicast Adresler (Küresel tekil gönderim adresleri)

IPV4 genel unicast adresleri gibi yönlendirilebilir adreslerdir. Bu adresler IANA tarafından RIPE NCC gibi bölgesel ip adresi dağıtıcılarına tahsis edilir. Bölgesel ip dağıtan kurumlardan da servis sağlayıcılarına tahsis edilir. 2000::/3 öneki ile başlayan adreslerdir.

* + 1. Link-local adresler (Bağlantı yerel tekil gönderim adresleri)

Bağlantı yerel tekil gönderim adresleri “1111111010” bit dizisi ile başlayan 10 bitlik adreslerdir. Bu diziden sonra 64. bite kadar “0” sayısı gelir, sonra da arayüz tanımlayıcısı gelmektedir. Bu sebeple bu tip adresler FE80::/64 öneki ile başlar.[[44]](#footnote-45)

Link-local adresleri dış dünyaya yönlendirilemezler. “Bağlatı yerel tekil gönderim adresleri sadece bir arayüz bağlantısı üzerinde otomatik adres yapılandırılması veya komşu keşfi gibi amaçlar ile kullanılan yerel adreslerdir.”[[45]](#footnote-46)

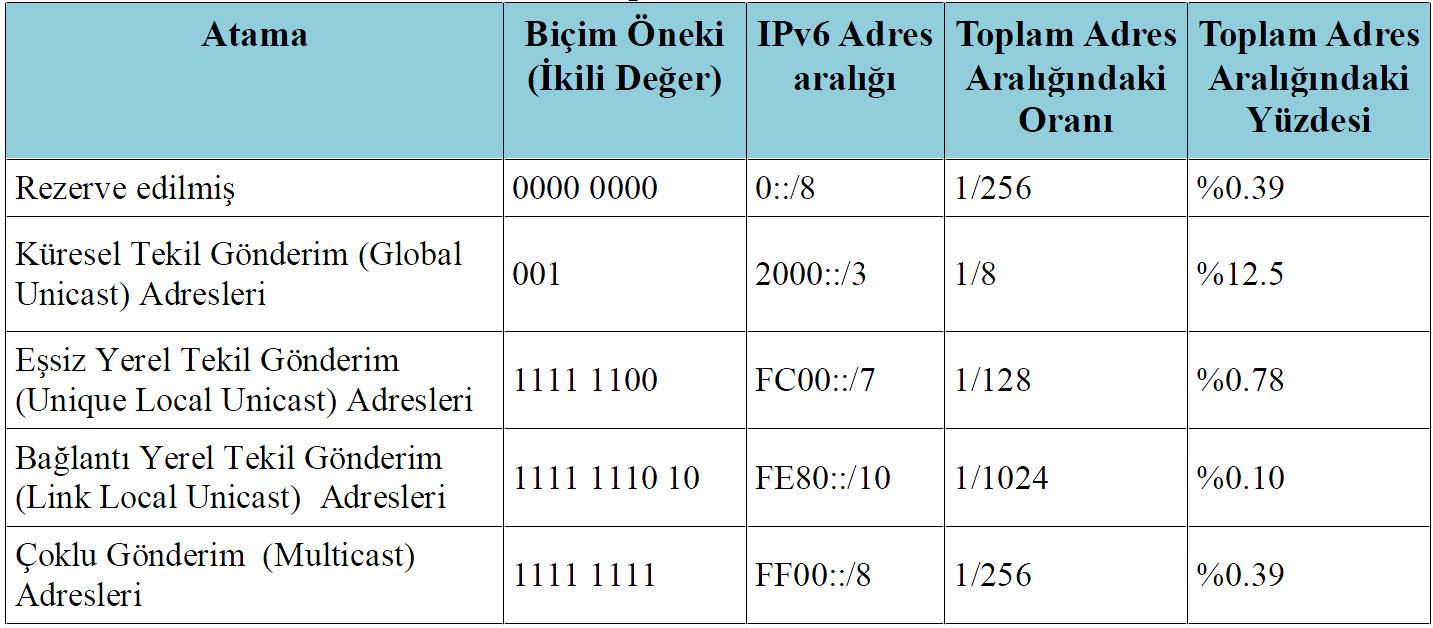
* + 1. Unique local adresler (Eşsiz tekil gönderim adresleri)

Yerel ağ trafiği için geliştirilmiş adresler olup dış dünyaya yönlendirilemezler. IPv4’de kullanılan özel IP bloklarına benzerler. Özel ağlarda kullanılabileni, rezerve edilmiş, FC00::/7 önekini kullanan adreslerdir.[[46]](#footnote-47)

* + 1. Multicast (Çoklu Gönderim Adresleri)

Multicast adresleri belirli bir adres grubunu belirten IP adresleridir. Bu IP adresine gelen istekler o multicast grubu içerisindeki tüm cihazlara gönderilirler. FF00/8 önekine sahiptirler.

Şekil 15'de IPV6 adres türleri görünmektedir.[[47]](#footnote-48)



Şekil 0 IPv6 Adres Türleri

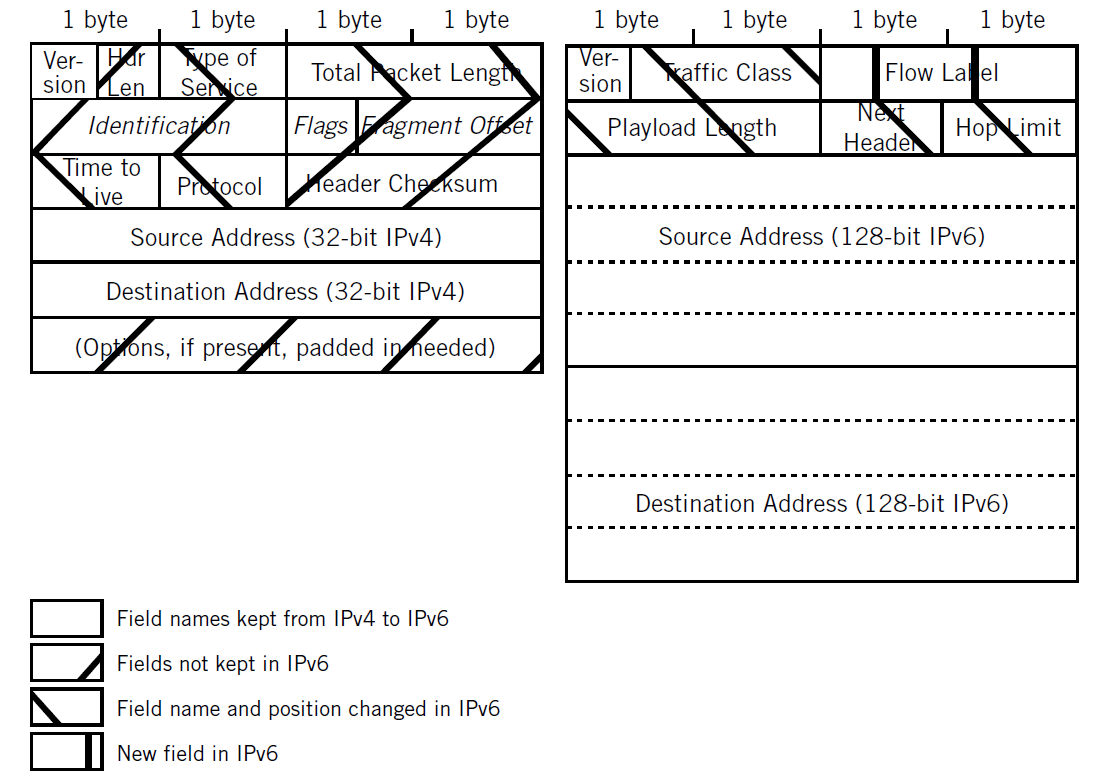
* 1. IPV6 Başlık Yapısı

Şekil 16'da görüldüğü gibi IPV6 adres başlığında IPV4'e göre bazı değişiklikler yapılmıştır. Bölüm 1.3.2.1'de detayları açıklanan header lenght, identification, flags, fragment offset, header checksum bölümleri IPV6 başlığından çıkarılmıştır. Type of service, total packet lenght, time to live ve protocol alanları ise isimleri ve bazı özellikleri değiştirilerek IPV6 başlığına aktarılmıştır. Ayrıca flow label adında yeni bir kısım oluşturulmuştur.[[48]](#footnote-49)

IPV6'da IPV4'den farklı olarak istenildiği takdirde IPV6 başlığına ilave edilebilen eklenti başlıkları bulunmaktadır. IPV4 adres başlığı yapısında "options" kısmında IPV4 adresi ile ilgili seçenekler bulunur. Bu alan kullanılmasa bile yönlendiriciler tarafından her pakette incelenir. IPV6'da bu alan kaldırılarak eklenti başlıkları bölümü getirilmiştir. Eklenti başlıkları kullanıldığı takdirde IPV6 başlığına kullanılan kısımları ilave edilir. Eğer kullanılmazsa bu alan eklenilmez. Bu da yönlendiricilerin iş yükünü azaltan bir özelliktir.[[49]](#footnote-50) IPV6 eklenti başlıkları RFC 2460'da açıklanmıştır.

IPV6 eklenti başlıkları sırası ile şunlardır:

* Hop-by-Hop options header (Atlama noktası seçenekleri başlığı)
* Destination options header (Hedef seçenekleri başlığı)
* Routing header (yönlendirme başlığı)
* Fragment header (Parçalara ayırma başlığı)
* Authentication header (Kimlik doğrulama başlığı)
* Encapsulation security payload header (Güvenlik başlığı)



Şekil 0 IPv4 Ve IPv6 Adres Başlıkları

Bir IPV6 başlığında sırası ile aşağıdaki alanlar bulunur:

Version**:** IPV4'de bulunan “version” alanıyla aynı şekildedir. IPV6 için bu değer 6'dır.

Traffic class**:** IPV4'de bulunan “type of service” kısmı yerine getirilmiştir. 8 bitlik bir alandır.

Flow label: IPv6’da yeni IPv6 da isteğe bağlı olarak kullanılabilen bu bölümdeki etiketlere bakılarak gerçek zamanlı verilerin hızlı bir şekilde yönlendirilmesi ya da MPLS (Multi Protocol Label Switching) gibi alt katmandaki teknolojilerin verimli kullanılması mümkün olmaktadır.[[50]](#footnote-51)

Payload length: IPV4'deki total “packet length” alanına karşılık gelmektedir.

Next Header: IPV4'deki “protocol” alanına karşılık gelmektedir.

Hop limit: IPV4'deki “time to live” kısmına karşılık gelmektedir.

Source Address: 128 bitlik kaynak ip adresi kısmıdır.

Destination Address: 128 bitlik hedef ip adresi kısmıdır.

* 1. IPV6 İle Gelen Yenilikler:
  3. 1. Adres uzayının genişlemesi:

Bölüm 2.2' de de bahsedildiği gibi IPV6 adresleri 128 bir adres olarak 32 bitlik IPV4 adreslerine göre çok daha fazla adres sayısı içermektedir.

* + 1. Geliştirilmiş Güvenlik:

IPV6 özellikleri IPV6 düğümleri için IPsec (internet protocol security) kullanımını zorunlu tutar. Bu nedenle IPV6 IPV4'e göre daha güvenlidir. Ayrıca IPV6 iletişim kaynağı kimlik doğrulaması ve payload encryption gibi güvenlik özelliklerini içerir.[[51]](#footnote-52) Bu özellikler IPV6 başlığındaki eklenti başlıkları kısmı ile yapılandırılır.

