
**BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ**
**Fen Bilimleri Enstitüsü**
**Bilgisayar Mühendisliği Anabilim Dalı**

# IPV4 VE IPV6 İNTERNET PROTOKOL SÜRÜMLERİNDE SES TAŞIMA ANALİZİ VE UYGULAMASI

**Murat ÖZALP**
**Yüksek Lisans Tezi**

**Tez Danışmanı**
**Prof. Dr. Kırali MÜRTEZAOĞLU**

**BİLECİK, 2014**

**Ref No: 10046235**


**BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ**
**Fen Bilimleri Enstitüsü**
**Bilgisayar Mühendisliği Anabilim Dalı**

# IPv4 ve IPv6 İNTERNET PROTOKOL SÜRÜMLERİNDE SES TAŞIMA ANALİZİ VE UYGULAMASI

**Murat ÖZALP**
**Yüksek Lisans Tezi**

**Tez Danışmanı**
**Prof. Dr. Kırali MÜRTEZAOĞLU**

**BİLECİK, 2014**


**BILECIK SEYH EDEBALI UNIVERSITY**
**Graduate School of Sciences**
**Department of Computer Engineering**

# VOICE TRANSPORT ANALYSIS AND APPLICATION ON IPV4 AND IPV6 INTERNET PROTOCOL VERSIONS

**Murat ÖZALP**
**Master's Thesis**

**Thesis Advisor**
**Prof. Dr. Kırali MÜRTEZAOĞLU**

**BİLECİK, 2014**

| BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ | YÜKSEK LİSANS<br>**JÜRİ ONAY FORMU** |
|---|---|

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ..... tarih ve ..... sayılı kararıyla oluşturulan jüri tarafından 25.06.2014 tarihinde tez savunma sınavı yapılan Murat ÖZALP' ın "IPv4 VE IPv6 İNTERNET PROTOKOL SÜRÜMLERİNDE SES TAŞIMA ANALİZİ VE UYGULAMASI " başlıklı tez çalışması Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak oy birliği/oy çokluğu ile kabul edilmiştir.

**JÜRİ**

**ÜYE (TEZ DANIŞMANI): Prof. Dr. Kırali MÜRTEZAOĞLU**

**ÜYE: Doç. Dr. Cihan KARAKUZU**

**ÜYE: Doç. Dr. Mehmet KURBAN**

**ONAY**

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun .../.../..... tarih ve ...../..... sayılı kararı.

İMZA MÜHÜR

# TEŞEKKÜR

Bu çalışmanın yürütülmesi sırasında desteğini esirgemeyen danışmanım Prof. Dr. Kırali Mürtezaoğlu'na, yoğun çalışmalarım sırasında sabır gösterdiği ve bana katlandığı için eşim Nigar'a, sürekli çalışmama izin verdiği için küçük kızlarım Ayşe ve Sare'ye, motivasyon desteği için Şakir'e, çalışmalarım sırasında ümit verdiği ve destek olduğu için Bilecik Şeyh Edebali Üniversitesi Bilgi İşlem Daire Başkanlığı'nda çalışan iş arkadaşlarıma ve özellikle gerekli tüm kolaylıkları gösteren Daire Başkanı Murat Fidan'a, sağladığı mükemmel çalışma ortamı ve manevi destek nedeniyle Yusuf Muştu'ya, istatistik hesapları konusunda destek veren Yrd. Doç. Dr. Serpil Türkyılmaz'a ve Uzman Burakhan Çubukçu'ya, Mühendislik Fakültesi'nde öğretim üyesi olan Yrd. Doç. Dr. Uğur Yüzgeç ile Doç. Dr. Cihan Karakuzu'ya, yazım kuralları denetimi konusunda yardımı için Alpaslan Ersöz'e ve çalışmam sırasında küçük veya büyük yardımını esirgemeyen herkese teşekkür ederim.

**Murat ÖZALP**

**Temmuz–2014**

# ÖZET

Ağ üzerinden farklı cihazların birbirleri ile haberleşebilmesi için "protokol" adı verilen ortak bir dile ihtiyaç vardır. Dünyanın en büyük ağı olan İnternet'te kullanılan protokole "Internet Protokolü (IP)" denmektedir. IP kullanan her cihazın kendine özel olan tanımlayıcısına, "IP adresi" denir. İnternet'in hızla büyümesi neticesinde, IP sürüm 4'te (IPv4) kullanılabilen adresler tükenmiştir. Küresel IP dağıtıcısı, elindeki son IP bloklarını 2011 yılında bölgesel IP dağıtıcılarına teslim etmiştir. 1996 yılında resmen duyurulmuş olan yeni sürüm IP (IPv6) artık seçimlik değil zorunlu durumdadır. Geçiş sürecinde; iki protokol beraber çalıştırılmaktadır. Bu nedenle, IPv4'te sürdürülmekte olan hizmetlerin IPv6 üzerinde yeniden uygulanması ve denenmesi gerekmektedir.

IP üzerinden ses taşıma (VoIP) uygulaması, günümüzde çok yaygın kullanılmaktadır. Bu çalışmada IPv6 geçişine VoIP penceresinden bakılmış; olası problemler ve performans farklarını görebilmek için uygulama ve analizler yapılmıştır. Öncelikle IP'nin iki sürümünü de çalıştıran bir ağ kurulmuş ve çok sayıda eşzamanlı VoIP çağrısı ile zorlama testleri yapılmıştır. Testler sonucunda; iki protokolün performansının birbirine çok yakın olduğu, test ortamındaki asıl darboğazın ise bilgisayarların donanım kaynakları olduğu görülmüştür. Baştan öngörülemeyen bu kısıt nedeniyle, laboratuvar ortamı yeniden düzenlenmiştir.

Yeniden düzenlenen test ortamında; iletim kapasitesi ve hizmet kalitesi açısından, uzak alan ağlarına (WAN) benzetilen bir ağ tasarlanmıştır. Bu ağ üzerinde hattın %44,5 ve %85,5 doluluk oranlarında, IPv4 ve IPv6 üzerinden yapılan sesli çağrıların trafik verileri incelenmiştir. Analizler sonucunda; özellikle ağdaki trafik yükünün az olduğu durumda, kayıp paketler ve gecikme açısından IPv4 ve IPv6 arasında kayda değer bir fark olmadığı (*%1'den daha az*) görülmüştür. Bu tez kapsamında yapılan çalışma neticesinde elde edilen bulguların önceki çalışmalarla uygun olduğu gözlenmiştir.

**Anahtar sözcükler:** İnternet Protokolü, IP, IPv6, VoIP

# ABSTRACT

To communicating network devices with each other, a common language is required which is called protocol. The world's largest network is the “Internet” and the protocol used on the Internet is called as “Internet Protocol (IP)”. Every device on the Internet has a unique IP address. As a result of the rapid growth of the Internet, IP version 4 (IPv4) addresses that can be used has been exhausted. Global IP authority gave the last IP blocks to regional authorities in 2011. New version of IP (IPv6) which is officially announced in 1996 is no longer optional but is on mandatory status. During the transition period; both protocols will be used. Therefore, the services and applications used in IPv4 should be retested on IPv6 network.

Voice-over-IP (VoIP) applications are widely used nowadays. In this study we have examined IPv6 transition and especially about VoIP. We have made test and analysis in order to see differences in performance and possible problems. Firstly, a network that is running both versions of IP was established. Force tests were performed with multiple concurrent VoIP calls. As a result of the tests; the performance of two protocols were found to be very close together and the main bottleneck in the test environment was found to be the hardware resources of the computer. Due to those unpredictable constraints, the laboratory was reorganized.

In the new test lab; In terms of transmission capacity and quality of service, a network designed like WAN. Voice calls made over IPv4 and IPv6 traffic have been examined at occupancy rate of 44.5% and 85.5% of the network. As a result of analysis; lost packets and latency difference was insignificant between IPv4 and IPv6 (less than 1%) were observed, especially when the network traffic load is low. The findings of this study were found to be suitable with previous studies.

**Keywords:** Internet Protocol, IP, IPv6, VoIP

# İÇİNDEKİLER

**Sayfa No**

# ÇİZELGELER DİZİNİ

**Sayfa No**

# ŞEKİLLER DİZİNİ

**Sayfa No**

# SİMGELER VE KISALTMALAR DİZİNİ

| | |
|---|---|
| **ARP** | Address Resolution Protocol (Adres Çözümleme Protokolü) |
| **ARPANET** | Advanced Research Project Agency Network (İleri Araştırma Projeleri Ajansı) |
| **ASCII** | American Standard Code for Information Interchange (Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi) |
| **CBR** | Constant Bit Rate (Sabit Bit Oranı) |
| **CIDR** | Classless Inter Domain Routing (Alanlar Arası Sınıfsız Yönlendirme) |
| **CLI** | Command Line Interface (Komut Satırı Arabirimi) |
| **DHCP** | Dynamic Host Configuration Protocol (Dinamik İstemci Yapılandırma Protokolü) |
| **DNS** | Domain Name System (Alan Adı Sistemi) |
| **FQDN** | Fully Qualified Domain Name (Tümüyle Tanımlanan Alan Adı) |
| **GUI** | Graphical User Interface (Grafik Kullanıcı Arabirimi) |
| **HTML** | Hypertext Markup Language (Hiper Metin İşaret Dili) |
| **HTTP** | Hypertext Transfer Protocol (Hareketli Metin Taşıma Protokolü) |
| **IANA** | Internet Assigned Numbers Authority (İnternet Atanmış Numaralar Otoritesi) |
| **ICMP** | Internet Control Message Protocol (İnternet Denetim Mesaj Protokolü) |
| **IEEE** | Institute of Electrical and Electronics Engineers (Elektrik Elektronik Mühendisleri Enstitüsü) |
| **IETF** | Internet Engineering Task Force (İnternet Mühendislik Görev Gücü) |
| **IGMP** | Internet Group Management Protocol (İnternet Grup Yönetim Protokolü) |
| **IP** | Internet Protocol (İnternet Protokolü) |
| **IPSec** | Internet Protocol Security (İnternet Protokol Güvenliği) |
| **IPv4** | Internet Protocol version 4 (İnternet Protokolü Sürüm 4) |
| **IPv6** | Internet Protocol version 6 (İnternet Protokolü Sürüm 6) |
| **ISDN** | Integrated Services Digital Network (Bütünleşik Hizmetler Sayısal Ağı) |
| **ITU-T** | International Telecommunications Union, Telecommunication Standardization Sector (Uluslararası Telekomünikasyonlar Birliği, Telekomünikasyon Standartlaştırma Sektörü) |
| **IVR** | Interactive Voice Response (Etkileşimli Sesli Yanıt) |
| **İSS** | İnternet Servis Sağlayıcı |
| **LAN** | Local Area Network (Yerel Alan Ağı) |
| **LIR** | Local Internet Registry (Yerel İnternet Kayıtçısı) |
| **MAC** | Media Access Control (Medya Erişim Denetimi) |
| **MGCP** | Media Gateway Control Protocol (Medya Geçidi Denetim Protokolü) |
| **MILNET** | Military Network (Askeri Ağ) |
| **MLD** | Multicast Listener Discovery (Çokluyayın Dinleyici Keşfi) |

| | |
|---|---|
| **MMUSIC** | Multi-Party Multimedia Session Control Working Group (Çok Aboneli Çoklu Ortam Oturum Denetimi Çalışma Grubu) |
| **NAT** | Network Address Translation (Ağ Adres Dönüşümü) |
| **NTP** | Network Time Protocol (Ağ Zaman Protokolü) |
| **NVP** | Network Voice Protocol (Ağ Ses Protokolü) |
| **QoS** | Quality of Service (Hizmet Kalitesi) |
| **PBX** | Private Branch Exchange (Özel Telefon Santrali) |
| **PPS** | Packet Per Second (Saniyedeki Paket Sayısı) |
| **PSTN** | Public Switched Telephone Network (Genel Anahtarlamalı Telefon Şebekesi) |
| **RFC** | Request For Comments (Yorumlar İçin Talepler) |
| **RIPE** | Réseaux IP Européens (Avrupa IP Ağları) |
| **RIR** | Regional Internet Registry (Bölgesel İnternet Kayıtçısı) |
| **RTCP** | Real-Time Transfer Control Protocol (Gerçek Zamanlı Taşıma Denetim Protokolü) |
| **RTP** | Real-time Transport Protocol (Gerçek Zamanlı Taşıma Protokolü) |
| **S/MIME** | Secure/Multipurpose Internet Mail Extensions (Güvenli/Çok Amaçlı İnternet Posta Uzantıları) |
| **SDP** | Session Description Protocol (Oturum Tanımlama Protokolü) |
| **SIP** | Session Initiation Protocol (Oturum Başlatma Protokolü) |
| **SMTP** | Simple Mail Transfer Protocol (Basit Posta Gönderme Protokolü) |
| **SSH** | Secure Shell (Güvenli Kabuk) |
| **TCP** | Transmission Control Protocol (Aktarım Denetim Protokolü) |
| **TFTP** | Trivial File Transfer Protocol (Basit Dosya Transfer Protokolü) |
| **TLS** | Transport Layer Security (Taşıma Katmanı Güvenliği) |
| **TTL** | Time To Live (Yaşam Süresi) |
| **TÜBİTAK** | Türkiye Bilimsel ve Teknolojik Araştırma Kurumu |
| **UDP** | User Datagram Protocol (Kullanıcı Veri Bloğu Protokolü) |
| **ULAK6NET** | Ulusal Akademik IPv6 Ağı |
| **ULAKBİM** | Ulusal Akademik Ağ ve Bilgi Merkezi |
| **ULAKNET** | Ulusal Akademik Ağ |
| **URL** | Uniform Resource Locator (Tek Biçimli Kaynak Konumlandırıcısı) |
| **VBR** | Variable Bit Rate (Değişken Bit Oranı) |
| **VoIP** | Voice Over IP (IP Üzerinden Ses) |
| **WAN** | Wide Area Network (Geniş Alan Ağı) |

# 1. BÖLÜM: GİRİŞ

Ses ve video gibi verileri uzak mesafede bir yere ulaştırmak için en hızlı ve güvenli yol, günümüzde veri ağı şebekeleridir. Ev telefonu gibi analog sistemlerde, cep telefonu gibi mobil sistemlerde dahi, aboneden alınan ses sayısala çevrildikten sonra, uzak mesafelere İnternet Protokolü (IP) üzerinden aktarılmaktadır. Canlı ses iletiminin, veri şebekeleri üzerinden aktarılması, maliyeti düşürmektedir. İş yükü açısından bakıldığında ise klasik İnternet trafiğinin yanında, ses trafiği çok küçük kalmakta, dolayısıyla veri şebekelerine getireceği iş yükü ticari açıdan önemsenmemektedir.

Ses trafiğinin IP üzerinden aktarılması konusunda yıllardır hem akademik hem de ticari anlamda çok fazla çalışma yapılmıştır. Çok sayıda ticari kuruluş, veri şebekesi üzerinden ses taşıma hizmetini müşterilerine sunmaktadır. Benzer şekilde bireysel ve kurumsal anlamda IP üzerinden ses taşıma (VoIP) teknolojileri oturmuş durumdadır. Ancak IP'nin yeni sürümünün (IPv6) çıkmış olması nedeniyle, IPv4 üzerinde çalıştırılan uygulamaların, sürdürülen hizmetlerin IPv6 üzerinde yeniden uygulanması ve denenmesi gerekmektedir. IPv6'nın iddialarından birisi, IP üzerinden ses taşıma işlemlerinin daha kolay ve kaliteli yapılmasıdır. Bu nedenle, IPv6 üzerinde ses taşıma konusunda çalışma yapılması tercih edilmiştir.

Çalışmanın birinci bölümünde, bu çalışmanın ortaya çıkışını sağlayan amaçlar ve çalışmada varılmak istenen sonuç hakkında bilgi verilmiştir.

İkinci ve üçüncü bölümlerde, İnternet Protokolü'nün tarihçesi hakkında bilgi verilmiş, IPv4 ve IPv6 hakkında bir inceleme yapılmıştır. Daha sonra, SIP ile ilgili yapılan literatür taraması çalışmasının sonuçları aktarılmıştır.

Dördüncü bölümde; uygulama için ikili yığın sistemi ile hem IPv6 hem de IPv4 çalıştıran bir ağ oluşturulmuş, bu ağ üzerinde IPv6 destekli bir SIP sunucu ve iki tane SIP istemci kurulumu yapılmıştır. SIP istemciler arasında her iki protokol üzerinden ses haberleşmesi yapılmıştır. Bu şekilde, IPv6 üzerinden SIP haberleşmesi için sunucu-istemci mimarisinde çalışan örnek bir uygulama ortamı oluşturulmuştur. Daha sonra bu ortam üzerinde SIP zorlama testleri yapılmış ve elde edilen veriler paylaşılmıştır.

Beşinci bölümde, uzak mesafe ağ bağlantısı koşulları laboratuvar ortamında oluşturulmaya çalışılmıştır. Belirlenen ağ kısıtlarına göre, altı tane bilgisayar ve iki tane ağ anahtarı kullanılarak tasarlanan laboratuvar ortamında IPv4 ve IPv6 iletim ortamlarında bant genişliğinin, ses aktarımına etkisini ölçmeye yönelik çalışmalar yapılmıştır. Laboratuvarda yapılan testler sonrasında elde edilen veriler işlenmiş, verilerden grafikler oluşturulmuş ve verilerden çıkarılan bulgular paylaşılmıştır.

Son bölümde, uygulama sonucunda elde edilen bulgular yorumlanmış; IPv6 ağı üzerinde alınan sonuçlar, IPv4 ağında alınan sonuçlarla karşılaştırılmıştır. Son olarak, bu konu üzerinde çalışmak isteyenler için öneriler paylaşılmıştır.

# 2. BÖLÜM: İNTERNET PROTOKOLÜ

## 2.1 İnternet Protokolü

Kısaca IP olarak isimlendirilen ve 791 numaralı RFC[1] (Request for Comments ~ Yorumlar İçin Talep) belgesinde tanımlanmış olan İnternet Protokolü, 1981 yılında geliştirilmiştir. Günümüze kadar kullanılmış olan IP'nin 4. sürümünden (IPv4) önce üç farklı sürüm üzerinde daha çalışılmış, ancak önceki sürümler yaygınlaşamamıştır. 1992 yılına kadar sadece IPv4 sürümü kullanılmış, ancak yıllar önce tanımlanmış olan bu sürümün yetersiz kalacağı düşüncesiyle, 1993 yılında yeni bir IP sürümü çalışması başlamıştır. Bu sürüme IPv6 adı verilmiştir.

Dünyada internetin yaygınlaşması da yaklaşık olarak IPv6 çalışmalarının başladığı yıllara tekabül etmektedir. İnternetin temelleri ilk tasarlandığı zaman, bu kadar büyüyeceği tahmin edilemediğinden, IPv4'ün tüm ihtiyaçları uzun süre karşılayacağı planlanmaktaydı. Ancak İnternet'in öngörülemez bir hızda büyümeye başlaması neticesinde, IPv4'ün gelecek olan ihtiyaçları karşılayamayacak olduğunun farkına varılması, IPv6 çalışmalarının da başlangıcına ışık tutmuştur.

İnternet Protokolü, günümüzde İnternet'in ortak dili halini almıştır. İnternet'e bağlanmak isteyen tüm bilgisayar ve cihazlar IP kullanmaktadır. Bu şekilde İnternet, mekândan ve katılımcı cihazların fiziksel özelliklerden bağımsız, günden güne hızla büyüyen bir ağ haline gelmiştir. IP'nin bu kadar yaygınlaşması ve esnek olması, IP'yi sadece bilgisayar haberleşmesi protokolü olmaktan çıkarmış, bilgisayarlar haricinde farklı sistemlerin de IP üzerinden haberleşebilir hale gelmesini sağlamıştır. Günümüzde telefon sistemleri, video konferans, GSM şebekeleri ve cihazları, güvenlik kamerası, yangın algılama, geçiş kontrol, anons ve benzeri birçok sistem IP üzerinden haberleşebilmektedir. Bu tarz sistemlerin sayısı günden güne artmaktadır.

IP üzerinden çalışan sistemlerin sayısı arttıkça, IPv4'ün eksiklikleri ve kısıtlamaları daha da hissedilir hale gelmiştir. Özellikle IP adres sayısının yetersiz

[1] RFC: Request For Comments. IETF tarafından; protokoller, davranışlar, araştırmalar ve yenilikler ile ilgili çıkarılan yayınlardır.

olması ve bu nedenle NAT (Network Address Translation ~ Ağ Adres Dönüşümü) türü uygulamalara ihtiyaç olması, temel sorundur. NAT uygulaması, kurumlara tahsis edilmiş olan IP adreslerinin, ağda kullanılan tüm cihazlar için yetersiz olduğu durumlar için geliştirilmiş bir yamadır. NAT kullanımında, iç ağında sanal IP adresleri kullanan kurumlardaki cihazlar, İnternet üzerinden iletişim kuracağı zaman kuruma tahsis edilmiş olan gerçek IP adresi havuzundan bir gerçek IP adresi alarak, İnternet iletişimini gerçekleştirir ve işi bittiğinde kullandığı gerçek IP adresini yeniden havuza bırakır. İç ağda ise tamamen sanal IP adresleri kullanılarak iletişim sağlanır.

### 2.1.1 İnternet Protokolü'nde sürüm numaraları

İnternet Protokolünde, her paketin başlığında 4 bitlik bir alanda IP sürümü yazmaktadır. Örneğin, IPv4'sürüm alanında ikilik sistemde "0100" (onluk sistemde karşılığı: "4") yazmaktadır. IPv6'dan daha önce, 1990 yılında RFC 1190 ile tanımlanmış olan "Experimental Internet Stream Protocol, Version 2" (Deneysel İnternet Akış Protokolü Sürüm 2), IP paket başlığındaki sürüm alanına ikilik sistemde "0101" (onluk sistemde karşılığı: "5") yazılacak şekilde tasarlanmıştır. Bu protokol aslında IPv4'ün bir üst sürümü değildir, günümüzde de kullanılmamaktadır. Fakat ikilik 0101 değeri daha önce kullanıldığından, karışıklık olmaması için farklı bir protokolde de aynı değerin kullanılmaması tercih edilmiştir. İnternet protokolünün yeni sürümüne de bir sonraki kullanılabilecek olan sayı yani "0110" (onluk sistemde karşılığı: "6") kalmıştır.

IP'ye ait 4'ten önceki sürümler de asla var olmamıştır. Sürümün doğrudan 4'ten başlamasının sebebi; IP'nin 4. sürümünde, önceden bir arada olan TCP (Transmission Control Protocol ~ Aktarım Denetim Protokolü) ve IP bileşenlerine ayrılmasıdır. Önceki sürümler de aslında TCP'ye ait sürümlerdir.

Kısacası, İnternet Protokolü'nün iki tane sürümü vardır. İlk sürümü 4'tür, son sürümü de 6'dır. IPv1, IPv2, IPv3 ve IPv5 adlarında gerçek anlamda bir İnternet Protokolü hiçbir zaman olmamıştır (Lawrence, 2010).

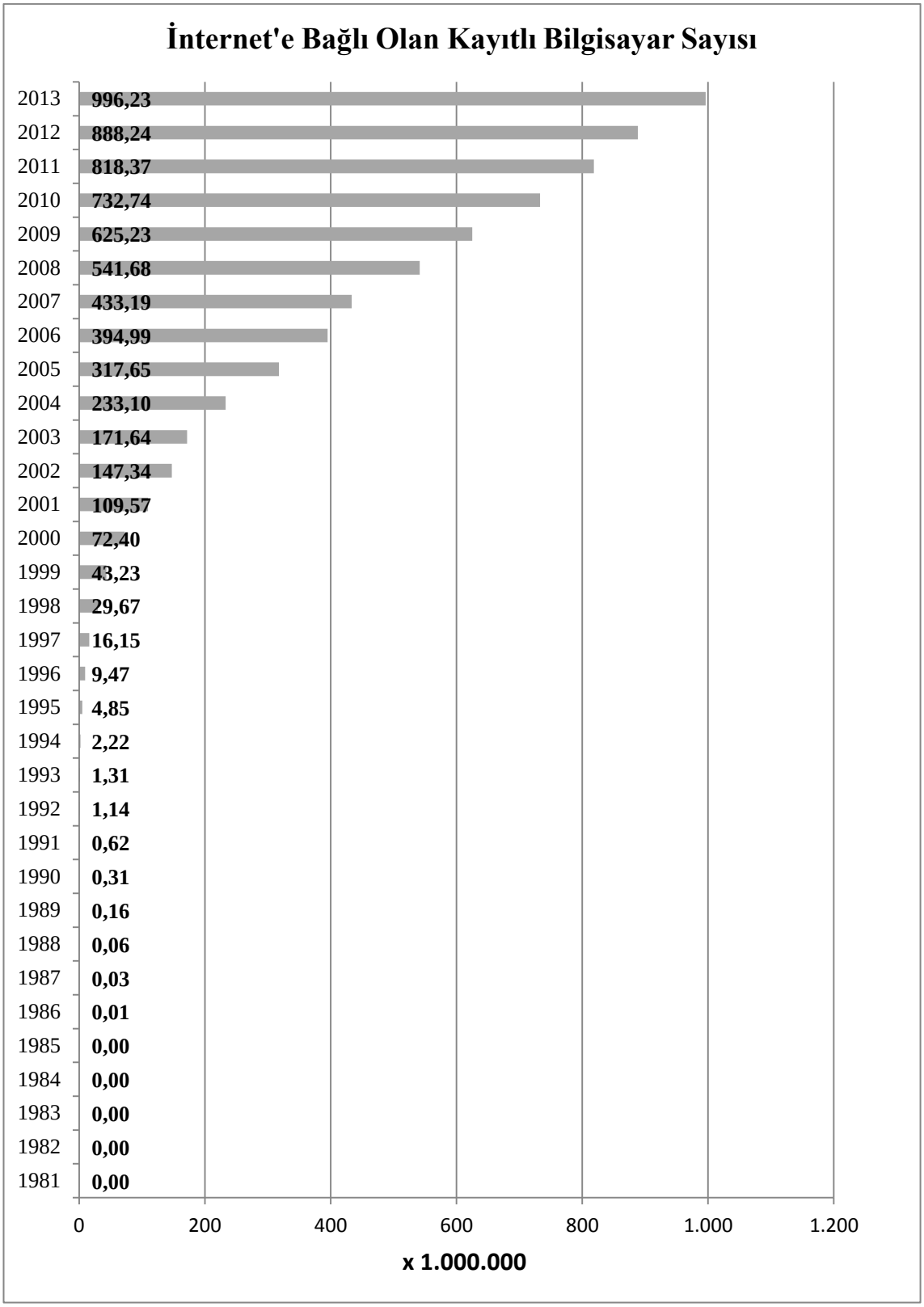
### 2.1.2 İnternet Protokolü'nün tarihçesi

İnternet'in gelişmesine bakıldığında, IP'den çok daha önce de farklı ağ uygulamaları görülmektedir. İlk bilgisayar ağı uygulamaları 1950-1960'lı yıllarda noktadan noktaya bağlantı şeklinde bilgisayarın gelişimine kadar gitmektedir. Paket anahtarlamalı ağlar ise 1960'ların sonu ve 1970'lerin başından itibaren başlamıştır. Uzak mesafe ağların birbirine bağlanması konusunda en büyük çalışmalar ABD (Amerika Birleşik Devletleri) Savunma Bakanlığı'na bağlı olan ARPANET (Advanced Research Project Agency Network ~ İleri Araştırma Projeleri Ajansı Ağı) sayesinde yapılmıştır.