* + 1. Geliştirilmiş Servis Kalitesi (QOS)

Belirli trafiğe ait paketleri etiketleyerek gönderenden gelen paketlere özel işlem yapabilme olanağı verir. Gerçek zamanlı trafik gibi bir trafik diğer trafiklerden daha farklı bir işlem görebilir. internet üzerinden yapılan telefon görüşmelerinin kopuk kopuk olması yerine daha düzgün ve pürüzsüz olması bu özelliğe örnek olarak verilebilir.[[52]](#footnote-53)

* + 1. Multicast Dinleyici Keşfi (Multicast Listener Discovery, MLD)

IPV6'da adres aralığının geniş olması çoklu gönderim (multicast) adres aralığının da genişlemesi anlamına gelmektedir. Bu özellik IPv4'de karşılaşılan aynı IP adreslerini farklı multicast gruplarının kullanması sorununu ortadan kaldıracaktır. IPv6 adresinde bulunan bazı yeni bilgiler sayesinde multicast yayınlarının gönderileceği ağların sınırlandırması yapılabilmektedir. IPv4'te ağ cihazlarının hangi multicast grubuna üye oldukları bilgisini paylaştığı protokol IGMP (internet group management protocol) protokolüdür. IPv6’da ise bu işlem için kullanılan protokoller MLD1 ve MLD2 protokolleridir. MLD1 protokolü IGMPv2 protokolünden türetilirken MLD2 protokolü ise ICMPv3 özelliklerini göstermektedir.[[53]](#footnote-54)

* + 1. Internet Control Message Protocol Version 6 (ICMPv6)

IPV4'de olduğu gibi IPV6'da kontrol için ICMP protokolü kullanılır. icmpv6 İPV4'de kullanılan ICMP protokolünün IPV6'ya uyarlamış halidir. ICMPv6 birçok amaca yönelik kullanılan bir protokoldür. ICMPv6, iletişim sırasında oluşan hataları bildirir. Yankı isteği ve yankı cevabı paketleri ile iletişimi kontrol edebilmeyi sağlar. Ayrıca multicast dinleyici keşfi, komşu keşfi gibi özelliklerde ICMPv6 ile çalmaktadır. ICMPv6 mesajları hata ve bilgi mesajları olarak ikiye ayrılmıştır.[[54]](#footnote-55) IcmpV6 konusu RFC 4443'de detaylı olarak açıklanmıştır.

IcmpV6'da kullanılan hata mesajları hedef ulaşılamaz, paket çok büyük, zaman aşımı ve parametre problemi mesajlarını içerir. Bilgi mesajlarına örnek olarak ise yankı isteği ve yankı cevabı örnek olarak verilebilir.[[55]](#footnote-56)

* + 1. Komşu Keşfi (Neighbor Discovery)

**“**IPv4’de kullanılan yönlendirici keşfi (router discovery-RDISC), adres çözümleme protokolü (address resolution protocol-ARP) ve ICMP yeniden yönlendirme bileşenlerinin görevleri IPv6’da komşu keşfi tarafından yapılmaktadır.”[[56]](#footnote-57)

Komşu keşfi işlemlerine örnek olarak yönlendirici keşfi, önek keşfi, Parametre keşfi, otomatik adres yapılandırması, adres çözümlemesi (IPV4 ARP işlemi yerine), next-hop kararı, Komşu ulaşılamaz keşfi, çakışan adres keşfi gibi işlemler gösterilebilir.[[57]](#footnote-58) Komşu keşfi detayları RFC 4861'de açıklanmıştır.

* + 1. IPV6 Yönlendirme Protokolleri

IPV6 yönlendirme protokolleri temel olarak IPV4'deki yönlendirme protokollerine benzer şekilde çalışırlar. Statik yönlendirme IPV4'dekine benzer şekilde yapılır. IPV4'den farklı olarak istemcilere varsayılan ağ geçidi (default gateway) atama zorunluluğu yoktur. İstemciler komşu keşfi mesajları ile varsayılan ağ geçitlerini bulabilirler. Dinamik yönlendirme protokolleri olarak ise RIPNG (routing information protocol next generation), OSPFv3 (open shortest path version 3), EIGRP (enhanced interior gateway routing protocol) for IPv6, BGP4+ (border gateway protocol 4+) gibi protokoller örnek gösterilebilir.

* + 1. Otomatik Yapılandırma (Autoconfiguration)

IPV6 ağa bağlanan network ekipmanlarının bağlantısını kolaylaştıran tak ve çalıştır mekanizmasını içerir. Gerekli konfigürasyon otomatik olarak yapılır. Bu özellik durum denetimsiz otomatik yapılandırma (stateless autoconfiguration) olarak adlandırılır. Büyük hacimdeki IPV6 ağlarında bu işlem ağa bağlanma hızını arttırır. Ağ yöneticileri ağdaki tüm cihazlara IP atamak zorunda kalmazlar. Durum denetimli (Statefull) mekanizmasında ise ağda bulunan bir DHCP (Dynamic host configuration server) ağda bulunan cihazlara IP adreslerini dağıtır. Bu durumda yönlendiriciden herhangi bir prefix bilgisine ihtiyaç duyulmaz.[[58]](#footnote-59)

Durum denetimsiz otomatik yapılandırma işleminde yönlendiriciden önek bilgisini alan cihaz IP adresinin 64 bitlik kısmını bu bilgi ile oluşturur. Geri kalan 64 bitlik kısmını ise MAC adresinden türetir. 48 bitlik MAC adresinden türetme işlemi araya FFFF kısmı eklenerek şu şekilde yapılır:

0060.d673.1987 MAC adresine sahip bir arayüz için araya FFFF kısmını eklersek 0060:D6FF:FE73:1987 şekline dönüşür. Ayrıca MAC adresinin 7. biti kontrol amacıyla değiştirilir. Bu işlemden sonra adres 0260:D6FF:FE73:1987 haline gelir. yönlendiriciden öğrendiği 64 bitlik prefix bilgisini de başına yerleştirdikten sonra IPV6 adresini oluşturmuş olur. Bu 64 bitlik kısım EUI-64 arayüz tanımlayıcısı (EUI-64 interface identifier) olarak adlandırılır.

* + 1. DHCPv6

IPV6 için DHCP protokolü DHCPV6 olarak isimlendirilmiştir. Detayları RFC 3315'de açıklanmıştır. IPV6 protokolünde otomatik yapılandırma özelliği olmasına rağmen bazı sebeplerden dolayı DHCP kullanılması gerekebilir.

* Ağ içerisinde kullanılan adreslerin yönetilmesi, izlenilmesi gibi işlemlerin yapılması gerektiğinde,
* DNS gibi bazı bilgilerin istemciye gönderilmesi gerektiği durumlarda,[[59]](#footnote-60)

IPv6 otomatik yapılandırma özellikleri tek başına yeterli olmayacağı için DHCPv6 kullanılması gerekecektir.

IPv4’ten farklı olarak durum denetimli bir ağda çalışan DHCPv6, istemcilere varsayılan ağ geçidi bilgisi göndermez. İstemciler yönlendirici ilanı gönderen cihazın IP adresini varsayılan ağ geçitleri olarak kabul ederler.

“DNS sunucusu yapılandırılırken IPv4 yapılandırmasından farklı olarak, alan adları çözülürken IPv4 için kullanılan A kaydı yerine IPv6 için AAAA kaydı girilmesi, ters çözümlemelerde IPv4 için kullanılan .in-addr.arpa uzantısı yerine .ip6.arpa uzantısı kullanılması gerekmektedir.”[[60]](#footnote-61)

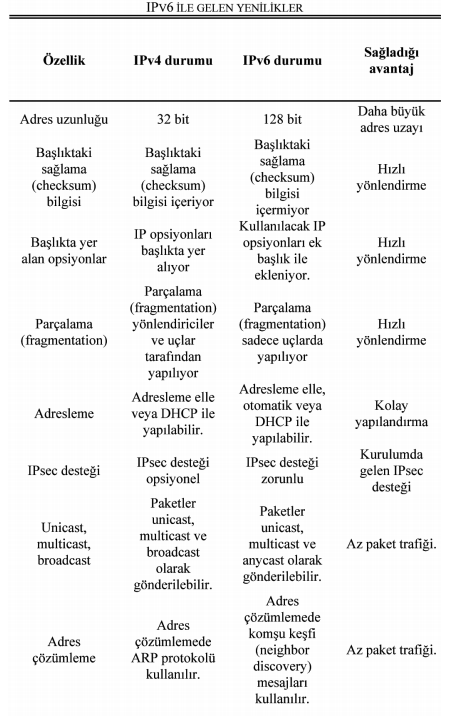
* + 1. Dolaşılabilirlik (Mobility)

IPV6 ile birlikte gelen;

* Genişletilmiş adres uzayı,
* Otomatik yapılandırma,
* IPv6 yapısı içerisinde bulunan şifreleme ve kimlik denetimi uygulamaları,
* Servis kalitesindeki gelişim,
* Geliştirmelere uyumlu esnek yapısı,

gibi IPv4’e göre daha gelişmiş özelliklerden dolayı IPV6 ile birlikte dolaşılabilirlik yeteneği artmıştır[[61]](#footnote-62) . RCF 3775'te IPV6'nın mobility desteği detaylı olarak açıklanmıştır.

Şekil 17'de IPV6 ile IPV4 karşılaştırılması tablo olarak gösterilmektedir.[[62]](#footnote-63)



Şekil 0 IPv6 İle Birlikte Gelen Yenilikler

* 1. IPV6 Geçişi

IPV6' nın getirdiği yenilikler ve IPV4'ün adres havuzunun tükenmesinden dolayı IPV6 geçişin zaruri hale gelmeye başladığı ikinci bölümde açıklandı. Bu konuda ulusal ve uluslararası kuruluşların çeşitli çalışmaları bulunmaktadır. 17-18 Haziran 2008’de Seul’da OECD (organisation for economic co-operation and development) tarafından yayınlanan “İnternet Ekonomisinin Geleceği için Seul Deklarasyonu” ile büyük özel gibi şirketler gibi kamu kurumları tarafından da IPV6 protokolüne geçişin teşvik edileceği deklare edilmiştir.[[63]](#footnote-64)  Ülkemizde de bu konu ile ilgili çeşitli çalışmalar yapılmıştır. Bu konu ile ilgili TÜBİTAK Kamu Kurumları Araştırma ve Geliştirme Projelerini Destekleme Programı çerçevesinde kabul edilen "Kamu Kurum ve Kuruluşları için IPv6’ya Geçiş Planı" hazırlanmıştır. Bu planın detaylarına www.ipv6.net.tr adresinden ulaşılmaktadır. Ayrıca başbakanlık tarafından "Kamu Kurum ve Kuruluşları için IPV6'ya geçiş planı” konulu genelge yayınlanmıştır. Hazırlanan plan ve yayınlanan genelgede kamu kurumlarının internet üzerinden verdiği hizmetlerin IPv6’ya geçirilmesi konusuna yoğunlaşılmış kurum içinde kullanılan diğer yapılar ilk aşamada göz ardı edilmiştir.