Paket anahtarlamadan önce devre anahtarlama kullanılmaktaydı. Devre anahtarlamalı iletişimde, telefon görüşmesinde olduğu gibi iletişim bitene kadar iki ucun da başka uçlar ile iletişime geçmesi olanaksızdı. Paket anahtarlama yöntemi ise; bir sistemin tek bir iletişim hattı kullanarak birden çok makineyle haberleşebilmesi için verinin küçük parçalara ayrılıp bu parçaların daha sonra paketler halinde düzenlenmesi esasına dayanmaktadır. Bu açıdan bakıldığında İnternet'in atası olarak ARPANET gösterilmektedir.

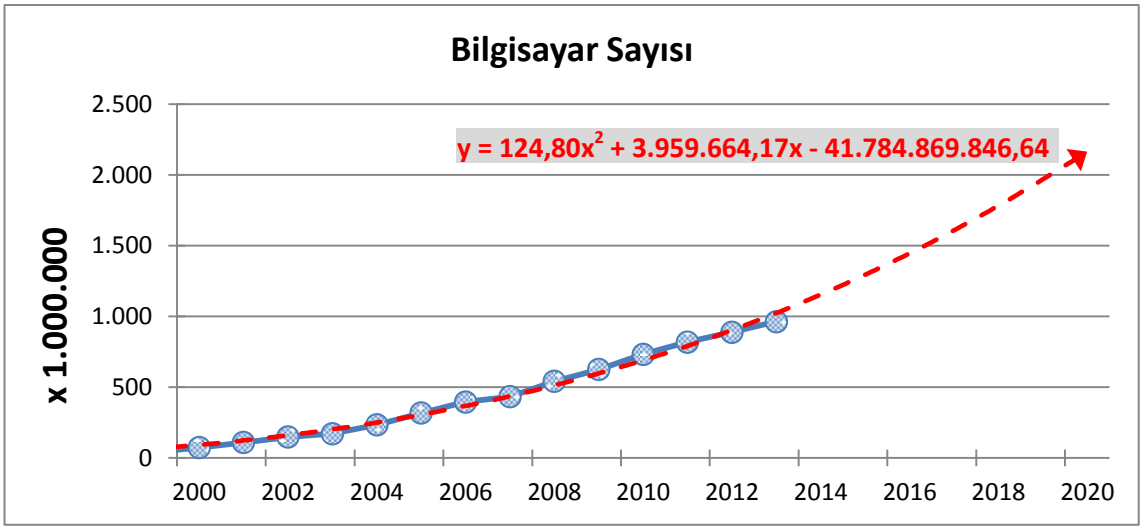
İnternet'in ortak dili olan İnternet Protokolü; farklı yerlerde bulunan farklı tipte cihazların da ağ üzerinden iletişim sağlayabilmesini amaçlayan standart bir protokol olarak geliştirilmiş ve IETF (Internet Engineering Task Force ~ İnternet Mühendislik Görev Gücü) tarafından ilk belgesi Ocak 1980'de RFC 760 numarası ile yayınlanmıştır. Daha sonra, Eylül 1981'de RFC 791 ile yeniden tanımlanarak standart hale gelmiştir.

Şekil 2.1'de, İnternet'in başlangıcından bu yana internet üzerindeki kayıtlı (DNS üzerinden anons edilen) bilgisayar sayıları gösterilmiştir (http://www.isc.org/solutions/survey/history, 19.07.2014).




**Şekil 2.1.**Yıllara göre İnternet üzerindeki kayıtlı bilgisayar sayıları.

Şekil 2.1'de gösterilmiş olan grafikteki veriler, Microsoft Excel 2010™ programında işlenerek 2020 yılına kadar olan tahmini sayılar elde edilmiş ve bu sayıların grafiği Şekil 2.2'de gösterilmiştir. Artışın bu oranla devam etmesi durumunda, 2020 yılında, İnternet'e bağlı cihaz sayısının 2 milyarı geçeceği öngörülmektedir.




**Şekil 2.2.** İnternet'e bağlı olan cihaz sayılarının 2020 yılına kadar tahminleri.

İnternet'in Türkiye'de ve dünyadaki tarihsel gelişim süreci aşağıda özetlenmiştir (Leiner vd., 2009), (http://www.ipv6.net.tr/, Ocak 2014):

- **1971** Ray Tomlinson, ağ üzerinden ilk e-postayı gönderdi.
- **1972** Kaliforniya Üniversitesi'nde iki bilgisayar arasında ilk "sohbet" yapıldı.
- **1973** FTP protokolünün teknik ayrıntıları tanımlandı. Bu, internet üzerinde halen dosya aktarım için kullanılan protokolün ortaya çıkışıdır.
- **1977** Bir ağ ses protokolü olan NVP (Network Voice Protocol ~ Ağ Ses Protokolü), RFC 741 ile yayınlandı. Ancak ARPANET üzerinden yapılan ses görüşme denemeleri teknik nedenlerle başarılı olamadı. Uzun süre ağ üzerinden ses taşıma işlemi başarılamadı.
- **1983** ARPANET altyapısında IP kullanmaya başladı ve ARPANET içerisindeki ordu ile ilgili olan kısım MILNET (Military Network ~ Askeri Ağ) adı altında bu ağdan ayrılarak farklı bir ağa taşındı.
- **1985** 15 Mart'ta "symbolics.com" ismi, kayıt edilmiş ilk alan adı oldu.
- **1992** İnternet üzerindeki cihaz sayısı 1.000.000'u aştı.

- **1992** IETF, yeni nesil IP için öneri istedi.
- **1993** Mosaic web tarayıcı programı geliştirildi.
- **1993** Türkiye'nin ilk İnternet bağlantısı ODTÜ üzerinden 64Kb/s ile sağlandı.
- **1994** Tam metin web arama motorları geliştirildi.
- **1995** IETF IPv6'yı resmen duyurdu.
- **1999** IEEE (Institute of Electrical and Electronics Engineers ~ Elektrik Elektronik Mühendisleri Enstitüsü) 802.11b kablosuz ağ standardı yayınlandı.
- **2003** Türkiye'nin akademik ağı olan ve TÜBİTAK (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu) tarafından finanse edilen, TÜBİTAK'a bağlı bir enstitü olan ULAKBİM (Ulusal Akademik Ağ ve Bilgi Merkezi) tarafından yönetilen ULAKNET (Ulusal Akademik Ağ) isimli ağ, küresel IPv6 ağına Türkiye'den doğrudan bağlanan ilk ağ oldu.
- **2007:** 5651 sayılı "*İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun*" yayınlandı.
- **2010** "*Kamu Kurum ve Kuruluşları için IPv6'ya Geçiş Planı*" konulu, kamu kurum ve kuruluşlarının IPv6'ya geçiş süreçlerini 3 yıllık bir döneme yayan 27779 sayılı ve 08.12.2010 tarihli Başbakanlık Genelgesi yayınladı.
- **2011:** IP dağıtım yetkisini elinde bulunduran IANA (Internet Assigned Numbers Authority ~ İnternet Atanmış Numaralar Otoritesi), elindeki son 5 adet /8 IPv4 adreslerini[1] bölgesel internet kayıtçılarına verdi.
- **2011:** Türkiye'de 37 üniversite IPv6 ağına bağlı.
- **2012:** 27779 sayılı genelgenin 2. aşaması tamamlandı. (*IPv6 bağlantısı ve adresi temin eden kamu kurumları 31.12.2012 tarihine kadar internet üzerinden verdikleri en az bir hizmeti pilot olarak IPv6 destekli hale getireceklerdir.*)
- **2013:** 27779 sayılı genelgenin 3. aşaması tamamlandı. (*Kamu kurum ve kuruluşları en geç 31 Ağustos 2013 tarihine kadar internet üzerinden verdikleri kamuya açık tüm hizmetleri IPv6'yı destekler hale getireceklerdir.*)
- **2014 (Haziran):** Google'a IPv6 üzerinden gelen isteklerin oranı %4'ü buldu.

---

[1] /8 şeklindeki IP adres aralığı gösterimine CIDR (Classless Inter Domain Routing ~ Alanlar Arası Sınıfsız Yönlendirme) denmektedir. CIDR gösterimi hakkında detaylı bilgi, 2.2.1.1'de aktarılmıştır. Kısaca; /8 olarak ifade edilen IPv4 adres sayısı, teorik olarak 16.777.214 adettir. IPv4 adreslerindeki son üç oktet'in, aralığın tahsis edildiği kurumun kullanımına bırakılması durumudur. Bu tarz adres aralıklarına "A sınıfı IP adresi" de denmektedir.

## 2.2 İnternet Protokolü sürüm 4'e genel bakış

IPv4, 32 bitlik adresleme sistemi kullanmaktadır. Bu, teorik olarak 4 milyardan[1] fazla bilgisayarın adreslenebileceği anlamına gelmektedir. Ancak uygulamada hiçbir zaman bu hesap mümkün değildir. Protokolün tanımı gereği; bazı adresler özel adres, bazı adresler de çoklu yayın gibi amaçlar için ayrılmıştır. Diğer taraftan, 2.2.1 başlığında detaylandırılmış olan, IPv4'ün sınıflandırılmış adresleme yapısı nedeniyle bazı kurumlara ihtiyacından çok fazla IPv4 adresi tahsis edilmiştir. Bu nedenlerle, nicelik olarak çok fazla gibi görünen IPv4 adresleri günümüzde tükenmek üzeredir.

IP adresleri tahsis edilirken, erken başvuran ve maliyetini karşılayan kuruluşlara "/8" şeklinde ($2^{[32-8]}=2^{24}=16.777.216$) IP adresi tahsisi yapılmıştır. Çizelge 2.1'de A sınıfı IP adresi tahsis edilen bazı şirket ve kurumlar gösterilmiştir (www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml, Haziran 2014).

**Çizelge 2.1.** "/8" Şeklinde IPv4 adresi tahsis edilen bazı kurumlar.

| **Şirket** | **Tahsis tarihi** | **IPv4 adresleri** |
|---|---:|---:|
| Bell-Northern Research | Ocak 1991 | 47.0.0.0/8 |
| Xerox Corporation | Eylül 1991 | 13.0.0.0/8 |
| E.I. duPont de Nemours and Co., Inc. | Aralık 1991 | 52.0.0.0/8 |
| Apple Inc. | Temmuz 1992 | 17.0.0.0/8 |
| IBM | Ağustos 1992 | 17.0.0.0/8 |
| Massachusetts Institute of Technology | Ocak 1994 | 18.0.0.0/8 |
| General Electric Company | Mayıs 1994 | 3.0.0.0/8 |
| Hewlett-Packard Company | Temmuz 1997 | 15.0.0.0/8 |

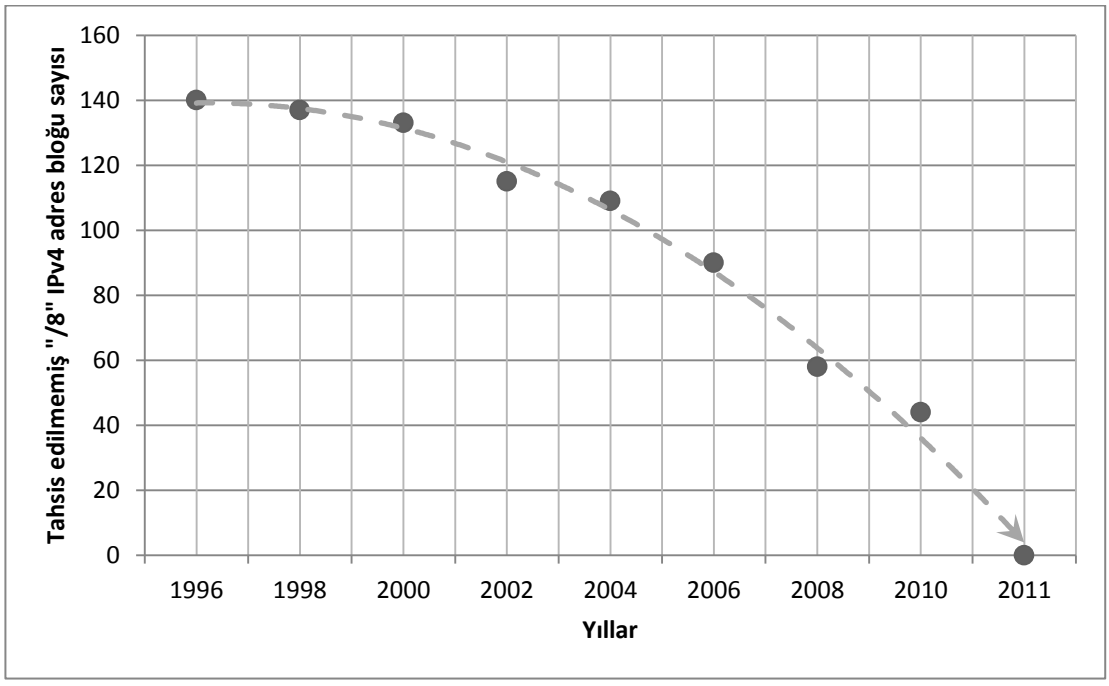
Sadece Çizelge 2.1'de gösterilen 8 adet şirket ve kuruma tahsis edilen IP adreslerinin sayısı, 134.217.728 olmaktadır. IANA tarafından dağıtımı yapılmış olan tüm "/8" A sınıfı IP adreslerinin listesi IANA[2] web sitesinden görülebilir.

2011 yılında; Microsoft firması, Nortel Networks firmasına tahsis edilmiş olan (47.0.0.0/8) aralıktan, Nortel Networks'e 7,5 milyon dolar ücret ödeyerek 666.624 adet

[1] IPv4 sisteminde; 32 bitlik adresleme sistemi kullanıldığından, 32 bit ile adreslenebilecek cihaz sayısı, $2^{32}$= 4.294.967.296 şeklinde hesaplanabilir.
[2] http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

IPv4 adresi satın almıştır. Satın alınan IP adresi sayısı, Nortel Networks'e tahsis edilen IP adreslerinin yaklaşık %4'ü kadardır. Bu satın alma için IP adresi başına maliyeti, 11,25 dolar olmaktadır (Silvestre, B.A., vd. 2011).

Şekil 2.3'te 1996 yılından itibaren günümüze kadar olan zamanda, IANA'nın elinde bulunan (herhangi bir kuruma tahsis edilmemiş olan) "/8" IPv4 adres bloklarının grafiği gösterilmektedir. Grafikte de görülebileceği gibi, özellikle 2000'li yıllardan itibaren tahsis edilmemiş IPv4adres aralığı sayısında hızla düşüş yaşanmış ve 2011 yılında "/8" IPv4 adres blokları tükenmiştir. Aslında IPv6 geçişinin zorunlu hale gelmesindeki en büyük etken IPv4 adreslerinin artık tükenmiş olmasıdır (http://en.wikipedia.org/wiki/IPv4_address_exhaustion, Haziran 2014).




**Şekil 2.3.** 1996 yılından itibaren tahsis edilmemiş "/8" IPv4 adreslerinin sayısı.

IPv4 adresleri ikili sayı sisteminde 32 bitlik olarak tanımlanmasına rağmen uygulamada genelde onluk sayılarla gösterilir. 32 bitlik bir adres, 8 bitlik 4 parçaya (oktet) ayrılır, her oktet onluk sisteme çevrilir ve oktetler arasına nokta konarak IPv4 adresi oluşturulur. Örneğin; "00001010 00000001 00000010 00000011" şeklindeki bir IPv4 adresinin onluk gösterimi, 10.1.2.3 şeklindedir.

IPv4 adreslerinin kullanımı uygulamada çok işlevsel olmadığı için DNS (Domain Name System ~ Alan Adı Sistemi) adı verilen sistem geliştirilmiştir. DNS, günümüzde de kullanılan, alan adlarını IP adreslerine veya IP adreslerini alan adlarına çevirme işlemini yapmaktadır. Bu şekilde İnternet üzerinde bir adrese ulaşmak istendiğinde, IP adresi yerine kullanımı daha kolay olan alan adlarını yazarak erişilebilmektedir (Mockapetris, 1987a; Mockapetris, 1987b).

### 2.2.1 IPv4 adres sınıflandırması

IPv4 adreslemede, her bir IP adresinin yüksek öncelikli bitleri bağlı olduğu ağı gösterirken, geriye kalan düşük öncelikli bitler ise ağdaki bilgisayarı adreslemek için kullanılır.

IPv4 adresleri kullanılarak ağ oluşturulurken, ağdaki bilgisayar sayısına göre IP adresi ayrılması gerekmektedir. Bu durumda, IP israfını engellemek için büyük ağlarda daha fazla IP adresi, küçük ağlarda ise daha az sayıda IP adresi tahsis edilmektedir. Bunu sağlayabilmek için, IPv4 sisteminde IP adresi sınıfları geliştirilmiştir. IP adresinin ilk oktetine göre hangi sınıfa dâhil oldukları Çizelge 2.2'de gösterilmiştir.

**Çizelge 2.2.** IPv4 adres sınıfları.

| Sınıf | Toplam ağ sayısı | Her bir ağda kullanılabilecek IPv4 adres sayısı | Başlangıç adresi | Bitiş adresi |
|---|---|---|---|---|
| **A** | $2^7$=128 | $2^{24}$=16.777.216 | 0.0.0.0 | 127.255.255.255 |
| **B** | $2^{14}$=16.384 | $2^{16}$=65.536 | 128.0.0.0 | 191.255.255.255 |
| **C** | $2^{21}$=2.097.152 | $2^8$=256 | 192.0.0.0 | 223.255.255.255 |
| **D (çoklu yayın)** | tanımsız | tanımsız | 224.0.0.0 | 239.255.255.255 |
| **E (rezerve)** | tanımsız | tanımsız | 240.0.0.0 | 255.255.255.255 |

D ve E sınıfı adresler özel amaçlar için ayrıldığından, günümüzde internet üzerinde sadece A, B ve C sınıfı IP adresleri kullanılmaktadır. Bu sınıflar da kurumlara IPv4 adres aralığı tahsis edilirken, kurumun ihtiyacına uygun sayıda IP adresi sağlamak için kullanılmaktadır. Eğer kuruma 1–256 arasında IP adresi yetiyorsa, C sınıfı IPv4

adres aralığı tahsis edilmektedir. C sınıfı adresin yetmediği durumlarda da -*kurumun ihtiyacına göre*- B ve A sınıfı adres aralıkları tahsis edilmektedir.

Dünyada olduğu gibi ülkemizde de İnternet bağlantısını önce yapan kurumlara çok sayıda IP adresi tahsis edilmiştir. Aşağıda /16 şeklinde[1] IP adres bloğuna sahip üniversitelerimiz listelenmiştir:

- Ege Üniversitesi; 155.223.0.0 - 155.223.255.255
- Bilkent Üniversitesi; 139.179.0.0 - 139.179.255.255
- ODTÜ; 144.122.0.0 - 144.122.255.255
- İTÜ; 160.75.0.0 - 160.75.255.255

IPv4 adreslerinin ilk tahsisi sırasında, İnternet'in günümüzdeki kadar genişleyeceği tahmin edilemediğinden, birçok kuruma, ihtiyacı olmadığı halde A ve B sınıfı adres aralıkları tahsis edilmiştir. Bu nedenle, IPv4 adresleri hızla tükenmektedir.

#### 2.2.1.1 İnternet Protokolü sürüm 4'te alt ağlara bölme

IPv4 adresleme sistemindeki sınıflandırma yapısı nedeniyle önceleri, kurumlara A, B veya C sınıfı adres aralığı tahsis edilmiştir. Bu durum, uygulamada IP adreslerinin israfına sebep olmaktadır. Örneğin; C sınıfı IP adres bloğu (256 adet IP adresi) yetmeyen bir kuruma, B sınıfı IP adres bloğu (65.536 adet IP adresi) tahsis edilmektedir. Bu da zaten yetersiz gelen IPv4 adreslerinin daha hızlı tükenmesine yol açmaktadır. Bu sorunun önüne geçebilmek için, IPv4 ağlarında "alt ağlara bölme (subnetting)" adı verilen bir yöntem uygulanmaktadır.

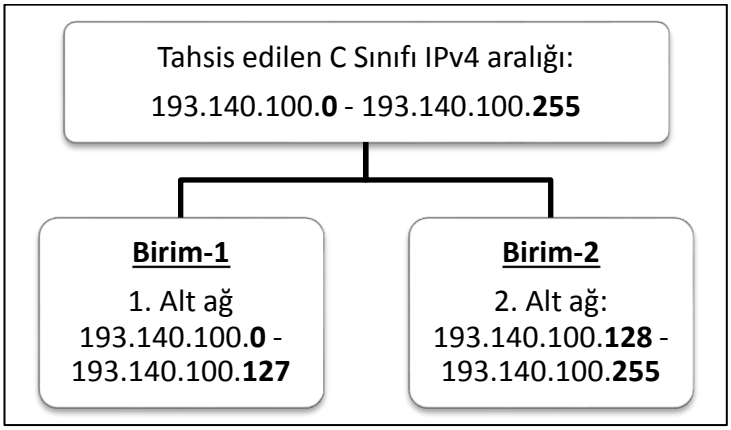
Alt ağlara bölme konusu; bir kuruma IP adres aralığı tahsis edilirken A, B veya C şeklinde tüm bir ağın tahsis edilmesi yerine, IP bloğunun, daha küçük parçalara bölünmesi ve tahsisinin bu şekilde yapılması amacıyla ortaya çıkmıştır. Benzer şekilde, kurumlar da kendilerine tahsis edilmiş olan IPv4 adreslerini, iç ağlarındaki birimlerine dağıtmak için, iç ağlarda da daha alt seviye alt ağlara bölme işlemi yapılmaktadır.

---

[1] Teorik olarak; $2^{(32-16)} = 2^{16} = 65.536$ adet IP adresi

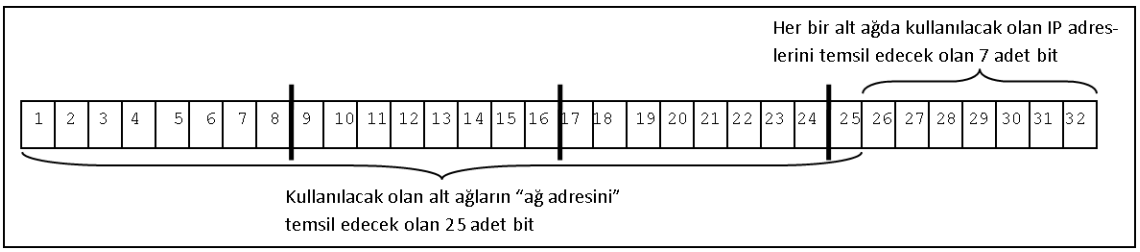
Herhangi bir ağı alt ağlara bölmek için, 32 bitten oluşan IP adresi iki kısma ayrılır. Bu durumda; sol taraftan itibaren belirli sayıda bit ağı temsil eder, geriye kalan sağdaki bitler de IPv4 ağındaki bilgisayarların kendi adresini temsil etmek için kullanılır.

Örneğin C sınıfı bir ağın, her bir alt ağında 128 adet IP bulunan alt ağlara bölüneceğini varsayalım. Şekil 2.4'te bu örnek için, alt ağlara bölme işlemi şematik olarak gösterilmiştir.




**Şekil 2.4.** C sınıfı bir ağın alt ağlara bölünmesi uygulaması.

Her bir ağda kullanılacak olan IP adresi sayısı 128 olacağından, alt ağlarda kullanılabilecek olan IP adreslerini temsil edebilmek için, 7 adet bite (7 adet iki durumlu bit kullanılarak, $2^7$=128 ayrı durum temsil edilebilir) ihtiyaç vardır. IPv4 adresleri 32 bitten oluştuğu için, bu durumda geriye kalan 25 bit de ağın adresini temsil eder. Şekil 2.5'te alt ağ maskesinde kullanılan bitlerin anlamı gösterilmiştir.




**Şekil 2.5.** Alt ağ maskesinde kullanılan bitlerin anlamı.

Bir C sınıfı IP bloğu, 256 adet IP adresi içermektedir. Örnekte bahsedilen alt ağlara bölme işlemi sonucunda, 2 tane 128 adet IP adresi barındıran alt ağ ortaya çıkacaktır.