Hazırlanan Kamu Kurum ve Kuruluşları için IPv6’ya Geçiş Planı'na göre çeşitli aşamalarla bu geçişin yapılması gerektiği belirtilmiştir. Bu aşamalara öncelikle kurumda bilgi işlem yöneticisi olarak çalışan personelin gerekli eğitimleri alarak yeterli bilgi birikimini edinmesi gerekmektedir. Daha sonra kurumda kullanılan üçüncü seviye anahtarlama cihazları, güvenlik duvarları, yönlendiriciler ve kurumların dışarıya hizmet verdiği yazılımların envanteri çıkarılarak bu kalemlerde IPV6 desteği olup olmadığı belirlenecektir. IPV6 desteği olmayan cihaz ve yazılımların son kullanım ömürleri de dikkate alınarak yenilme çalışmaları yapılacaktır. Alt yapıda kullanılan bu cihaz ve IPV6 desteğini sağlar hale geldikten sonra ise kurumda en az bir pilot uygulama IPV6 destekler hale getirilecektir. Çeşitli testler yapıldıktan sonra dışarıya hizmet veren tüm uygulamalar için IPV6 desteği sağlanacaktır.[[64]](#footnote-65)

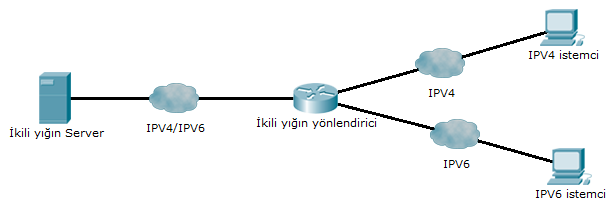
“IPv4’ten IPv6’ya geçiş sürecinde, internetin dünya çapında yaygınlığı, geçiş sürecinin tüm dünyada homojen olmaması ve mevcut sistemlerin ekonomik ömürlerini tamamlamadan değiştirilmek istenmemesi gibi gerekçeler İPv4 ve İPv6 sistemlerin bir süre beraber çalışmasını gerektirmektedir.”[[65]](#footnote-66) IPV6'ya geçişte tüm network mimarisi dikkate alınarak geçişin nasıl yapılacağı planlanmalıdır. Geçiş süresince IPV4 ve IPV6 protokolleri bir süre bir arada kullanılacaktır. Bu sürecin problemsiz olması için IETF tarafından çeşitli geçiş yöntemleri önerilmiştir. Bu yöntemler ikili yığın (dual stack), çeviri (tunneling) ve çeviri (translation) yöntemleridir.[[66]](#footnote-67)

* 1. 1. İkili Yığın (Dual Stack) Yöntemi:

İkili yığın yöntemi RFC 2893' de tanımlanmıştır. Bu yöntemde bir network düğümünde IPV4 ve IPV6 yığınları paralel olarak çalışır. IPV6 uygulamaları IPV6 yığınını IPV4 uygulamaları ise IPV4 yığınını kullanırlar. Temel olarak akış kararı IP başlığındaki versiyon bölümüne dayanır.[[67]](#footnote-68)

İkili yığın mekanizması temel ve en çok kullanılan geçiş mekanizmasıdır. İkili yığın mekanizmasının birincil avantajı network içerisinde herhangi bir tünelleme gerektirmemesidir. IPV4 ve IPV6 protokolleri network kaynaklarını paylaşmamaları dışında birbirinden bağımsız olarak çalışabilirler. IPV4 ve IPV6 aynı cihaz üzerinde bağımsız yönlendirme tablolarına, bağımsız servis kalitesi ve güvenlik politikalarına sahiptir.[[68]](#footnote-69)

Teknik stratejiler bakımından ikili yığın yaklaşımı tüm cihazların (bilgisayarlar, yönlendiriciler, cep telefonları vb...) IPV4 cihazlarla IPV4 paketler kullanarak IPV6 cihazlarla ise IPV6 paketler kullanarak haberleşmesini belirtir. İnternetteki çoğu ağın amacı diğer ağlarla iletişimini arttırmak olduğundan günümüzde IPV6 implementasyonlarının çoğu ikili yığın yöntemiyle yapılmaktadır. İkili yığın yaklaşımı altyapıdaki yönlendirici, güvenlik duvarı, DNS, güvenlik ve yönetim yazılımı gibi cihazlarda önemlidir. Uç cihazlarda ise tercihe göre ikili yığın, sadece IPV4 veya sadece IPV6 kullanılabilir.[[69]](#footnote-70)



Şekil 0 İkili Yığın Gösterimi

* + 1. Tünelleme Yöntemi:

Tünelleme geçiş yönteminde IPV6 paketleri IPV4 networkleri üzerinden IPV6 cihazların uçtan uca iletişim kurmasına izin vermek için kullanılır. Tünelleme yönteminde mevcut IPV4 yönlendirme altyapısı üzerinde sarmalanmış IPV6 paketleri taşınarak iletişim kurulur. Bu sarmalanmış paketler uç cihazda tekrar açılır.[[70]](#footnote-71)

Dünyada halen IPV4 protokolü yaygın olarak kullanıldığı için aralarında IPV4 ağları bulunan iki IPV6 ağını haberleştirmek tünelleme yöntemi kullanılır. İleride IPV6 yaygın protokol olduğunda ise tam tersine tünelleme yapılabilir.

Tünelleme yöntemlerine örnek olarak aşağıdaki yöntemler söylenebilir:

* Elle yapılandırılmış (manually configured) tüneller
* 6to4 tüneller
* Isatap
* Teredo
  + - 1. Elle Yapılandırılmış Tüneller

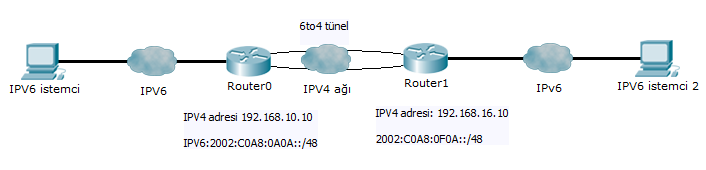
Elle yapılandırılmış tüneller statik olarak IPV6'nın IPV4 içerisinde tanımlanmasıdır. Bu tüneller birçok yönlendirme cihazı tarafından desteklenir. RFC 4213 hali hazırda var olan IPV4 ağı üzerinden IPV6 paketlerini iletebilen elle yapılandırılmış tünellerin özelliklerini belirtir. Bu yöntem IPV4 ağı üzerinden IPV6 paketlerini taşıyabilmek geliştirilen ilk geçiş yöntemlerinden biridir. Adres başlığı yapısında bulunan data ve IPV6 adresi kısmı IPV4 adresi ile sarmalanarak iletilir. Tünelin karşısındaki cihazda ise bu sarmal çözülür.[[71]](#footnote-72)

Bu yöntemin dezavantajı olarak her uç nokta için yapılandırma yapmak söylenebilir. Eğer çok fazla sayıda tünel varsa bunların yönetimi zorlaşır.

* + - 1. 6to4 Tüneli

6to4 tünelin özellikleri RFC 3056'da tanımlanmaktadır. Tipik olarak sınır yönlendiricilerde yapılandırma gerektirirken otomatik tünelleme mekanizmasıdır. Tünel hedef adresleri IPV6 adreslerinin içerisine gömülen IPV4 adresleridir.[[72]](#footnote-73)

6to4 en yaygın kullanılan otomatik tünelleme mekanizmasıdır. 6to4 ağlarında adres yapısında 2002:IPV4ADDR::/48 şeklindeki özel bir adres öneki kullanılır.[[73]](#footnote-74) Örneğin yönlendiricinin tünel IPV4 adresi 192.168.10.10 olsun. Bu IP adresi için IPV6 öneki 2002:C0A8:0A0A::/48 olacaktır.



Şekil 0 6to4 Tünel Gösterimi

6to4 yönteminde dikkat edilmesi gereken nokta tünelin arkasında NAT işlemi yapılmışsa ve tünelin kurulduğu yönlendirici ile NAT yapılan cihaz farklı cihazlarsa NAT arkasında kalan istemciler bu yöntemi kullanamazlar.[[74]](#footnote-75)

6to4 yönteminde üç farklı bileşen kullanılır. Bu bileşenler 6to yönlendirici, 6to istemci ve 6to4 nakledici yönlendiricidir.

6to4 yönlendirici bir taraftaki arayüzünde 6to4, diğer taraftaki arayüzünde ise IPV4 ağ bulunan yönlendiricidir. 6to4 yönlendiricinin IPV4 ağına bakan arayüzüne yönlendirilebilir bir IPV4 adresi atanmalıdır. 6to4 yönlendiricinin 6to4 ağına bakan arayüzüne ise 2002:IPV4ADDR::/48 öneki ile başlayan IPV6 adresi atanır. Bu arayüzündeki öneki 6to4 istemcilere duyurarak onların da IPV6 adreslerini oluşturmasını sağlar.[[75]](#footnote-76)

6to4 istemci, 6to4 yönlendiriciden aldığı öneki kendi arayüz tanımlayıcısı ilebirleştirerek 6to4 IPv6 adresini elde eder. 6to4 istemcide herhangi bir tünelleme işlemi yapılmaz.

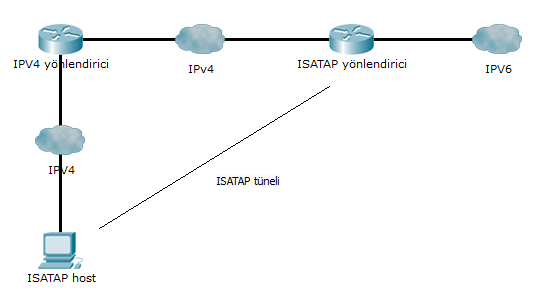
6to4 nakledici yönlendirici ise bir tarafında 6to4 ağı, diğer tarafında ise IPV6 ağı bulunan yönlendiricilerdir.

* + - 1. Isatap geçiş yöntemi

ISATAP IPV6 uç noktalarının IPV4 ağları üzerinden haberleşmesi için kullanılan tünelleme yöntemlerinden bir tanesidir. RFC 5214 isatap yönteminin detaylı olarak açıklamaktadır. isatap tünelleri IPV4 adresini IPV6 adresinin son 32 bitinin içine gömer. isatap adreslerinin:

* İlk 64 biti link-local yada global IPV6 adresi önekidir.
* Daha sonra gelen 32 bit 0000:5EFE'dir.
* Son 32 biti ise IPV4 adresini içerir.[[76]](#footnote-77)

IPv6 desteği sunan Microsoft işletim sistemlerinde isatap desteği bulunmaktadır. Şekil 20'de bir isatap tünel yapısı gösterilmektedir.



Şekil 0 ISATAP Tüneli

* + - 1. Teredo Geçiş Yöntemi

Teredo Tüneli NAT arkasında kalan IPv6 cihazlara IPv4 ağı üzerinden erişebilmek için kullanılır. teredo tünelinde iletişim UDP paketleri ile sağlanır. Ağdaki NAT cihazları ipv6 yönlendirme yapamadıklarında ve 6to4 dönüştürücü özellikleri olmadığı durumlarda teredo yöntemi kullanılabilir.[[77]](#footnote-78) Bu yöntemin 6to4 ve isatap yöntemlerinin kullanılamadığı durumlarda son çare olarak kullanılması önerilmektedir.[[78]](#footnote-79)

Teredo tünelleme yapısında teredo sunucusu, teredo istemcisi ve teredo nakledicisi olmak üzere 3 adet bileşen bulunmaktadır. Tünel teredo istemcisi ve teredo nakledicisi arasında kurulur.

Teredo öneki için IPV6 adres havuzunda 2001:0000:: /32 aralığı rezerve edilmiştir.