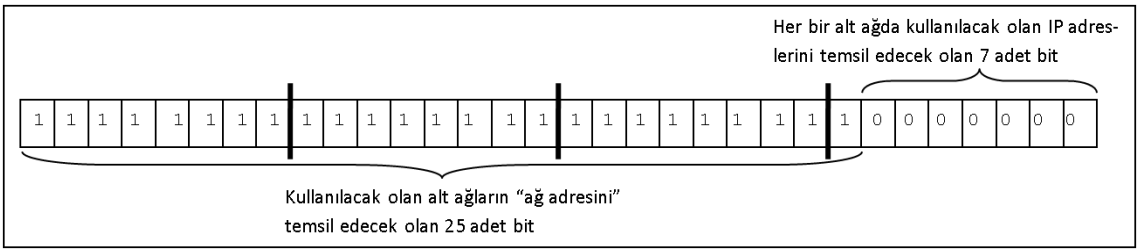
Alt ağlara bölmenin tek gerekçesi IP adresi sayısının yetersizliği değildir. Yayın mesajları denilen ve ağdaki tüm bilgisayarlara iletilmesi gereken verilerin fazla olması, ağın performansını düşürür. Bu nedenle, bir ağ ne kadar fazla alt ağa bölünürse, cihazlara gelen yayın mesajlarının sayısı o kadar azalacaktır. Diğer taraftan, yönetim ve güvenlik açısından da alt ağlara bölmenin faydaları vardır. Alt ağlara bölme sonucunda, ağlardaki trafik birbirinden soyutlanmış olacaktır. Ağların arasında yönlendirme işlemi yapan "ağ geçidi" cihazlarının üzerinde, güvenlik denetimleri yapma olanağı ortaya çıkmaktadır.

Bir ağın alt ağlara bölünmesi durumunda, ağdaki cihazların haberleşmek istedikleri bir IP adresinin kendi ağında olup olmadığını bilmesi gerekmektedir. Bilgisayarların, "hedef IP, benimle aynı ağda mı?" sorusuna verecekleri yanıt sonrasında, iletilmek istenen paket ya doğrudan hedef IP adresine gönderilecektir veya hedef IP adresi farklı bir ağda ise, gönderilecek olan paket diğer ağa iletilmek üzere ağ geçidi görevi yapan cihaza teslim edilecektir. Ağ geçidi olarak kullanılan cihazlara genel anlamı ile "yönlendirici" ismi verilmektedir. Ancak bazen ağ geçidi cihazlarından, yönlendirmenin haricinde de görevler beklenmektedir. Bu açıdan bakıldığında; ağ anahtarları (switch), güvenlik duvarı (firewall) cihazları veya özel yazılımlar yüklenen bilgisayarlar da "ağ geçidi" olarak görev yapabilmektedir.

IPv4 ağlarında, ağdaki cihazların veri göndermek istediği IP adreslerinin kendi ağlarında olup olmadığını anlamasının yolu, "alt ağ maskesi" (subnet mask) kullanmaktır. Alt ağ maskesinin temel görevi, 32 bitten oluşan IPv4 adreslerinin hangi bitlerinin ağı temsil ettiğini, hangi bitlerinin de ağdaki IP adreslerini temsil ettiğini belirlemektir. Her bir ağ tanımlanırken, alt ağ maskesinin de belirtilmesi gerekmektedir.

Alt ağ maskesinin gösterimi de IP adreslerine benzer şekildedir. 32 bitten oluşur ve onluk sayı sistemi kullanılarak yazılır. 4 oktetten oluşur, her bir oktet nokta (.) işareti

ile birbirinden ayrılır. Alt ağ maskesi hesaplanırken; bir IP adresi için, ağı temsil eden bitlerin yerine ikili sayı sisteminde "1" konulur, ağdaki bilgisayar adreslerini temsil eden bitler için de "0" konulur. Şekil 2.5'te açıklaması gösterilmiş olan örnek alt ağ maskesinin ikili sayı sistemine göre yazılmış hali Şekil 2.6'da gösterilmiştir.



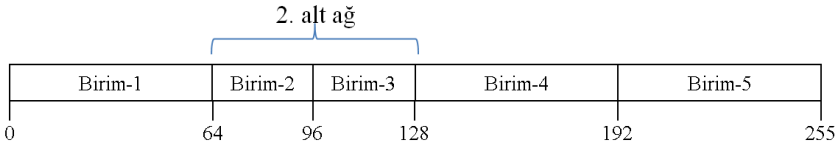

**Şekil 2.6.** "255.255.255.128" şeklindeki alt ağ maskesinin bitlerinin gösterimi.

Şekil 2.4'te verilen, "bir C sınıfı ağı iki alt ağa bölme" örneği için alt ağ maskesi ikilik sistemde yazılacak olursa, 11111111.11111111.11111111.10000000 şeklinde olacaktır. Bu yapıda, "1" ile gösterilen ilk 25 bit ağı temsil etmektedir. "0" ile gösterilen düşük değerli 7 bit ise her bir alt ağda kullanılabilecek olan IP adreslerini temsil etmek için kullanılmaktadır. Aynı alt ağ maskesi, onluk sayı sisteminde yazılırsa, 255.255.255.128 şeklinde olacaktır.

Alt ağlara bölünmüş bir ağda; "hangi bitlerin ağı temsil ettiğini" dolayısıyla, her bir ağda kullanılabilecek olan IP adresi sayısını belirtmenin bir diğer yolu da CIDR (Classless Inter Domain Routing ~ Sınıfsız Alanlar Arası Yönlendirme) biçimi denen yöntemi kullanmaktır. Bu yöntemde, herhangi bir IPv4 ağını belirtebilmek için, IP adresinin en sağına bölü (/) işareti koyulur ve hemen sonra ağı temsil eden bit sayısı yazılır. Örneğin, 192.1.1.0 şeklindeki bir C sınıfı ağın iki adet alt ağa bölüneceğini varsayalım. Bu durumda, iki farklı gösterim yönteminden birisi tercih edilir. Alt ağlardan ilki için; alt ağ maskesi kullanılarak ifade edilecekse, "*ağın adresi: 192.1.1.0, alt ağ maskesi: 255.255.255.128*" şeklinde yazılır. Aynı ağ; CIDR biçiminde, "*192.1.1.0/25*" şeklinde ifade edilir. Benzer şekilde ikinci ağ için; alt ağ maskesi kullanılarak ifade edilecekse, "*ağın adresi: 192.1.1.128, alt ağ maskesi: 255.255.255.128*" şeklinde yazılır. Aynı ağı CIDR biçimine uygun olarak ifade etmek için ise, "*192.1.1.128/25*" şeklinde kullanılır.

Alt ağlara bölme konusunda ağ üzerindeki cihaz yapılandırmalarında da yukarıda bahsedilen durumlar aynı şekilde geçerlidir. Ağdaki her bir bilgisayara, kendi ağına ait bir IP adresi ve doğru yapılandırılmış alt ağ maskesi verilir. Eğer bir bilgisayarın diğer ağlardaki bilgisayarlarla haberleşmesi (yerel veya geniş ağlarda) gerekiyorsa, bu durumda bilgisayara bir de bu ağın diğer ağlarla bağlantısını sağlayan ve yönlendirme işlemi yapan "ağ geçidi" için IP adresi tanımlanır.

Şekil 2.7, Çizelge 2.3 ve Şekil 2.8'de, C sınıfı bir adres aralığı (193.140.100.0 - 193.140.100.255) tahsis edilmiş olan farklı bir örnek kurum için, kurumun iç ağında uygulayabileceği örnek alt ağlara bölme işlemi gösterilmiştir. Bu örnek kurumda 5 farklı birim bulunmaktadır. 3 birimde 64 adet IP adresi içeren alt ağlar yeterli olurken, iki birimde ise 32 adet IP adresi içeren alt ağların yeterli olduğu varsayılmıştır. Kuruma tahsis edilen 256 adreslik IPv4 aralığı, kurumun kendi iç ağındaki birimler için 64'er adet IPv4 adresi kullanılacak şekilde 4 eşit parçaya bölünmüştür. Daha sonra, "*2. Alt ağ*" olarak adlandırılmış olan bir alt ağ, küçük birimlerde daha küçük aralıklara ihtiyaç olabileceğinden, 32'şer IP içeren iki alt ağa daha bölünmüştür.



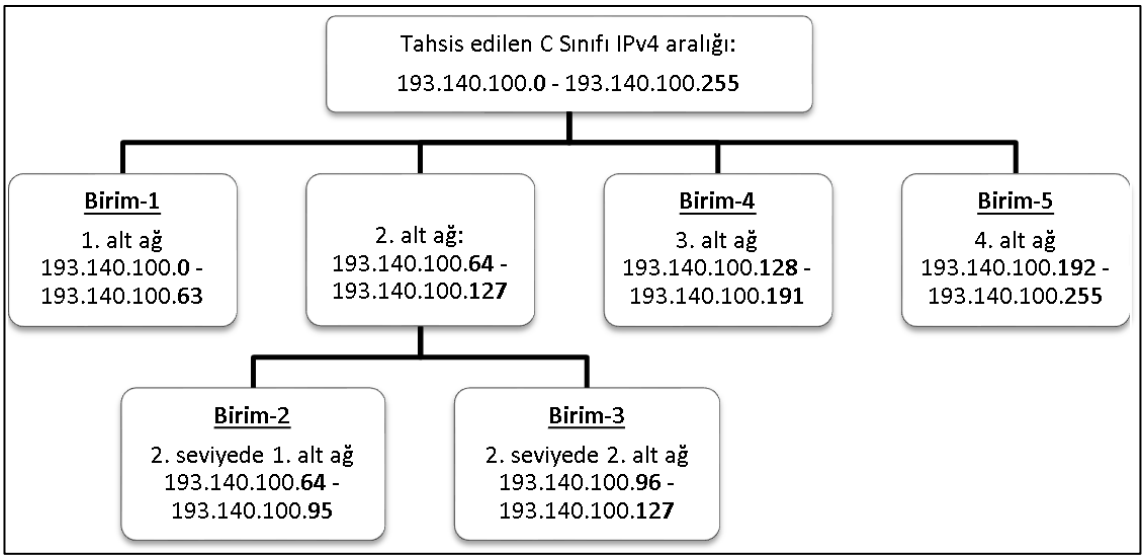

**Şekil 2.7.** Örnek kurum için IP aralığının beş birime paylaştırılması

Çizelge 2.3'te, beş adet birimi olan örnek kurum için, her bir birime tahsis edilen IP adresi aralıkları gösterilmiştir.

**Çizelge 2.3.** Örnek kurum için birimlere tahsis edilmiş olan alt ağ bilgileri.

| | **IP Adresi sayısı** | **İlk IP adresi** | **Son IP adresi** |
|---|---|---|---|
| Ana IPv4 aralığı | 256 | 193.140.100.0 | 193.140.100.255 |
| Birim–1 | 64 | 193.140.100.0 | 193.140.100.63 |
| Birim–2 | 32 | 193.140.100.64 | 193.140.100.95 |
| Birim–3 | 32 | 193.140.100.96 | 193.140.100.127 |
| Birim–4 | 64 | 193.140.100.128 | 193.140.100.191 |
| Birim–5 | 64 | 193.140.100.192 | 193.140.100.255 |

Şekil 2.8'de, örnek kuruma ait birimler ve her birime tahsis edilen IP adres aralıkları gösterilmiştir. Şekilde görülen "2. alt ağ", bütün olarak hiçbir birime tahsis edilmemiştir. Çünkü bu alt ağ, iki ayrı alt ağa bölünmüş ve bölüm sonucunda çıkan 32 IP adresine sahip olan iki adet alt ağ, iki ayrı birime tahsis edilmiştir.



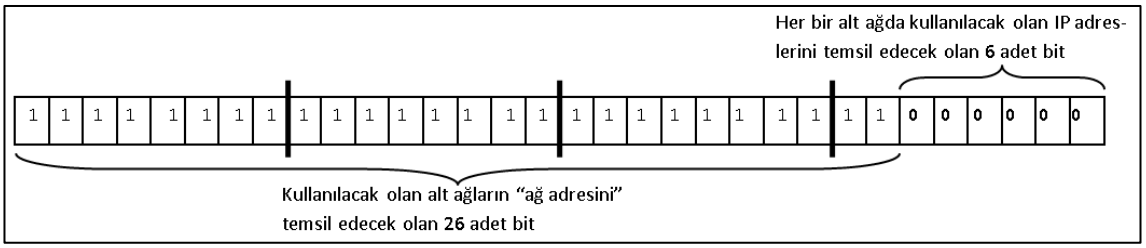

**Şekil 2.8.** Örnek bir kurum için IPv4 alt ağlara bölme uygulaması.

Örnek uygulamadaki 5 adet birimde temel olarak, iki farklı büyüklükte alt ağ kullanılmaktadır. Birim-2 ve Birim-3 için, 32 adet IP adresi kapasiteli alt ağlar hesaplanmıştır. Birim-1, Birim-4 ve Birim-5 için ise 64 adet IP adresi kapasiteli alt ağlar planlanmıştır. Alt ağ maskeleri ağdaki IP sayısına göre hesaplandığından, örnek uygulamada iki tip alt ağ maskesinin kullanılması yeterlidir. Çizelge 2.4'te örnek uygulamadaki birimler için kullanılabilecek olan alt ağ maskeleri belirtilmiştir.

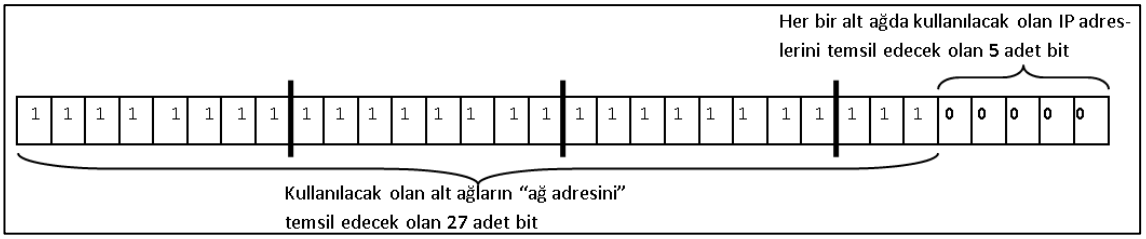
**Çizelge 2.4.** Örnek uygulamanın birimleri için alt ağ maskeleri.

| Birim İsmi | IP Adresi Sayısı | CIDR Gösterimi | Alt Ağ Maskesi |
|---|---|---|---|
| Birim-1 | 64 | 193.140.100.0/26 | 255.255.255.192 |
| Birim-2 | 32 | 193.140.100.64/27 | 255.255.255.224 |
| Birim-3 | 32 | 193.140.100.96/27 | 255.255.255.224 |
| Birim-4 | 64 | 193.140.100.128/26 | 255.255.255.192 |
| Birim-5 | 64 | 193.140.100.192/26 | 255.255.255.192 |

Şekil 2.9'da örnek kurum uygulamasındaki Birim-1, Birim-4 ve Birim-5'te kullanılabilecek olan alt ağ maskesinin ikili sayı sisteminde gösterilişi verilmiştir. Şekil 2.10'da ise Birim-2 ve Birim-3'te kullanılabilecek olan alt ağ maskeleri ikili sayı sisteminde gösterilmiştir.




**Şekil 2.9.** 64 adet IP adresi olan alt ağ için, alt ağ maskesi




**Şekil 2.10.** 32 adet IP adresi olan alt ağ için, alt ağ maskesi

### 2.2.1.2 IPv4 ağlarında IP Yapılandırması

IP ağlarında; iki bilgisayarın birbirine bağlanmasıyla oluşturulabilecek olan küçük bir ağdan, milyonlarca bilgisayarın bağlanmasıyla oluşan dev ağlar da kurulabilmektedir. Günümüzün en büyük IP ağı ise, Internet adı verilen küresel ağdır. IP ağlarının bu esnekliği aynı zamanda yönetimsel olarak bazı sorunları da beraberinde getirmektedir. Bu sorunlardan bir tanesi de IP adreslerinin dağıtım sistematiğidir.

Küresel bazda, IP adreslerinin dağıtımından IANA isimli kuruluş sorumludur. Günümüzde IANA, IP adreslerinin dağıtım görevini dünyada toplam 5 adet olan bölgesel internet kayıtçılarına devretmiştir. IP adresleri, yüksek öncelikli bitlerine (en soldaki bitler [Most Significant Bits ~ MSB]) göre, belirli aralıklar halinde öncelikle IANA tarafından bölgesel internet kayıtçılarına, talep eden kurumlara dağıtılmak üzere tahsis edilir. Daha sonra bölgesel internet kayıtçıları, kendilerinden IP aralığı talep eden

kurumlara, ihtiyaçları oranında IP aralıklarını tahsis ederler. En son olarak, kurumlar kendilerine tahsis edilen IP aralıklarını verimli kullanabilmek için, kendi birimlerinde alt ağlara bölme işlemi yaparlar.

Herhangi bir IP ağı planlanırken; bu ağ için ayrılacak olan IP aralığı, o ağın ihtiyacını uzun vadede görebilecek olan minimal IP adresi sayısı içerecek şekilde hesaplanır. Bunun nedeni, IP adreslerinin israfını engellemektir. IP adreslerinin israf edilmemesi iki nedenden dolayı önemlidir. Birincisi, IP adreslerinin de maliyeti vardır ve talep eden kurumlar bu maliyeti üstlenmektedir. Diğer sebebi ise, dünyanın çeşitli yerlerinde gerçekten o IP adreslerine ihtiyacı olması muhtemel kurumlar olmasıdır.

Kendi iç ağında IP dağıtım hiyerarşisini hazırlayan kurumlar, kurumlarında kullanılan bilgisayarlara IP adreslerini atayabilirler. Internet üzerinde faaliyet göstermek isteyen her bilgisayarın en az bir adet IP adresi sahibi olması zorunludur. Ancak, bilgisayarlara IP adresi dağıtılırken de sistematik bir şekilde planlama yapılmaktadır. Küresel çapta IP adresleri dağıtılırken bir takım kurallara uyulduğu gibi, kurum içi ağlarda da IP adresleri dağıtılırken belirli kurallara uyulmaktadır.

Kurum içerisinde IP dağıtımı yapılırken uyulması gereken en önemli nokta, alt ağlara bölme işlemidir. Kurum içerisinde birbirinden ayrı şekilde bölünmüş olan her alt ağın IP yapılandırması farklı olacaktır. Bir alt ağda IP ile çalışabilen bilgisayar, başka bir alt ağa geçtiğinde IP yapılandırması uyumsuz olacağından çalışmayacaktır. Bu nedenle; sistem yöneticileri tarafından her alt ağ için belirlenmiş olan IP yapılandırmasına, bu alt ağlarda çalışacak olan bilgisayarlar için dikkat edilmektedir.

IP adresi dağıtılırken dikkat edilmesi gereken önemli bir nokta da birden fazla bilgisayara aynı IP adresinin verilmemesidir. Bu durumda “IP çakışması” denilen sorun ortaya çıkar. Ağ üzerinde paketler birbirlerine IP ile iletilirken, her bilgisayara ulaşması gereken veri, onun IP adresinin “hedef” olarak yazıldığı bir paket ile gönderilir. Birden fazla bilgisayarda aynı IP adresi kullanılırsa, ağ üzerindeki paketler doğru hedefe ulaşamayacaklarından iki bilgisayarın da ağ bağlantısında sorun oluşacaktır. Bu risklerden dolayı, her bir alt ağda IP adreslerinin yapılandırması, kurumun bütününü

ilgilendiren bir planın, küçük parçalar halinde alt ağlarda uygulanması şeklinde yapılır. Bu şekilde, IP adreslerinin rastgele kullanılmasından veya doğru olmayan IP yapılandırmasından kaçınılmaktadır.

IPv4 ağlarında ağdaki bilgisayarların IP yapılandırmasını yapabilmek için iki yöntem vardır. Birincisi, "*elle (manuel) IP adresi vermek*"tir. Bu durumda, her bilgisayara (bilgisayarda kullanılan işletim sistemi vasıtasıyla) elle sabit olarak bir IP adresi tanımlanır. Özellikle büyük ağlarda bu yöntemi kullanmak işlevsellikten oldukça uzaktır. IP dağıtımını sağlamak için kullanılan diğer yöntem ise "otomatik IP dağıtma" yöntemidir. IP ağlarında otomatik IP dağıtmak için kullanılan protokole DHCP (Dynamic Host Configuration Protocol ~ Dinamik bilgisayar yapılandırma protokolü) denir. IP ağlarında, ağda kullanılacak olan bilgisayarların IP adreslerinin yapılandırmasında yaşanan karışıklıklar, hatalar ve zorlukların önüne geçilebilmesi için IP ağlarında, bilgisayarlara IP dağıtım işlemi genelde otomatik olarak yapılır.

DHCP, 1993 yılında RFC 1531 ile tanımlanmıştır. Bu protokole göre; ağa fiziksel anlamda yeni katılmış ve henüz IP adresi olmayan bir bilgisayar, kendi ağının tamamına yayın mesajı göndererek ağda bir DHCP sunucusu olup olmadığını sorar. Ağda bir DHCP sunucusu varsa, sunucu kendisinin bu konuda yetkili olduğunu beliren bir cevap yayınlar. Daha sonra DHCP sunucusu tarafından istemci bilgisayara bir IP adresi atanır ve bu bilgiler istemci bilgisayara gönderilir. IP adresinin yanında; alt ağ maskesi, ağ geçidi, DNS (Domain Name System ~ Alan Adı Sistemi) sunucusu, NTP (Network Time Protocol ~ Ağ Zaman Protokolü) sunucusu gibi başka parametreler de istemci bilgisayara DHCP üzerinden gönderilebilir (Droms, 1993).

### 2.2.2 İnternet Protokolü sürüm 4'te yaşanan sorunlar

IPv4'ün ARPANET'te kullanılmaya başladığı 1983 yılından bir yıl sonrasında İnternet üzerindeki kayıtlı bilgisayar sayısı ancak 1.000'i geçmiştir. Sonrasında, 1992 yılında 1 milyonu geçmiş, 2001 yılında 100 milyonu geçmiş ve günümüzde 1 milyarı bulmuştur. IP ağlarının çok fazla büyümesi ve IP üzerinden kullanılacak olan uygulamaların sayısının hızla artması, hem IP sayısının yetmemesine hem de IPv4'ün

teknik olarak yetersiz kalmasına yol açmıştır. IPv4'ün en önemli sorunu, adreslenebilecek olan IP sayısının yetersiz kalmasıdır.

IPv4 sisteminde kullanılabilecek olan adres sayısı $2^{32}$ adettir. Yani teorik olarak 4.294.967.296 adet bilgisayar adreslenebilmektedir (Internet Protocol - Darpa Internet Program Protocol Specification, 1981). Ancak IPv4 yaygınlaşmaya başladığında, IP adresi dağıtım işlemleri İnternetin büyümesi doğru öngörülemeden yapılmıştır. IP adresleri, talep eden kurumlara dağıtılmaya başlandığında, ücretini karşılayan her kuruma istediği sayıda IPv4 adresleri tahsis edilmiştir.

1991 yılında Xerox firmasına, 1992 yılında IBM firmasına, 1995 yılında Ford Motor Company firmasına ve benzeri şekilde birçok kuruma, A sınıfı (16 milyondan fazla IP adresi) IP adres aralığı tahsis edilmiştir. IBM firmasının, 2010 yılı itibarıyla çalışan sayısının 426,751 olduğu düşünülürse, ihtiyacından ne kadar fazla IPv4 adresi tahsis edildiği daha iyi anlaşılmaktadır. Bu nedenle, birçok kurumun elinde çoğunu kullanmadığı halde IP adresleri boşta kalmış, diğer taraftan İnternet'in çok büyük kısmında da kurumlar kısıtlı IPv4 adresleri kullanmak zorunda kalmıştır (http://www.ibm.com/ibm/tr/tr/, Haziran 2014).

IPv4'ün teknik yetersizlikleri uygulamada farklı yöntemlerle aşılmaya çalışılmıştır. Örneğin; kurumlar yeterli sayıda IPv4 adresi edinemediğinden, NAT adı verilen uygulamalar kullanılmıştır. NAT uygulamasında, kurumun iç ağında sanal IP adresleri kullanılır. Herhangi bir bilgisayar İnternet'e bağlanacağı anda, kurumun ağ geçidi tarafından bu sanal IP adresi İnternet üzerinde tanımlı gerçek bir IP adresi ile eşleştirilir. İnternet üzerinden oluşturulan trafik tamamlandığında, bilgisayar bu gerçek IP adresini boşa bırakır. Bu şekilde kurumun elinde kısıtlı sayıda olan gerçek IP adresleri, iç ağdaki çok fazla sayıda bilgisayar tarafından ortaklaşa kullanılır.

NAT kullanımı da bir takım sorunlara yol açmaktadır. NAT yapıldığında, herhangi bir kurum tarafından gerçek IP adresi kullanılarak İnternet üzerinde oluşturulan bir trafiğin kayıtlarını tutmak zor olmaktadır. Adli bir olay olduğunda, bu IP adresinin kurum içindeki hangi sanal IP adresi tarafından kullanıldığının tespiti sorun

oluşturmaktadır. Diğer taraftan NAT uygulamasında giden ve gelen paketlerin başlık bilgilerinde değişiklik yapıldığından, IP üzerinden ses taşıma gibi bazı uygulamalarda istenilen başarı elde edilememektedir (Holdrege, 2001). Yine benzer şekilde, iç ağdaki bilgisayarlara İnternet üzerinden erişim için özel işlemler uygulanmak zorunda kalınmaktadır.

IPv4'ün bir başka sorunu da hiyerarşik olarak adres dağıtımına uygun olmadığından, İnternet'e bağlı olan yönlendiricilerde yönlendirme tablolarının aşırı şişerek performans sorunlarına neden olmasıdır (Loshin, 2004).

IPv4 ağlarında, bilgisayarlara IP adresi atanırken iki tip IP adresi dağıtımı yöntemi kullanılmaktadır. Bunlardan birincisi elle IP verme yöntemi, diğeri de DHCP kullanılarak otomatik IP yapılandırmasıdır. DHCP sunucusu kullanılmadığı zaman, ağdaki bilgisayarlara zorunlu olarak elle IP adresi verilmesi gerekmektedir. IPv4 ağlarında, ağ cihazları üzerinden ağ bilgilerinin anons edilerek istemci bilgisayarların kendi IP yapılandırmasını yapması mümkün değildir (Lawrence, 2010).