Teredo yönteminde kullanılan adresleme mekanizmasında:

* İlk 32 biti değeri 2001:0000:: /32 olan teredo önekini
* Sonraki 32 biti teredo sunucusunun IPV4 adresinin 16'lık sistemde gösterimini
* Sonraki 16 biti adres tipi ve NAT belirleyen bayraklar kısmını
* Sonraki 48 biti ise istemciye ulaşacak olan NAT cihazının genel IPv4 adresini ve istemcinin dinlediği Teredo portuna ulaşacak NAT cihazı portu bilgisini belirtmektedir.[[79]](#footnote-80)
  + 1. Çeviri Yöntemi

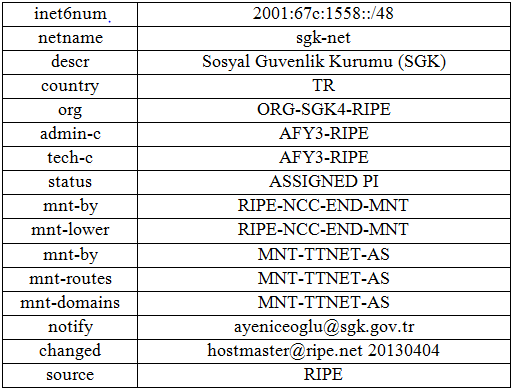
Geçiş yöntemleri içerisinde bahsedilen üçüncü yöntem ise RFC 2766'da detayları açıklanan NAT protokolü çevirisidir. NAT-PT IPV4 ağı ile IPV6 arasındaki, bu iki ağı ayıran sınır yönlendiricilere uygulanır.NAT-PT yönteminde herhangi bir enkapsülasyon yoktur. Bu yöntemde paketteki kaynak IP bilgisi değiştirilerek yerine IP adresi gelir. IPV4 NAT işlemindeki gibi statik, dinamik ve birden fazla IP adresini bir IP adresine atayan “many-to-one” NAT-PT türleri vardır.[[80]](#footnote-81)

BÖLÜM 3

IPV6 GEÇİŞİ UYGULAMA ÇALIŞMASI

1. 1. Geçiş Hazırlığı

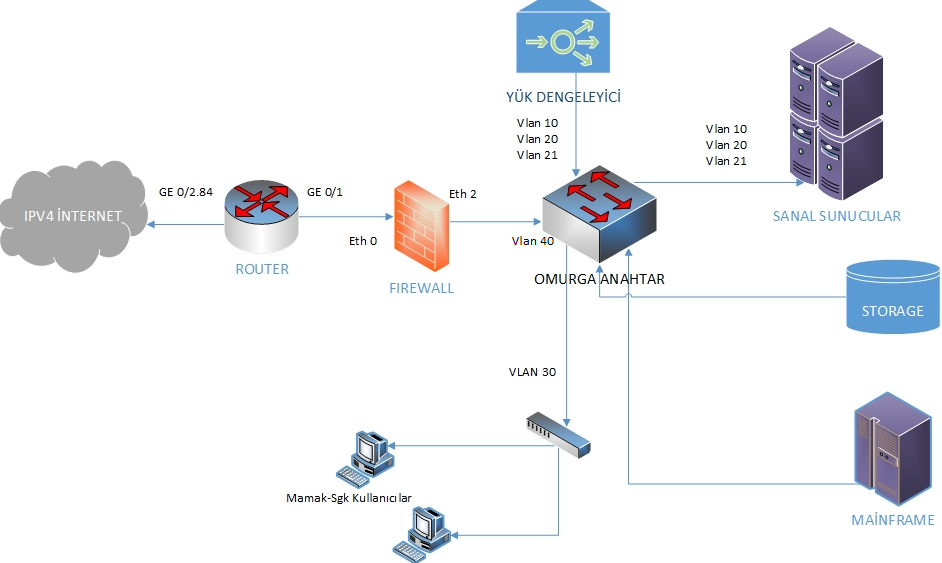
Hazırlanan bu çalışma kapsamında Sosyal Güvenlik Kurumu altyapısı da dikkate alınarak İnternet üzerinden kullanıcılara sağlanan hizmetlerin IPV6 protokolüne geçirilmesi için örnek bir uygulama yapılacaktır. Bu işlem için öncelikle Sosyal Güvenlik Kurumu için RIPE NCC'den IPV6 adresleri alınmıştır. Bu işlem için RIPE NCC'ye Sosyal Güvenlik Kurumu servis sağlayıcısı Türk Telekom aracılığıyla başvuru yapılmıştır. Başvuru sonucunda RIPE NCC'den gelen "IPv6 PI Assignment Request Form" adlı döküman doldurularak gönderilmiştir. Bu dökümanda RIPE NCC tarafından kurumla ilgili sorulan çeşitli sorulara cevap verilmiştir. Ve istenilen IPV6 bloğunun /48 olduğu belirtilmiştir. Bu işlemden sonra RIPE NCC tarafından aşağıdaki bilgiler kuruma gönderilerek IP ataması yapılmıştır.



Şekil 0SGK IPv6 bilgileri

RIPE tarafından SGK'ya atanan bu bilgilere göre kurumun global unicast IPV6 adres bloğu 2001:67c:1558::/48 olarak belirlenmiştir.

IPV6 adres bloğu alındıktan sonra hazırlık için ikinci aşama olan dışarıya hizmet veren uygulamalar için topoloji ve ağdaki üçüncü seviye yönlendirici ve güvenlik cihazları için envanter çalışması yapılmıştır. Yapılan bu çalışmaya göre SGK bünyesinde bulunan, vatandaşlara hizmet veren uygulamaların topolojisi genel hatları ile şu şekildedir.



Şekil 0 Uygulama Topolojisi

Bu topolojiye göre internet üzerinden gelen bir kullanıcı öncelikle yönlendiriciden geçmektedir. Yönlendiricinin GE 0/2,84 arayüzü ISP olan Türk Telekom'la aradaki bağlantıyı sağlayan /30 subnetli noktadan noktadan IPV4 adresine sahiptir. Yönlendiricinin GE 0/1 arayüzü ise SGK'ya atanmış C sınıfı bir genel IPV4 adresine sahiptir. Bu IP bloğu aynı zamanda ateş duvarının dış (external) arayüzü IP bloğudur. Ateş duvarı içerisinde kalan özel IP'ler ateş duvarından dışarı çıkarken NAT işlemine tabi tutularak internette yönlendirilebilen genel IP'lere çevrilir. Ateş duvarının genel IP'sine gelen istekler Ateş duvarından içeri girerek omurga anahtar tarafından önce yük dengeleyici cihaza gönderilmektedir. Yük dengeleyicinin sanal IP'sine gelen istekler bu sanal IP'nin ait olduğu sunucu havuzundan bir sunucuya gönderilir. Sunucu arka tarafta diğer sunucular ve veritabanıyla yapması gereken işlemi gerçekleştirdikten sonra istemciye aynı şekilde cevap döner.

Topoloji çalışması yapıldıktan sonra bu topolojide geçen üçüncü seviye yönlendirme ve güvenlik cihazları için envanter çalışması yapılmıştır. IPV6 geçişi için kritik olan bu cihazlar şunlardır:



Şekil 0 Üçüncü Seviye Yönlendirme Ve Güvenlik Cihazları

Şekil 23'te görüldüğü gibi kurum altyapısında kullanılan üçüncü seviye yönlendirme ve güvenlik cihazları IPV6 protokolünü desteklemektedir. Bu nedenle geçiş çalışması yapılırken herhangi bir maliyet oluşturacak ek yatırıma ihtiyaç duyulmamaktadır.

Envanter ve topoloji çalışması tamamlandıktan sonra hangi geçiş yönteminin kullanılacağı tespit edilmelidir. Servis sağlayıcı olan Türk Telekom IPV6 desteği sunabildiği ve bir IPV4 networku üzerinden IPV6 paketleri geçirme ihtiyacı duymayacağımız için tünelleme yöntemlerini kullanmayacağız. Literatürde şartlar uygun olduğu takdirde geçiş için en iyi yöntemin ikili yığın yöntemi olduğu belirtilmiştir. Bu çalışmada da geçiş kullanılacak olan yöntem ikili yığın yöntemi olacaktır.

Kurum bünyesinde bulunan ve dışarı hizmet veren sigorta ,e-eczane, e-hastane, e-optik gibi uygulamalar yük dengeleyici arkasında çalıştığından planlanan geçişte yük dengeleyici cihazının önemli bir özelliği kullanılacaktır. Yük dengeleyici cihaz çalışma mantığı olarak kendi sanal IP'sine gelen bir isteği o sanal IP'nin ait olduğu sunucu havuzundaki bir sunucuya yönlendirmektedir. Bu cihazın IPV6 geçişinde kullanılacak özelliğinde ise aynı havuza bir de IPV6 sanal adresi atanabilmektedir. Atanan bu IPV6 sanal adresine gelen istekler bu adresin ait olduğu havuzdaki IPV4 adresli sunuculardan birine gönderilebilmektedir. Bu özelliğin kullanılması ile birlikte sunucuların her birine ikili yığın konfigürasyonu yapma zorunluluğu ortadan kalkmaktadır. Zaman içerisinde tüm sunucularda da ikili yığın konfigürasyonu ve en nihayetinde yalın IPV6 konfigürasyonu yapılabilir.

Geçiş hazırlığı kısmında son olarak IP planlaması yapılmıştır. Yapılan IP planlamasına göre alınan /48'lik IP bloğu /64'lük daha küçük parçalara ayrılmıştır. Ve bu /64'lük bloklar gerekli yerlere atanmıştır. Uygulama topolojisinde gözüken yönlendiricinin GE0/1 arayüzü ile ateş duvarının Eth0 arayüzü arasına 2001:1558:67c:1::/64 bloğu atanmıştır. Ateş duvarının Eth2 arayüzü ile Omurga anahtar arasına (Vlan 40) 2001:1558:67c:6::/64 bloğu atanmıştır. Omurga anahtar üzerindeki diğer Vlan'larda kullanılmak üzere Vlan 10 için 2001:67c:1558:3::/64 bloğu, Vlan 20 için 2001:67c:1558:4::/64 bloğu, Vlan 21 için 2001:67c:1558:5::/64 bloğu, Vlan 30 için ise 2001:67c:1558:2::/64 bloğu atanmıştır.

Bahsedilen geçiş hazırlığı çalışmaları tamamlandıktan sonra geçiş için üçüncü seviye yönlendirme ve güvenlik cihazları yapılandırılmasına başlanmıştır.

* 1. Geçiş Çalışmaları

1. 2. 1. Yönlendirici Yapılandırması

Bölüm 3.1'de gösterilen uygulama topolojisine göre en dışta bulunan 3. seviye cihazı yönlendirici cihazıdır. İlk olarak yönlendirici cihazı ikili yığın çalışacak şekilde yapılandırılacaktır. Bu yapılandırma için Şekil 22'te görülen yönlendiricinin GE0/2.84 arayüzüne, mevcut IPV4 adresine ek olarak servis sağlayıcı olan Türk Telekom’la yapılacak bağlantı için Türk Telekom’dan alınan IPV6 adresi atanacaktır. GE0/1 arayüzüne ise 2001:1558:67c:1::1/64 IPV6 adresi atanacaktır.

Bu işlemin gerçekleştirilebilmesi için Türk Telekom'la irtibata geçilmiş ve internet bağlantısı için IPV6 adresi talep edilmiştir. Ayrıca SGK'ya RIPE NCC tarafından tahsis edilen IPV6 adres bloğunun verilecek bu IPV6 adresine yönlendirilmesi istenmiştir. Bu talep üzerine Türk Telekom tarafından bağlantı için kurum tarafına 2a01:358:4000:004E::2/64 IP'si tahsis edilmiştir. Bu IP içinde Türk Telekom tarafı IP'sinin 2a01:358:4000:004E::1/64 olduğu bilgisi verilmiştir. Türk Telekom'dan alınan bu bilgilerle yönlendirici arayüz yapılandırılması yapılmıştır.

Newtork cihazları üzerinde yapılandırmalar iki şekilde yapılabilir. Birinci yöntem komut cihaza consol, telnet yada ssh bağlantısı yaparak komut satırı üzerinden yapılandırmaktır. Bu işlemler için putty yada Secure Crt gibi yazılımlar kullanılabilir. İkinci yöntem ise cihaza tarayıcı (browser) üzerinden erişip web arayüzü ile işlem yapmaktır. Yönlendirici üzerinde yapılan tüm işlemler komut satırı üzerinden yapılmıştır.

Burada önemli olan bir nokta IPV6 ataması yapmadan önce cihazda config modda "ipv6 unicast routing" komutu kullanılmıştır. Bu komutla yönlendirici IPV6 yönlendirici olarak çalışmaya başlamıştır.

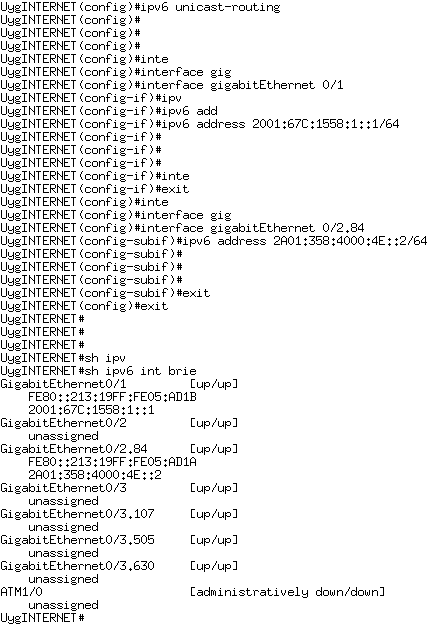
IPV6 yapılandırması ise yine config modda şu şekilde yapılır:

(config)#ipv6 unicast-routing

(config)#interface gigabitEthernet 0/1

(config-if)#ipv6 address 2001:67C:1558:1::1/64

Tüm arayüzlere aynı şekilde IPV6 adresleri atandıktan sonra config moddan çıkarak "sh ipv6 int brief" komutu ile yapılandırılmış IPV6 adresleri kontrol edilebilir. Yönlendirici üzerinde yapılan işlemler Şekil 24'te gözükmektedir.

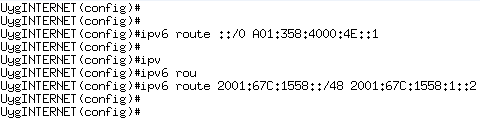


Şekil 0 Yönlendirici Arayüz Yapılandırması

Yönlendirici cihazda arayüz IP'leri atandıktan sonra rotaların yazılması gerekmektedir. İç taraf için kuruma tahsis edilen IPV6 bloğu için 2001:1558:67c::/48 IP bloğu 2001:1558:67c:1::2 IP adresine yönlendirilmiştir. Bu IP adresi ateş duvarının dış arayüzüne verilmiştir. İnternete çıkış için ise varsayılan rota yazılması gerekmektedir. Yönlendirici en dıştaki cihaz olduğu için bu iki şekilde yazılabilir. Birinci yazılım "0::0" şeklindedir. Bu gösterim tüm IP adresleri anlamına gelmektedir. İkinci yazılım ise 2000::/3 şeklindedir. Bu gösterim de tüm global tekil gönderim IP adresleri demektir. İnternette global tekil gönderim yönlendirilebildikleri için bu gösterim de doğrudur. Yönlendirici üzerinde yönlendirme yapılandırması kurum altyapısında da kullanılan statik yönlendirme işlemi yapılacaktır. Statik yönlendirme işlemi config modda şu şekilde yapılır:

(config)#ipv6 route ::/0 A01:358:4000:4E::1

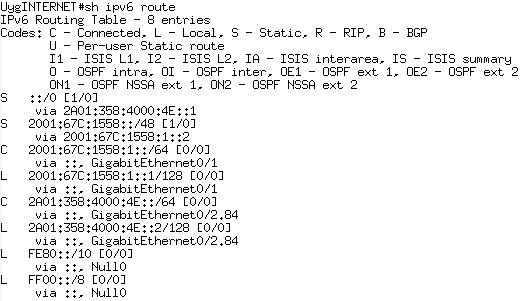
şekil 25'de yönlendirici üzerinde yapılan işlem gözükmektedir.



Şekil 0 Yönlendirici İçin Yönlendirme Yapılandırması

Yapılan bu işlemlerden sonra cisco 7200 yönlendirici üzerindeki yapılandırma tamamlanmıştır. Tüm bu işlemler cihaz üzerinde var olan yapılandırmaya ek olarak, cihaz çalışırken yapılmıştır. İkili yığın yönteminde cihaz IPV6 yapılandırılırken normal IPV4 çalışmasına devam eder. IPV4 rota tablosunun yanında bir de IPV6 rota tablosu oluşturur. Bu iki tablo birbirinden bağımsızdır. Aynı arayüz üzerinde IPV4 ve IPV6 yapılandırması çalışır. Gelen paket IPV6 ise IPV6 adreslerine yönlendirme yapılır. Paket IPV4 ise IPV4 adreslerine yönlendirme yapılır.

Yönlendiricinin IPV6 rota tablosunu kontrol etmek için config moddan çıkarak "sh IPV6 route" komutu kullanılır. Şekil 26'de bu komutun çıktısı gözükmektedir.



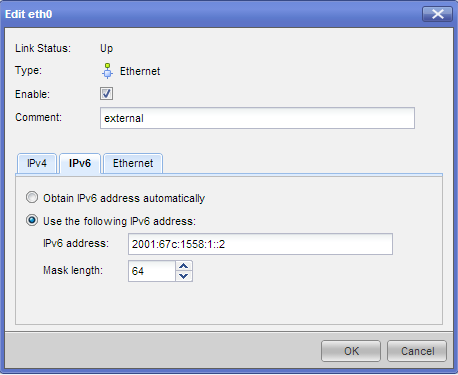
Şekil 0 Yönlendiricinin IPv6 Rota Tablosu

* + 1. Ateş Duvarı Yapılandırması

Yapılan çalışmanın kurumun güvenlik politikalarına aykırı olmaması için mevcut çalışan ateş duvarı kullanılmamıştır. Bunun yerine bir fiziksel sunucu üzerine checkpoint ateş duvarı kurularak, ağa dahil edilmiştir. Kısıtlı erişim politikaları ile yönlendirme yapılmıştır. Çalışma bittikten sonra kurulan ateş duvarı kaldırılmıştır.

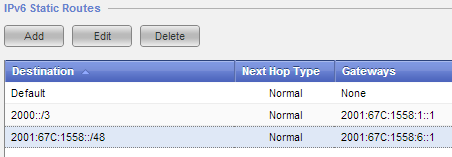
Ateş duvarı için de arayüz yapılandırmaları yapılmış ve yönlendirme tablosu oluşturulmuştur. Bu işlemler için şekil 22'de gözüken ateş duvarının Eth0 arayüzüne 2001:67c:1558:1:2 /64 IPV6 adresi atanmıştır. Eth2 arayüzüne ise 2001:67c:1558:6::2 /64 IPV6 adresi atanmıştır. Ateş duvarının Eth0 arayüzü external (dış) arayüzü olacaktır. Bu arayüz güvenli olmayan dış ortama bakan arayüzdür. Eth2 arayüzü ise internal (iç) arayüzü olacaktır. Bu arayüz ateş duvarı politikalarından dolayı güvenli olan iç ağa bakan arayüzdür.

Ateş duvarının arayüz yapılandırmaları sahip olduğu web arayüzü üzerinden yapılmaktadır. Şekil 27'de Eth0 için ateş duvarının arayüz yapılandırması gözükmektedir. Diğer arayüzler de aynı şekilde yapılandırılır.



Şekil 0 Ateş Duvarı Arayüz Yapılandırması

Ateş duvarında arayüz yapılandırma işlemi tamamlandıktan sonra ateş duvarı üzerindeki yönlendirmelerin yapılması gerekmektedir. Ateş duvarı üzerinde internete çıkış için 2000::/3 IP bloğu 2001:67c:1558:1::1 IP adresine yönlendirilmiştir. 2001:67c:1558:1::1 IP adresi ateş duvarının önündeki yönlendiricinin IP adresidir. İç taraf içinse 2001:67c:1558::/48 bloğu ise 2001:67c:1558:6::1 IP'sine yönlendirilmiştir. 2001:67c:1558:6::1 IP'si ise omurga anahtarın ateş duvarına bakan Vlan olan Vlan 40 ait IP'dir. Şekil 28'de ateş duvarı yönlendirme tablosu gözükmektedir.



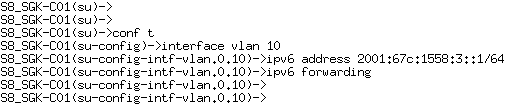
Şekil 0 Ateş Duvarı Rota Tablosu

Ateş duvarının netwok konfigürasyonları yapıldıktan sonra kurumun güvenlik politikaları doğrultusunda ateş duvarı politikaları yapılandırrılmalıdır. IPV6'da NAT işlemi olmadığı için güvenlik duvarı politikalarında bu konu dikkate alınmalıdır. Ayrıca IPV6'nın bazı özellikleri ICMPv6 üzerinden çalıştığı için gerekli ICMPv6 başlıklarına izin verilip geri kalanların kapatılması gerekmektedir.

* + 1. Omurga Anahtar Yapılandırması

Omurga anahtar üçüncü seviye yönlendirme özellikleri de taşıyan bir anahtardır. Bu anahtarda Vlan'lar oluşturulup oluşturulan bu Vlan'lara IP ataması yapılabilmektedir. Şekil 22'te gösterilen topoloji yapısında omurga anahtar üzerindeki Vlan'lar gösterilmiştir. Bu gösterime göre ateş duvarı ve omurga anahtar arasında Vlan 40 bulunmaktadır. Sunucu tarafında Vlan 10,20 ve 21 bulunmaktadır. Kullanıcıların bulunduğu kısım ise Vlan 30'dur. Omurga anahtar cihazı bu Vlan'lar arasında yönlendirmeler yapmaktadır. Hali hazırda bu Vlan'lar üzerinde IPV4 adresleri bulunmaktadır. Anahtar ise gerekli ayarlarda yapılandırılmış şekildedir. Bu çalışma kapsamında anahtarın var olan Vlan arayüzlerine IPV6 adres tanımlamaları yapılmış ve gerekli yönlendirmeler anahtar üzerinde de tanımlanmıştır. Anahtar üzerindeki Vlan'lara Vlan 10 için 2001:67c:1558:3::1/64, Vlan 20 için 2001:67c:1558:4::1/64, Vlan 21 için 2001:67c:1558:5::1/64 bloğu, Vlan 30 için 2001:67c:1558:2::1/64, Vlan 40 için ise 2001:67c:1558:6::1/64 IP adresleri atanmıştır. Bu ip adresleri ataması yapıldıktan sonra yönlendirme işleminin yapılabilmesi için omurga anahtar üzerinde "ipv6 forwarding" komutunun çalıştırılması gerekmektedir.

Omurga anahtar üzerindeki Vlan'lara IP ataması şekil 29'da gösterildiği şekilde yapılır.



Şekil 0 Omurga Anahtar Vlan Arayüz IP Yapılandırması

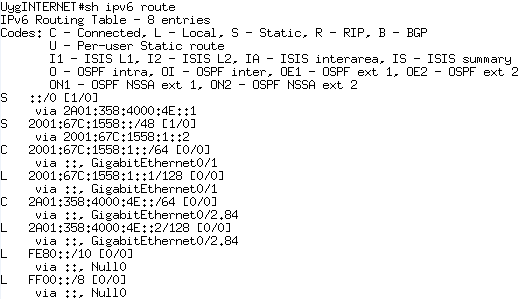
Tüm Vlan arayüzleri IP yapılandırması aynı şekilde yapıldıktan sonra "sh ipv6 int brief" komutu kullanılarak IP yapılandırmaları görülebilir. Şekil 30'da bu komutun çıktısı gözükmektedir.



Şekil 0 Vlan Arayüz IP'leri

Vlan arayüz IP adresleri atandıktan sonra Vlan 30'da bulunan bulunan kullanıcı bilgisayarlarına da omurga anahtar tarafından otomatik IPV6 adresleri dağıtılmıştır.