IPv4’te, protokolün doğasında şifreleme yoktur. IPv4'te iki bilgisayar arasında şifreli iletişim sağlamak için IPv4 yaması olarak IPSec (Internet Protocol Security ~ İnternet Protokol Güvenliği) protokolü devreye alınmıştır. Bunu uygulayabilmek için, trafiğin iki ucunda da IPSec kurulu olmalıdır. Bu da ilave şifreli iletişim için ilave bir yapılandırma yükü getirmektedir.

IPv4 üzerinde ses ve görüntü taşımada da sorunlar yaşanabilmektedir. Bu tarz uygulamalar, veri taşıma hizmetlerinden daha öncelikli olmalıdır. Çünkü IP üzerinden telefon görüşmesi veya gerçek zamanlı video taşıması sırasındaki aksamalar tolere edilememektedir. Gerçek zamanlı ses ve görüntü taşıma uygulamalarında, hizmet önceliklendirmesi (QoS ~ Quality of Service ~ Hizmet Kalitesi) yapılarak, trafik sınıflandırılmalı ve öncelikli trafiğe bant genişliği ayrılması sağlanmalıdır. IPv4, QoS uygulanmasında sınırlı destek vermektedir.

## 2.3 İnternet Protokolü sürüm 6'ya genel bakış

IPv4'ün doğuracağı sıkıntılara çözüm arayışı resmi olarak ilk defa 1992 yılında başlamıştır. Sonrasında yapılan çalışmalarla 1995 yılında IPv6 resmen duyurulmuştur. IPv6 çalışmalarının temel amacı, IPv4'ün artık yetersiz kalacağının öngörülmesi ve özellikle Başlık 2.2.2'te bahsedilmiş olan kısıtlamalarıdır.

IPv6 protokolünün tarihsel süreci aşağıda özetlenmiştir (http://www.ipv6.net.tr/ (Haziran 2014)).

- **1992** IETF, yeni nesil IP çalışmaları için öneri istedi.
- **1993** IETF, RFC 1550 ile yeni nesil IP önerileri için çağrıda bulundu.
- **1995** IPv6 resmen duyuruldu.
- **1996** Linux 2.1.8 çekirdeğinde IPv6 desteği sağlandı.
- **1998** Temel IPv6 protokolü RFC 2460 ile yayınlandı.
- **1999** Japonya IPv6 adres tahsisine başladı.
- **1999** Sun Solaris, 8 sürümünden itibaren IPv6 desteği sağladı.
- **2001** Cisco, IPv6'ya tam destek veren IOS'u yayınladı.
- **2001** Windows XP SP1 ve Windows Server 2003 IPv6 desteği sağladı.
- **2003** ULAKNET, küresel IPv6 ağına Türkiye'den doğrudan bağlanan ilk ağ oldu.
- **2003** Apple Mac OS X v10.3 "Panther" ile IPv6 desteği sağladı.
- **2003** DHCPv6 (RFC 3315) yayınlandı.
- **2004** ULAKNET, akademik ağdaki kurumlara IPv6 dağıtmaya başladı.
- **2004** Mobil IPv6 (RFC 3775) yayınladı.
- **2004** IPv6 protokolüne akış etiket özellikleri (RFC 3697) eklendi.
- **2006** IPv6 mimarisinde (RFC 4291) istikrarlı çalışması için iyileştirmeler yapıldı.
- **2006** Düğüm "Node" gereksinimleri (RFC 4294) yayınlandı.
- **2008** Google, IPv6 üzerinden hizmet vermeye başladı.
- **2008** Olimpiyat Oyunları ve Engelliler Olimpiyatı, IPv6 üzerinden sunulan ilk büyük etkinlik oldu.
- **2009** Çanakkale Onsekiz Mart Üniversitesi, Mühendislik Binasında IPv6 kullanarak, Türkiye katkı seviyesi 8'e sahip ilk üniversite oldu.
- **2010** Başbakanlık; 27779 sayılı "*Kamu Kurum ve Kuruluşları için IPv6'ya Geçiş*

*Planı*" genelgesini yayınladı.

- **2011** 8 Haziran, Dünya IPv6 günü ilan edildi. Google, Facebook, Yahoo gibi bazı firmalar, 8 Haziran'da sadece IPv6 üzerinden hizmet vereceklerini duyurdular.
- **2011** Türkiye'de 37 üniversite IPv6 ağına bağlı.
- **2012** 27779 sayılı genelgenin 2. aşaması tamamlandı. (*IPv6 bağlantısı ve adresi temin eden kamu kurum ve kuruluşları 31 Aralık 2012 tarihine kadar internet üzerinden verdikleri en az bir adet hizmeti pilot uygulama olarak IPv6 destekli hale getireceklerdir.*)
- **2013** 27779 sayılı genelgenin 3. aşaması tamamlandı. (*Kamu kurum ve kuruluşları en geç 31 Ağustos 2013 tarihine kadar internet üzerinden verdikleri kamuya açık tüm hizmetleri IPv6'yı destekler hale getireceklerdir.*)
- **2014 (Haziran)** Google'a IPv6 üzerinden gelen isteklerin oranı %4'ü buldu.

IPv6 tamamen baştan tasarlanmıştır ve geriye doğru uyumluluk desteklenmemektedir. IPv6, IPv4'e alternatif olarak geliştirilmiş olmasına rağmen, IPv4'ten IPv6'ya çok keskin bir geçiş yapmak mümkün olamamaktadır. Çünkü IPv6'ya tamamen geçen bir kurum, halen IPv4 kullanan kurumların ağına bağlanamayacaktır. Bu nedenle iki protokolün de 10 ila 20 yıl arasında birlikte çalışacağı öngörülmektedir (Geesey, 2006).

IPv6 protokolünün herkes için yeni olması sebebiyle, önceden rahatlıkla kullanılan sistemler ve uygulamaların üzerinde yeniden çalışılması gerekmektedir.Ülkemizde IPv6 çalışmaları kapsamında; 2010 yılı sonunda Başbakanlık tarafından yayınlanan "Kamu Kurum ve Kuruluşları için IPv6'ya Geçiş Planı" konulu genelge ile kademeli bir IPv6 geçişi planlanmıştır. Bu genelgede 2013 Ağustos ayına kadar, tüm kamu kurum ve kuruluşlarının İnternet üzerinden verdiği servislerin tamamının IPv6 üzerinden de verilmesi kararlaştırılmıştır. Yine aynı genelge ile kamu kurum ve kuruluşları bilişim teknolojileri personellerinin, TÜBİTAK ULAKBİM bünyesinde oluşturulan "IPv6'ya Geçiş Eğitimi Merkezi"nde eğitim alması da öngörülmüştür (Resmi Gazete, Sayı: 27779, 2010). Zaten akademik ortamlarda IPv6 konusunda çalışmalar yapılmakta olan ülkemizde bu genelge ile IPv6 farkındalığı daha da artırılmış, IPv6 çalışmaları da hızlanmıştır.

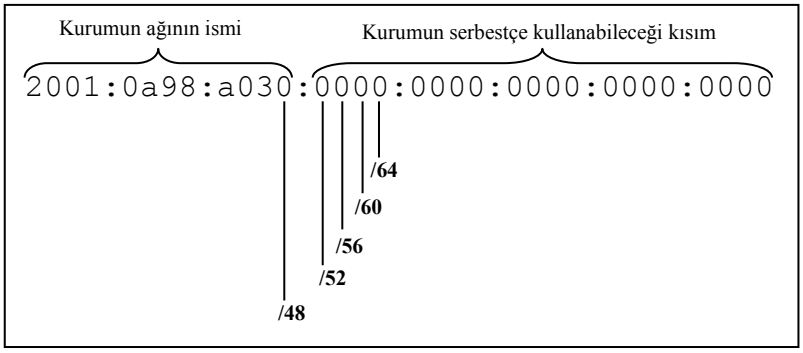
### 2.3.1 İnternet Protokolü sürüm 6'da alt ağlara bölme

IPv6 ağlarında alt ağlara bölme konusu, IPv4 ağlarına benzer şekildedir. Ancak IPv6 ağlarında artık alt ağ maskesi kullanılmamaktadır. Bunun yerine Başlık 2.2.1.1'de bahsedilmiş olan CIDR gösterimi yöntemi kullanılmaktadır. Ayrıca alt ağlara bölerken, bölünecek olan bitlerin sayısı, 16'nın ($2^4$) katları şeklinde, yani bit sayısı olarak 4'ün katları şeklinde bölünmektedir. Aksi takdirde, IPv6 istemci adreslerini ve ağ adreslerini 16'lık sayı sisteminde göstermek sorun olacaktır.

RIPE (Fr. "Réseaux IP Européens" ~ Avrupa IP Ağı), Avrupa'da IP adreslerinin dağıtımından sorumlu olan kuruluştur. IPv6 adresleri, RIPE tarafından Avrupa'da İnternet Servis Sağlayıcılara (İSS), /32 şeklinde verilmektedir. İSS'ler de kurumlara IPv6 tahsislerini genelde /48 şeklinde yapmaktadırlar. Bu yapıya göre; her bir İSS kendine tahsis edilmiş olan IPv6 adreslerinden, $2^{16}$=65.536 adet kuruma /48 şeklinde IPv6 adresi tahsisi yapabilmektedir. /48 şeklinde IPv6 adresi alan her kurum da teorik olarak, $2^{(128-48)}=2^{80}=\sim 1{,}2\text{x}10^{24}$ civarında IPv6 adresine sahip olmaktadır. IPv4 adresleme sistemine göre oldukça fazla sayıda IPv6 adresi olduğu bu hesaptan da görülebilmektedir.

IPv6 adreslerinin alt ağlara bölünürken, bitlerin sayısının 4'ün katlarından bölünmesi gerektiğinden yukarıda bahsedilmişti. Örnek bir kurumun /48 şeklinde IPv6 adresi aldığını varsayarsak, bu kurum kendine tahsis edilmiş olan /48 IPv6 adres aralığını; /52, /56, /60 ve /64 şeklinde alt ağlara bölebilir. /64'ten daha küçük parçalara bölünmemesinin sebebi ise IPv6 ağlarında, istemcilerin kendi IPv6 adreslerini üretmesi istenirse, en az 64 adet bite ihtiyaç olmasıdır.

Şekil 2.11'de, IPv6 ağlarında, alt ağlara bölmek için kullanılabilecek bit sayısı için bir örnek şema gösterilmiştir. Şekil 2.11'de, CIDR gösteriminde bit sayısı olarak kullanılan ifadelerin, IPv6 için ne anlama geldiği görülmektedir. "/48,/53,/56,/60 ve /64" şeklinde verilen bit sayıları IPv6 adreslerinin soldan itibaren bölündüğü noktayı (ağı temsil eden kısım ile bilgisayar adresini temsil eden kısmın ayrıldığı noktayı) göstermektedir.




**Şekil 2.11.** IPv6'da alt ağlara bölmek için kullanılabilecek bit sayısı örnekleri.

CIDR gösteriminde, IP adresinin yanında */ab* şeklinde yazılan ifadeler, bir IP adresinin hangi ağa bağlı olduğunu göstermek için kullanılır. */ab* şeklinde yazılan sayılar, birlikte verilen IP adresinin soldan itibaren ilk *ab* adet bitinin kurumun ağını (veya belirli bir alt ağını) temsil ettiğini belirtir. Geriye kalan diğer bitler (sağdan itibaren, [128 – *ab*] adet bit) ise, bu ağ içerisinde o bilgisayar için, diğer bilgisayarlardan ayırt edici numarasını (adresini) belirtir.

CIDR gösterimi, ev adreslerinde kullanılan il/ilçe ikilisine benzetilebilir. Ülkemizde aynı isimde birçok "ilçe" bulunmaktadır. Adreslerde bu ilçelerin karışmamasını sağlayan ise, kendisi ile birlikte verilen "il" adıdır. Tek başına bir "ilçe" ismi, ülke çapında adres tarifi için yeterli olmayabilir. Ancak "il" adı ile birlikte kullanıldığında, benzersiz bir şekilde tarif edilmiş olur. Buna benzer şekilde, CIDR gösteriminde belirtilen bitten sonraki (sağdaki) bitler, bilgisayarın bulunduğu ağ içerisindeki kendi adresini temsil eder. Dünyada birçok bilgisayarda bu şekilde aynı adres olabilir. Bu adreslerin birbirinden ayırt edilmesini (benzersiz olmasını) sağlayan kısım da, CIDR gösteriminde belirtilen bitten önceki bitlerdir. Bu şekilde, 128 bitlik IP adresinin tamamı kullanılarak, dünya üzerindeki bir bilgisayarın hatasız ve benzersiz olarak tarif edilmesi mümkün olmaktadır.

CIDR gösteriminde ağın adresi ile bilgisayarın adresini ayıran noktanın sürekli sabit olarak kullanılmamasının sebebi olarak ise yine il/ilçe örneğine benzetilerek, ilin/ilçenin büyük veya küçük olmasına bağlı olarak en fazla nüfus kapasitesini temsil ettiği söylenebilir. Bir ilde bulunan ilçelerin nüfusunun çok fazla olması gibi, bir alt ağda bulunan bilgisayarların sayısının çok fazla olması isteniyorsa, CIDR gösteriminde

daha küçük sayılar kullanılarak, bölme noktası sola doğru kaydırılabilir. Ancak bu durumda, ağın maksimum kapasitesi sabit olduğundan, kullanılabilecek olan alt ağ sayısı azalacaktır.