IP atama işlemleri omurga anahtar üzerinde tanımlandıktan sonra gerekli yönlendirmelerin yapılması gerekmektedir. Omurga anahtar üzerindeki Vlan'lara IP verildiği an, bu Vlanlar cihazın üzerinde olduğu için yönlendirme tablosunda Vlan'ları ve IP'lerini görülecektir. Dışarıya çıkış için ateş duvarına doğru bir yönlendirme yazılması gerekmektedir. Ateş duvarının omurga anahtara bakan arayüzünün IP'si 2001:67c:1558:6::2 olarak atandığı için 0::0/0 varsayılan rotası bu IP'ye yönlendirilerek omurga anahtar üzerindeki yönlendirme yapılandırması tamamlanır. "Sh ipv6 route" komutu ile omurga anahtar üzerindeki yönlendirme tablosu görülebilir. Şekil 31'da bu komutun çıktısı görülmektedir.

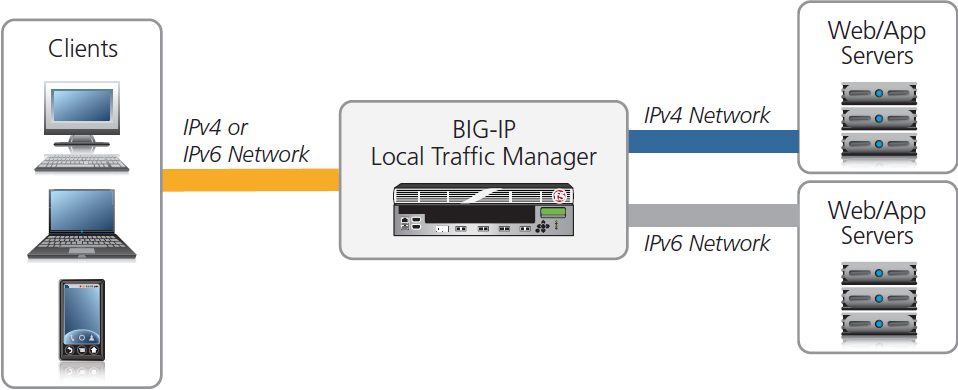


Şekil 0 Omurga Anahtar IPv6 Yönlendirme Tablosu

* + 1. Yük Dengeleyici Yapılandırması

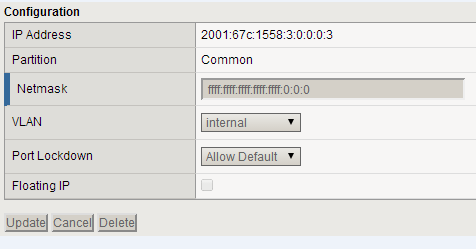
Yük dengeleyici cihazının temel olarak görevi kendi sanal IP'sine gelen istekleri o IP'nin ait sunucu havuzundaki sunuculara dağıtmaktır. IPV6 geçiş uygulama çalışmasında da bu cihazın IPV6 olan sanal IP'sine gelen istekleri arka taraftaki IPV4 sunuculara dağıtma özelliğinden faydalanılmıştır. Yük dengeleyici cihazda IPV6 adreslerine gelen istekleri IPV4 sunuculara dağıtma işleminin yanı sıra ihtiyaca bağlı olarak sanal IPV4 adresine gelen işlemleri IPV4 sunuculara dağıtabilme işlemi de yapılabilmektedir.

Şekil 32' de kurum alt yapısında da kullanılan yük dengeleyici olan F5 BIG-IP local traffic manager cihazının IPV6 sistem geçişinde nasıl kullanılabileceği gözükmektedir.[[81]](#footnote-82)



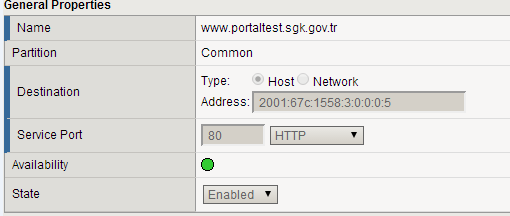
Şekil 0 Yük Dengeleyici Cihazın IPv6 Geçişinde Kullanılması

Bu işlem için öncelikle yük dengeleyici cihaza self IP atanmıştır. Self IP yük dengeleyici cihaz üzerinde tanımlı Vlan'lara ait bir IP bloğundan verilmelidir. Bu çalışma için yük dengeleyici cihaza 2001:67c:1558:3::3 IP'si self IP olarak verilerek tanımlı Vlan'a atanmıştır. Şekil 33'de bu işlem gözükmektedir.



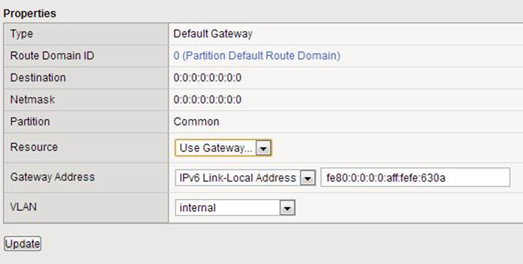
Şekil 0Yük Dengeleyeci Self-IP Ataması

Yük dengeleyicinin kendi IP'si olan Self-Ip atandıktan sonra hali hazırda test için kullanılan bir IPV4 sunucu havuzunun yük dengeleyici üzerindeki sanal IP'si IPV6 adresi ile değiştirilmiştir. Bu IP'ye gelen istekler arka taraftaki IPV4 sunuculara iletilecektir. Yük dengeleyici cihazında test için kullanılan sunucu havuzunun sanal IP'sine 2001:67c:1558:3::5 IP adresi atanıştır. Şekil 34'de bu işlem gözükmektedir.



Şekil 0 Yük Dengeleyici Sanal IP Ataması

Bu sunucu havuzu içerisinde sekiz adet üye bulunmaktadır. İstekler IPV4 adresine sahip bu üyelere dağıtılacaktır. Bu işlemden sonra yük dengeleyici cihaz için de yönlendirme ayarlarının yapılması gerekmektedir. 0::0/0 ağı omurga anahtarın Vlan 10'daki link-local IPV6 adresine yönlendirilmiştir. Şekil 35'de bu işlem gözükmektedir.

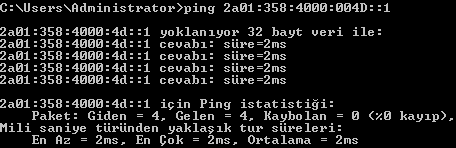


Şekil 0 Yük Dengeleyici Yönlendirme

Yük dengeleyici test havuzu üyeleri IPV4 adresleri kurum içinde kullanılan IPV4 adreslerinden oluştuğu için güvenlik gerekçesi ile bu çalışmada detaylı olarak belirtilmemiştir. Havuz içerisinde 10.X.X.X:YYYY şeklinde bir IPV4 adresi ve port numaralarına sahip 8 üye bulunmaktadır.

* + 1. Uygulamanın Test Edilmesi

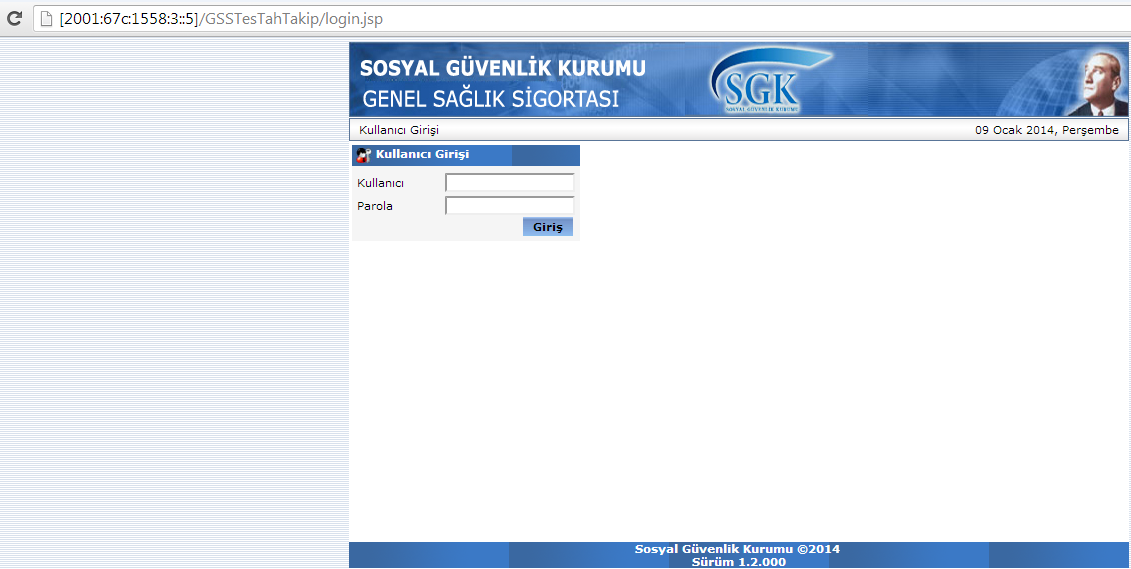
Şekil 23'de gösterilen topolojiye göre Vlan 30'da bulunan kullanıcı bilgisayarlarında IPV6 yapılandırması yapılmıştır. Ve bu kullanıcı bilgisayarlarından biri ile bağlantılar test edilecektir. Öncelikle bilgisayardan yönlendiricinin dış tarafındaki Türk Telekom IPV6 adresine ping atılmıştır. Şekil 36'da Türk Telekom bağlantısı testi gözükmektedir.



Şekil 0 Türk Telekom Tarafı Bağlantı Testi

Yönlendiricinin dış tarafındaki Türk Telekom IP adresine ping atılabilmektedir. Bu Türk Telekom ile aradaki IPV6 iletişiminin olduğunu gösterir. Daha sonra yük dengeleyici arkasındaki IPV4 test sunucularına IPV6 adresi üzerinden erişimin olup olmadığını kontrol etmek için tarayıcıya yük dengeleyicinin sanal IP'sine atadığımız IPV6 adresini yazarak iletişim kontrol edilir. Burada dikkat edilmesi gereken nokta tarayıcıya IPV6 adresleri yazılırken köşeli parantez içerisine alınır. Bunun sebebi tarayıcının IPV6 adresi port numaralarını karıştırmaması gerektiğidir. Şekil 37'de tarayıcı ekran görüntüsü gözükmektedir.

Yapılan uygulama sonucunda tarayıcıdan IPV6 üzerinden uygulamaya erişim başarılı olmuştur. IPV6 adresi ile yük dengeleyici arka tarafındaki IPV4 sunucularından birisi bağlantı kurulmuştur. Bu örnek uygulamada yapılan çalışma, gerekli DNS ayarları da yapıldıktan sonra Sosyal Güvenlik Kurumu IPV6'ya geçişi için kullanılabilir.



Şekil 0 Test Sunucusu Ekran Görüntüsü

DÖRDÜNCÜ BÖLÜM

SONUÇ VE ÖNERİLER

1980'li yıllarda geliştirilen TCP/IP protokolü zaman içeresinde internette kullanılan baskın protokol haline gelmiştir. TCP/IP'de kullanılan IPV4 teknoloji ilerledikçe ve internete bağlı cihaz sayısı arttıkça zaman içerisinde ihtiyaçları karşılamak için yetersiz hale gelmiştir. IPV4 ilk ortaya çıktığında yaklaşık 4 milyar IP adres havuzuna sahip bir protokol olarak düşünülmüştür. İnternete bağlı cihaz sayısının günümüzdeki kadar yaygın olacağı öngörülemediğinden ve IP dağıtımı hiyerarşik olarak düzenli yapılamadığından adres yetersizliği sorunu başlamıştır. Bunun sonucu olarak IPV6 adında yeni bir IP adresi versiyonu geliştirilmiştir. Geliştirilen IP adresi versiyonunda IPV4'ün bir kısım eksiklikleri de giderilmiş ve yeni özellikler eklenmiştir. Bu özellikler genişletilmiş adres havuzu, arttırılmış servis kalitesi ve güvenlik özellikleri, otomatik yapılandırma olarak sıralanabilir. Ayrıca IPV6 ile birlikte IP adresi başlık yapısı optimize edilerek daha performanslı bir protokol oluşturulması amaçlanmıştır.

IPV6'ya geçiş ile ilgili tüm dünyada ve ülkemizde çeşitli çalışmalar yapılmıştır. İnternet erişiminde sürekliliğin sağlanması açısından bu çalışmalar önem arz etmektedir. Ülkemizde Tübitak tarafından hazırlanman "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" ile kamu kurumlarının IPV6'ya geçişi ile ilgili bir yol haritası çizilmiştir.

Yapılan bu çalışmasının uygulaması kapsamında Sosyal Güvenlik Kurumu alt yapısına benzer bir test ortamı oluşturulmuş ve bu test ortamında IPV6 geçişi uygulaması test edilmiştir. Yapılan çalışma dışarıya hizmet veren Sosyal Güvenlik Kurumu web uygulamaları ile sınırlandırılmıştır. Çalışma sırasında alt yapıda kullanılan ve IPV6 için kiritik öneme sahip cihazların IPV6 desteklerinin olduğu görülmüş IPV6 geçişi için ek bir maliyet gerekmediği ortaya çıkmıştır. Çalışma sonunda ise test amacıyla seçilen bir web uygulaması IPV6 ile erişilebilir hale getirilmiştir. Çalışma sırasında uygulamaya sadece IPV6 adresi ile erişilmiştir. Gerçek ortamda IPV6 geçişi yapıldığında IPV6 için gerekli DNS ayarlarının da yapılması gerekmektedir.

IPV6 protokolü ile birlikte IPV4 kullanılan, bildiğimiz anlamdaki NAT işlemi kalkmıştır. Ayrıca IPV6'nın düzgün çalışması için bazı ICMPv6 paketlerine izin vermek gerekmektedir. Bunlar güvenlik anlamında yeni protokolle birlikte gelen dikkat edilmesi gereken noktalardır.

Yapılan test çalışmasının gerçek ortama aktarılırken öncelikle kullanım yoğunluğu görece az olan bir ve veya iki uygulama üzerinde denenmesi faydalı olacaktır. Bu uygulamaların IPV6'ya geçişinin sistem üzerindeki etkileri detaylı bir şekilde incelendikten sonra varsa problemler tespit edilip çözümler üretilmeli daha sonra aşama aşama tüm uygulamalar IPV6'ya geçirilmelidir.

Test çalışmasında, kurum altyapısında kullanılan uygulamaların büyük çoğunluğu yük dengeleyici cihaz arkasında çalıştığından bu noktaya yoğunlaşılmıştır. Yük dengeleyici arkasında çalışmayan uygulamalarda ise uygulamaların çalıştığı sunucuların ikili-yığın şeklinde yapılandırılması gerekmektedir.

Çalışma kapsamı her ne kadar dışarıya hizmet veren uygulamalarla sınırlı tutulsa da zamanla tüm altyapının IPV6'ya geçmesi kaçınılmaz görünmektedir. Bu işlem için kurum altyapısında kullanılan tüm yönlendirme, güvenlik, anahtarlama cihazları, istemci cihazlar ve sunucular gibi IPV6'yı desteklemesi gerekmektir. Ayrıca kurum içinde kullanılan yazılımlar içerisinde IP bağımlı yazılımlar varsa bu yazılımların düzenlenip IP yerine isim bazlı çalışması gerekmektedir.

**KAYNAKÇA**

**Kitaplar:**

**BROWN, Sam Ve Diğerleri**, *Configuring IPv6 for Cisco IOS*, Elsevier Inc., USA, 2002

**ÇAĞILTAY, Kürşat**, *Herkes için İnternet*, Metu Press, Ankara, 1997

**GORALSKI, Walter**, *How To TCP/IP Works In A Modern Network*, Elsevier Inc., USA, 2009

**LAMMLE, Todd**, *CCNA: Cisco Certified Network Associate Study Guide: Exam 640-802, 6th Edition*, wiley pub.,Indianapolis, 2007

**LIU, Dale**, [*Next Generation SSH2 Implementation*](http://www.sciencedirect.com/science/book/9781597492836)*, Securing Data in Motion*, Elsevier Inc., 2008

**MCFARLAND, Shannon Ve Diğerleri**, *ipv6 For Enterprise Networks*, Cisco Press, Indianapolis, 2012

**ODOM, Wendell**, *CCNA ICND1 640-822 Official Cert Guide Third Edition*, Cisco press., Indianapolis, 2012

**Makaleler:**

**AKTAŞ, Mahire**, SAĞIROĞLU, Şeref, "IPv6:Uluslararası Çalışmalar Ve Türkiye’de Durum" Ulusal IPV6 Konferansı, ANKARA, 2011

**C. Bouras, Ve Diğerleri** "The Deploymet Of IPV6 In An IPV4 World And Transition Strategies" Internet Research: Emeral Article, Vol. 13 Iss: 2 pp. 86 - 93

**CHANG, Fangzhe, WADDINGTON, Daniel G,** "Realizing the Transition to IPv6", IEEE Communications Magazine, Volume:40, Issue:6, 2002, s. 138-147

**DAY, John, ZIMMERMANN Hubert,** "The OSI Reference Model", Proceedings Of IEEE, VOL. 71, NO. 12, 1983

**DUNN,Tricia,** "The IPV6 Transition", Internet Computing, IEEE, Volume:6, Issue:3, 2002, s.11-13

**ERDOĞAN, Kenan, AKÇAM, Nursel,** "IPV4'ten IPV6'ya Geçiş Süreci İçin Bütünsel Bir Yaklaşım" EMO 2. Ağ Ve Bilgi Güvenliği Ulusal Sempozyumu Bildirileri, 2008

**LUKASIK, Stephen J.**, "Why the Arpanet Was Built", [Annals of the History of Computing, IEEE](http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=85), Volume:33 Issue:3, 2011

**R. Gilligan, E. Nordmark,** "Basic Transition Mechanisms for IPv6 Hosts and Routers", IETF RFC Belgesi, RFC 4213, 2005

**RFC 791**, "IP Protocol" IETF RFC Belgesi, 1981

**RFC 792**, “Internet Control Message Protocol”, IETF RFC Belgesi, 1981

**RFC 826**, “An Ethernet Address Resolution Protocol”, IETF RFC Belgesi, 1982

**SAILAN, Mohd. Khairil Ve Diğerleri**, "A Comparative Review of IPv4 and IPv6 for Research Test Bed", International Conference on Electrical Engineering and Informatics, Selangor, Malaysia, 2009

**YÜCE Emre**, "IPV4, IPV6 Ve IPV6 Geçiş Yöntemleri Performans Karşılaştırmaları", Ulusal IPV6 konferansı, ANKARA, 2011

**Diğer Kaynaklar:**

Address, Protocols And Ports, [http://www.cisco.com/en/US/docs/security/asdm/6\_2f/user/guide/ref\_ports.html#wp1007738](http://www.cisco.com/en/US/docs/security/asdm/6_2f/user/guide/ref_ports.html" \l "wp1007738) (10.01.2014)

**BOLAT, Ayşegül,** "Mobil IP: Mevcut Düzenlemeler Ve Türkiye Önerileri", Uzmanlık Tezi, Telekominikasyon Kurumu, Ankara, 2004

**ÇALIŞKAN, Beyhan Kaan Ve Diğerleri,** IPV6 El Kitabı V2.1, Tübitak, Ulakbim, 2012

<http://ulakbim.tubitak.gov.tr/sites/images/Ulakbim/ipv6_el_kitabi.pdf> (08.06.213)

IANA IPv4 Address Space Registry,

<http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml> (24.01.2014)

“Internet address space: Economic Considerations İn The Management Of IPV4 And İn The Deployment of IPV6", OECD Ministerial Meeting On The Future Of The Internet Economy Background Report, Seoul, 2008

<http://www.oecd.org/sti/40605942.pdf> (19.01.2014)

Introduction to IP Version 6, Microsoft White Paper, 2008, <http://technet.microsoft.com/en-us/library/bb726944.aspx> (04.10.213)

Kamu Kurum Ve Kuruluşları İçin IPV6'ya Geçiş Planı Konulu Başbakanlık Genelgesi, Sayı: 27779, Tarih: 8 Aralık 2010

**MURPHY, Alan,** "Managing IPv6 Throughout The Application Delivery Network", F5 White Paper,

<http://www.f5.com/pdf/white-papers/ipv6-wp.pdf> (17.12.2013)

Number Resources,

<http://www.iana.org/numbers> (24.01.2014)

RIPE NCC Begins to Allocate IPv4 Address Space From the Last /8, <http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8> (24.01.2014)

RIPE NCC IPv4 Available Pool – Graph,

<https://www.ripe.net/internet-coordination/ipv4-exhaustion/ipv4-available-pool-graph> (24.01.2014)

**ŞAHİN Mustafa,** "IPv6 Sistem Geçişi" Yüksek lisans tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006, s.4

The Seoul Decleration For The Future Of The Internet Economy, 2008

<http://www.oecd.org/internet/consumer/40839436.pdf> (19.01.2014)

Total IPV6 allocations,

<https://labs.ripe.net/statistics/total-ipv6-allocations> (24.01.2014)

Unicast, Multicast And Broadcast Definitions, <http://www.hp.com/rnd/device_help/help/hpwnd/webhelp/HPJ3288A/uni_multi_broadcast.htm> (24.12.2013)

1. LUKASIK, Stephen J., "Why the Arpanet Was Built", [Annals of the History of Computing, IEEE](http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=85), Volume:33 Issue:3, 2011 [↑](#footnote-ref-2)
2. ÇAĞILTAY, Kürşat, *Herkes için İnternet, Metu Press,* ANKARA, 1997, s.*3* [↑](#footnote-ref-3)
3. ŞAHİN Mustafa, "IPv6 Sistem Geçişi" Yüksek lisans tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006, s.4 [↑](#footnote-ref-4)
4. HAGEN, Silvia IPv6 Essentials, Second Edition, O’Reilly Media inc., Sebastopol, 2006 [↑](#footnote-ref-5)
5. LAMMLE, Todd, *CCNA: Cisco Certified Network Associate Study Guide: Exam 640-802, 6th Edition*, wiley pub.,indianapolis, 2007, s.9 [↑](#footnote-ref-6)
6. DAY, John, ZIMMERMANN Hubert, "The OSI Reference Model", **Proceedings Of IEEE,** VOL. 71, NO. 12, 1983 [↑](#footnote-ref-7)
7. LIU, Dale, [*Next Generation SSH2 Implementation*](http://www.sciencedirect.com/science/book/9781597492836)*, Securing Data in Motion,* Elsevier Inc., 2008, s.22 [↑](#footnote-ref-8)
8. LIU, Dale, [*Next Generation SSH2 Implementation*](http://www.sciencedirect.com/science/book/9781597492836)*, Securing Data in Motion,* Elsevier Inc., 2008, s.20 [↑](#footnote-ref-9)
9. ŞAHİN Mustafa, "IPv6 Sistem Geçişi" Yüksek lisans tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006, s.8 [↑](#footnote-ref-10)
10. LIU, Dale, [*Next Generation SSH2 Implementation*](http://www.sciencedirect.com/science/book/9781597492836)*, Securing Data in Motion,* Elsevier Inc., 2008, s.17 [↑](#footnote-ref-11)
11. LAMMLE, Todd, *CCNA: Cisco Certified Network Associate Study Guide: Exam 640-802, 6th Edition*, wiley pub.,indianapolis, 2007, s.54 [↑](#footnote-ref-12)
12. ŞAHİN Mustafa, "IPv6 Sistem Geçişi" Yüksek lisans tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006, s.10 [↑](#footnote-ref-13)
13. LAMMLE, Todd, *CCNA: Cisco Certified Network Associate Study Guide: Exam 640-802, 6th Edition*, wiley pub.,indianapolis, 2007, s.65 [↑](#footnote-ref-14)
14. RFC 791, "IP Protocol" **IETF RFC Belgesi**, 1981 [↑](#footnote-ref-15)
15. RFC 792, Internet Control Message Protocol, **IETF RFC Belgesi,** 1981 [↑](#footnote-ref-16)
16. RFC 826, An Ethernet Address Resolution Protocol, **IETF RFC Belgesi,** 1982 [↑](#footnote-ref-17)
17. ŞAHİN Mustafa, "IPv6 Sistem Geçişi" Yüksek lisans tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006, s.13 [↑](#footnote-ref-18)
18. Address, Protocols And Ports, http://www.cisco.com/en/US/docs/security/asdm/6\_2f/user/guide/ref\_ports.html#wp1007738 [↑](#footnote-ref-19)
19. Address, Protocols And Ports, http://www.cisco.com/en/US/docs/security/asdm/6\_2f/user/guide/ref\_ports.html#wp1007738 [↑](#footnote-ref-20)
20. Unicast, Multicast And Broadcast Definitions, http://www.hp.com/rnd/device\_help/help/hpwnd/webhelp/HPJ3288A/uni\_multi\_broadcast.htm [↑](#footnote-ref-21)
21. ODOM, Wendell, *CCNA ICND1 640-822 Official Cert Guide Third Edition,* Cisco press., Indianapolis, 2012, s.113 [↑](#footnote-ref-22)
22. LAMMLE, Todd, *CCNA: Cisco Certified Network Associate Study Guide: Exam 640-802, 6th Edition*, wiley pub.,indianapolis, 2007, s.89 [↑](#footnote-ref-23)
23. ODOM, Wendell, *CCNA ICND1 640-822 Official Cert Guide Third Edition,* Cisco press., Indianapolis, 2012, s.553 [↑](#footnote-ref-24)
24. LAMMLE, Todd, *CCNA: Cisco Certified Network Associate Study Guide: Exam 640-802, 6th Edition*, wiley pub.,indianapolis, 2007, s.566 [↑](#footnote-ref-25)
25. ŞAHİN Mustafa, "IPv6 Sistem Geçişi" Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006, s.2 [↑](#footnote-ref-26)
26. http://www.internetworldstats.com/stats.htm [↑](#footnote-ref-27)
27. BOLAT, Ayşegül, "Mobil IP: Mevcut Düzenlemeler Ve Türkiye Önerileri", Uzmanlık Tezi, Telekominikasyon Kurumu, ANKARA, 2004, s.38 [↑](#footnote-ref-28)
28. LAMMLE, Todd, *CCNA: Cisco Certified Network Associate Study Guide: Exam 640-802, 6th Edition*, wiley pub.,indianapolis, 2007, s.517 [↑](#footnote-ref-29)
29. C. Bouras, A. Karaliotas, P. Ganos, "The Deploymet Of IPV6 In An IPV4 World And Transition Strategies" **Internet Research: Emeral Article,** Vol. 13 Iss: 2 pp. 86 - 93 [↑](#footnote-ref-30)
30. http://www.iana.org/numbers [↑](#footnote-ref-31)
31. AKTAŞ, Mahire, SAĞIROĞLU, Şeref, "IPv6:Uluslararası Çalışmalar Ve Türkiye’de Durum" **Ulusal IPV6 Konferansı**, ANKARA, 2011 [↑](#footnote-ref-32)
32. http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml [↑](#footnote-ref-33)
33. http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8 [↑](#footnote-ref-34)
34. https://www.ripe.net/internet-coordination/ipv4-exhaustion/ipv4-available-pool-graph [↑](#footnote-ref-35)
35. https://labs.ripe.net/statistics/total-ipv6-allocations [↑](#footnote-ref-36)
36. BOLAT, Ayşegül, "Mobil IP: Mevcut Düzenlemeler Ve Türkiye Önerileri", Uzmanlık Tezi, Telekominikasyon Kurumu, ANKARA, 2004, s.38 [↑](#footnote-ref-37)
37. SAILAN, Mohd. Khairil Ve Diğerleri, "A Comparative Review of IPv4 and IPv6 for Research Test Bed", **International Conference on Electrical Engineering and Informatics,** Selangor, Malaysia, 2009 [↑](#footnote-ref-38)
38. Kamu Kurum Ve Kuruluşları İçin IPV6'ya Geçiş Planı Konulu Başbakanlık Genelgesi, http://www.resmigazete.gov.tr/eskiler/2010/12/20101208-7.htm [↑](#footnote-ref-39)
39. ŞAHİN Mustafa, "IPv6 Sistem Geçişi" Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006, s.19 [↑](#footnote-ref-40)
40. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, Tübitak, Ulakbim, 2012, s.6 [↑](#footnote-ref-41)
41. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, Tübitak, Ulakbim, 2012, s.7 [↑](#footnote-ref-42)
42. BROWN, Sam Ve Diğerleri, *Configuring IPv6 for Cisco IOS*, Elsevier Inc., USA, 2002, s.127 [↑](#footnote-ref-43)
43. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, Tübitak, Ulakbim, 2012, s.6 [↑](#footnote-ref-44)
44. ŞAHİN Mustafa, "IPv6 Sistem Geçişi" Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006, s.19 [↑](#footnote-ref-45)
45. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, **Tübitak, Ulakbim**, 2012, s.10 [↑](#footnote-ref-46)
46. HINDEN, R., Haberman, B., “Unique Local IPv6 Unicast Addresses”, **IETF RFC Belgesi,** 2005 [↑](#footnote-ref-47)
47. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, **Tübitak, Ulakbim**, 2012, s.8 [↑](#footnote-ref-48)
48. GORALSKI, Walter, *How To TCP/IP Works In A Modern Network*, Elsevier Inc., USA, 2009, s.182 [↑](#footnote-ref-49)
49. Introduction to IP Version 6, **Microsoft White Paper**, 2008, http://technet.microsoft.com/en-us/library/bb726944.aspx [↑](#footnote-ref-50)
50. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, Tübitak, Ulakbim, 2012, s.11 [↑](#footnote-ref-51)
51. SAILAN, Mohd. Khairil Ve Diğerleri, "A Comparative Review of IPv4 and IPv6 for Research Test Bed", **International Conference on Electrical Engineering and Informatics,** Selangor, Malaysia, 2009 [↑](#footnote-ref-52)
52. GOVIL Jivika Ve Diğerleri, "An Examination of IPv4 and IPv6 Networks : Constraints and Various Transition Mechanisms", **IEEE Conference Publications**, Southeastcon, 2008, p.178-185 [↑](#footnote-ref-53)
53. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, Tübitak, Ulakbim, 2012, s.44 [↑](#footnote-ref-54)
54. ŞAHİN Mustafa, "IPv6 Sistem Geçişi" Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006, s.31 [↑](#footnote-ref-55)
55. Introduction to IP Version 6, **Microsoft White Paper, 2008**, http://technet.microsoft.com/en-us/library/bb726944.aspx [↑](#footnote-ref-56)
56. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, Tübitak, Ulakbim, 2012, s.18 [↑](#footnote-ref-57)
57. Introduction to IP Version 6, **Microsoft White Paper**, 2008, http://technet.microsoft.com/en-us/library/bb726944.aspx [↑](#footnote-ref-58)
58. SAILAN, Mohd. Khairil Ve Diğerleri, "A Comparative Review of IPv4 and IPv6 for Research Test Bed", **International Conference on Electrical Engineering and Informatics,** Selangor, Malaysia, 2009 [↑](#footnote-ref-59)
59. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, Tübitak, Ulakbim, 2012, s.22 [↑](#footnote-ref-60)
60. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, Tübitak, Ulakbim, 2012, s.31-32 [↑](#footnote-ref-61)
61. BOLAT, Ayşegül, "Mobil IP: Mevcut Düzenlemeler Ve Türkiye Önerileri", Uzmanlık Tezi, Telekominikasyon Kurumu, ANKARA, 2004, s.38 [↑](#footnote-ref-62)
62. YÜCE Emre, "IPV4, IPV6 Ve IPV6 Geçiş Yöntemleri Performans Karşılaştırmaları", **Ulusal IPV6 konferansı,** ANKARA, 2011 [↑](#footnote-ref-63)
63. The Seoul Decleration For The Future Of The Internet Economy, 2008, http://www.oecd.org/internet/consumer/40839436.pdf [↑](#footnote-ref-64)
64. BEKTAŞ, Onur Ve Diğerleri, "Türkiye İçin IPV6 Geçişi Zaman/Aşama Planı Önerisi" **Ulusal IPV6 Konferansı**, ANKARA, 2011 [↑](#footnote-ref-65)
65. ERDOĞAN, Kenan, AKÇAM, Nursel, "IPV4'ten IPV6'ya Geçiş Süreci İçin Bütünsel Bir Yaklaşım" **EMO 2. Ağ Ve Bilgi Güvenliği Ulusal Sempozyumu Bildirileri,** 2008 [↑](#footnote-ref-66)
66. R. Gilligan, E. Nordmark, "Basic Transition Mechanisms for IPv6 Hosts and Routers", IETF RFC Belgesi, RFC 4213, 2005 [↑](#footnote-ref-67)
67. CHANG, Fangzhe, WADDINGTON, Daniel G., " Realizing the Transition to IPv6", **IEEE Communications Magazine**, Volume:40, Issue:6, 2002, s. 138-147 [↑](#footnote-ref-68)
68. MCFARLAND, Shannon Ve Diğerleri, *ipv6 for enterprise networks,* cisco press, INDIANAPOLIS, 2012, s.48-49 [↑](#footnote-ref-69)
69. "internet address space: Economic Considerations in the management of IPV4 and in the deployment of IPV6", **OECD Ministerial Meeting On The Future Of The Internet Economy Background Report,** Seoul, 2008 [↑](#footnote-ref-70)
70. DUNN,Tricia, "The IPV6 Transition", **Internet Computing, IEEE, Volume:6, Issue:3**, 2002, s.11-13 [↑](#footnote-ref-71)
71. MCFARLAND, Shannon Ve Diğerleri, *ipv6 for enterprise networks,* cisco press, INDIANAPOLIS, 2012, s.51 [↑](#footnote-ref-72)
72. MCFARLAND, Shannon Ve Diğerleri, *ipv6 for enterprise networks,* cisco press, INDIANAPOLIS, 2012, s.55 [↑](#footnote-ref-73)
73. CHANG, Fangzhe, WADDINGTON, Daniel G., " Realizing the Transition to IPv6", **IEEE Communications Magazine**, Volume:40, Issue:6, 2002, s. 138-147 [↑](#footnote-ref-74)
74. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, Tübitak, Ulakbim, 2012, s.55 [↑](#footnote-ref-75)
75. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, Tübitak, Ulakbim, 2012, s.55-56 [↑](#footnote-ref-76)
76. MCFARLAND, Shannon Ve Diğerleri, *ipv6 for enterprise networks,* cisco press, INDIANAPOLIS, 2012, s.57 [↑](#footnote-ref-77)
77. ŞAHİN Mustafa, "IPv6 Sistem Geçişi" Yüksek lisans tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006,s.61 [↑](#footnote-ref-78)
78. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, **Tübitak, Ulakbim**, 2012, s.61 [↑](#footnote-ref-79)
79. ÇALIŞKAN, Beyhan Kaan Ve Diğerleri, *IPV6 El Kitabı V2.1*, **Tübitak, Ulakbim**, 2012, s.61 [↑](#footnote-ref-80)
80. DUNN,Tricia, "The IPV6 Transition", **Internet Computing, IEEE, Volume:6, Issue:3**, 2002, s.11-13 [↑](#footnote-ref-81)
81. MURPHY, Alan, "Managing IPv6 Throughout The Application Delivery Network", **F5 White Paper**, http://www.f5.com/pdf/white-papers/ipv6-wp.pdf [↑](#footnote-ref-82)