Çizelge 2.5'te IPv6'da alt ağa bölme işlemleri için kullanılabilecek olan bit sayıları verilmiştir. Bu örnek çizelgede /48 şeklinde IPv6 adres aralığı almış olan bir kurumun kendi alt ağlarına bölme işlemi yaptığı varsayılmıştır. İlk satırda (/48), her bir alt ağdaki bilgisayar sayısı en fazla ($2^{80}$) olan gösterilmiştir. Bu durumda sadece bir adet alt ağ oluşturulmuştur. Son satırda ise, alt ağlardaki bilgisayar sayısının minimal olması istenmiş ve bölünebilecek en küçük alt ağlara bölünmüştür. Bu durumda da en fazla alt ağ sayısı (65.536 adet alt ağ) elde edilmiştir.

**Çizelge 2.5.** IPv6 ağlarında /48 şeklindeki bir ağın alt ağlara ayrılması seçenekleri.

| IP adresi<br>(altı çizili olan kısım ağı temsil eder, koyu olan kısım ise, o ağdaki bilgisayarlara verilecek olan adresleri temsil eder) | CIDR gösterimi için bit sayısı | Kullanılabilecek alt ağ sayısı | Her bir alt ağda kullanılabilecek IP adres sayısı |
|---|---|---|---|
| 2001:0a98:a030:**0000:0000:0000:0000:0000** | /48 | $16^0=1$ | $2^{(128-48)}=2^{80}$ |
| 2001:0a98:a030:0**000:0000:0000:0000:0000** | /52 | $16^1=16$ | $2^{(128-52)}=2^{76}$ |
| 2001:0a98:a030:00**00:0000:0000:0000:0000** | /56 | $16^2=256$ | $2^{(128-56)}=2^{72}$ |
| 2001:0a98:a030:000**0:0000:0000:0000:0000** | /60 | $16^3=4.096$ | $2^{(128-60)}=2^{68}$ |
| 2001:0a98:a030:0000**:0000:0000:0000:0000** | /64 | $16^4=65.536$ | $2^{(128-64)}=2^{64}$ |

Çizelge 2.5'e göre örneğin, /48 şeklinde bir IPv6 aralığı tahsis edilen kurum, bu aralığı kendi iç ağında /52, /56, /60 veya /64 biçiminde bölebilir. Benzer şekilde, /60 şeklinde bir IPv6 aralığı tahsis edilen kurum da, alt ağlarını yalnızca /64 şeklinde bölebilir.

Çizelge 2.6'da, /48 olarak IPv6 adresi almış olan örnek bir kurum için alt ağlara bölme uygulaması gösterilmiştir. IPv6 adres tahsisi /48 olarak yapıldığından, kurumun ana ağı ilk 48 bitle temsil edilmektedir. Yani, "2001:0a98:a030" olarak ilk 48 bitlik kısım sabit olmak üzere, onun haricindeki 16'lık sayı sisteminde belirtilen tüm hanelerde değişiklik yapılarak farklı alt ağ yapılandırmaları kullanılabilir. Örnekte kurumun ağı, 16 eşit parçaya (alt ağa) bölünmüştür.

**Çizelge 2.6.** Örnek bir alt ağa bölme uygulaması.

| Alt ağ numarası | Alt ağ (CIDR gösterimi) | Ağı gösteren bit sayısı | Bilgisayar adreslerini gösteren bit sayısı | Kullanılabilecek bilgisayar sayısı |
|---|---|---|---|---|
| 1 | 2001:0a98:a030:**0**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 2 | 2001:0a98:a030:**1**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 3 | 2001:0a98:a030:**2**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 4 | 2001:0a98:a030:**3**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 5 | 2001:0a98:a030:**4**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 6 | 2001:0a98:a030:**5**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 7 | 2001:0a98:a030:**6**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 8 | 2001:0a98:a030:**7**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 9 | 2001:0a98:a030:**8**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 10 | 2001:0a98:a030:**9**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 11 | 2001:0a98:a030:**a**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 12 | 2001:0a98:a030:**b**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 13 | 2001:0a98:a030:**c**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 14 | 2001:0a98:a030:**d**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 15 | 2001:0a98:a030:**e**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| 16 | 2001:0a98:a030:**f**000:0000:0000:0000:0000/52 | 52 | 76 | $2^{76}$ (*) |
| (*) $2^{76}$=75.557.863.725.914.323.419.136 | | | | |

Çizelge 2.6'da, ikinci sütunda "Alt ağ" başlığı altında verilen ifadelerdeki altı çizili olan haneler, her alt ağ için değişen kısmı göstermektedir. Bu örnekte, baştan itibaren ilk 12 hane (ilk 48 bit) kurumun ana ağını temsil ettiği için, bu hanelerde kurum tarafından değişiklik yapılamaz. Ancak bundan sonraki hanelerde düzenleme yapılabilir. Örnekte, sadece 13. hane (49-52 arası bitler) değiştirilerek, 16 adet farklı alt ağ oluşturulmuştur. İlk 52 bit ağın adresini, sonraki bitler bilgisayar adreslerini temsil edeceği için, CIDR gösterimi /52 şeklinde olmaktadır.

### 2.3.2 IPv6 ağlarında IP yapılandırması

IPv4 ağlarında IP yapılandırması konusunda iki yöntem olduğu, Başlık 2.2.1.2'te ele alınmıştı. İlgili bölümde; kolay ve sağlıklı bir yöntem olması nedeniyle, genellikle otomatik IP yapılandırması yönteminin tercih edildiğinden bahsedilmişti.

IPv6 ağlarında ise hesaplama ve yapılandırma hatası olasılığı daha fazladır. Çünkü IPv6 adresleri 128 bitten oluşur ve 16'lık sayı sisteminde gösterildiğinde, 32 karakter (128/4=32) ile ifade edilir. Bu nedenle, IPv6 ağlarında elle IP yapılandırması IPv4 ağlarına göre çok daha zor olmaktadır. Ancak yine de elle IP yapılandırması yöntemi desteklenmektedir. Bununla beraber, otomatik IP yapılandırması için farklı bir yöntem daha geliştirilmiştir.

IPv4 ağlarında otomatik yapılandırmada kullanılan DHCP yöntemi, IPv6 ağlarında da geçerlidir. Ancak, DHCP protokolü, IPv6 ağlarında kullanılabilmek üzere yeniden tasarlanarak DHCPv6 şeklinde yeniden tanımlanmıştır (Droms vd., 2003).

IPv6 ağlarında kullanılabilecek olan yeni otomatik IP yapılandırması yöntemi ise, "durum denetimsiz otomatik yapılandırma" yöntemidir. Bu yöntemde, IP dağıtımı ile görevli bir sunucu bulunmasına gerek kalmamaktadır. Durum denetimsiz otomatik yapılandırma yöntemi, Başlık 2.4 altında incelenecektir.

## 2.4 IPv4 ile IPv6 Karşılaştırması

IPv6'nın yenilikleri aşağıda başlıklar halinde sıralanmıştır:

**Ölçeklenebilirlik:** IPv4 32 bitlik adresleme yapısı sunarken, IPv6'da 128 bitlik adresleme ortaya konmuştur. Teorik olarak IPv6'da adreslenebilecek IP sayısı $2^{128}$ ($\sim 3{,}4 \times 10^{38}$) adettir. 2010 yılı için dünyadaki insan nüfusunun 6,8 milyar olduğunu düşünülürse; kişi başına $5 \times 10^{28}$ adet IPv6 adresi düşmektedir (Deering vd., 1998).

IPv6'da teorik olarak adreslenebilecek IP adresi sayısı çok fazla olmakla birlikte; teorideki bu hesaplama uygulamada gerçekçi sonuçlar vermeyecektir. Çünkü IPv6 sisteminde alt ağlara bölme işleminde, tavsiye edilen hesaba göre İSS'lere "/48" verilmesi, İSS'lerin kurumlara "/64" tahsis etmesi, kurumların da alt ağlara bölerken en küçük alt ağı "/64" aralık olarak ayarlanması gerekmektedir. "/64"'ten daha küçük alt ağlara bölünmesinin istenmemesinin sebebi de, IPv6'da yeni gelen bir özellik olan "durum denetimsiz otomatik yapılandırma" sayesinde istemcilerin kendi bağdaştırıcılarının MAC (Media Access Control ~ Medya Erişim Denetimi)

adreslerinden otomatik olarak IP üretmesidir. MAC adresleri 48 bitten oluşmaktadır. MAC adresi kullanılarak üretilen IP adreslerinde bir istemci tanımlamak için 64 bit gerekmektedir. Bu nedenle alt ağlara bölerken istemciler için en az 64 bit ayrılması gerekmektedir (Thomson vd., 1998; Hinden vd., 2006; "Guidelines for 64-bit Global Identifier (EUI-64™)", 2003).

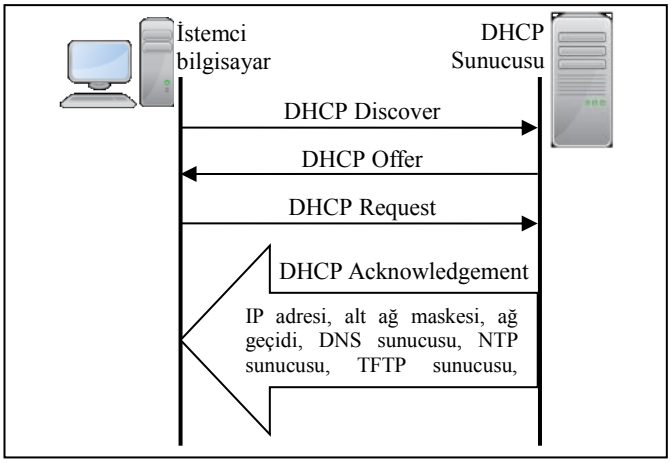
**Güvenlik:** IPv6'da, paketlerde veri kısmının şifrelenmesi ve iletişimde kaynağın doğrulanması gibi güvenlik özellikleri varsayılan olarak hazır halde gelmektedir. Bu sayede, İstemci bilgisayarlarda ilave bir yapılandırma yapmaya gerek kalmadan doğrudan IP seviyesinde şifreli iletişim sağlanabilmektedir. Kısacası, IPv6'da IPSec doğrudan protokolün içerisinde kullanıma hazır olarak gelmektedir (Mustell, 2009).

IPv4'te ise, protokolün doğasında şifreleme bulunmamaktadır. IPv4 ağlarında, iki bilgisayar arasında IP seviyesinde şifreli iletişim sağlamak için, IPv4 yaması olarak IPSec protokolü devreye alınmıştır. Bunu uygulayabilmek için, trafiğin iki ucunda da IPSec kurulu olmalıdır. Bu da ilave şifreli iletişim için ilave bir yapılandırma yükü getirmektedir.

**Gerçek zamanlı uygulamalar:** IPv6, gerçek zamanlı uygulamalara (VoIP gibi) daha iyi destek verebilmek için, yapısal olarak "akış etiketlerini" destekler. Bu mekanizma sayesinde, yönlendiriciler uçtan uca trafik akışındaki paketleri tanımlayabilir ve trafik önceliklendirmesini buna göre yapabilir. Trafik önceliklendirme işlemi, paket başlık bilgisindeki "Traffic Class (Trafik Sınıfı)" ve "Flow Label (Akış Etiketi)" alanlarına göre yapıldığından, paketlerin veri kısmı şifrelenmiş dahi olsa, önceliklendirme başarılı olarak yapılabilir. Özellikle akış etiketi özelliği sayesinde, iki uç arasında kurulan bir oturum süresince geçen tüm paketler aynı akış etiketi ile etiketleneceğinden, aktif oturum süresince trafiğin tamamı aynı hizmet önceliklendirmesine tabi tutulabilecektir. Dolayısıyla IPv6, doğal olarak üst katman protokollerin ihtiyacı olan önceliklendirme işlemlerine destek vermektedir (Can, 2006).

IPv4'te ise, gerçek zamanlı uygulamalardaki gecikmeleri ve bozulmaları engellemek için hizmet önceliklendirmesi (QoS) yapılmaktadır. Ancak hizmet önceliklendirmesi işleminde, paketler şifrelenmişse, paket içeriği bilinemediğinden hizmet önceliklendirmesi başarılı olamamaktadır. Diğer taraftan, akış etiketi desteği olmaması nedeniyle, iki uç arasında kurulan bir oturum süresince akan tüm trafikteki her bir paket için yeniden hizmet önceliklendirmesi hesaplanmakta ve dolayısıyla sistemlere ilave yük getirmektedir.

**Durum denetimsiz otomatik yapılandırma:** İstemcilerin IP yapılandırmasını kolaylaştırmak için IPv6'da iki yöntem kullanılmaktadır. Bunlardan birincisi, IPv4'te de kullanılan durum denetimli otomatik yapılandırmadır. Bu yöntemde DHCP sunucusu üzerinden istemcilere IP adresi, alt ağ maskesi, ağ geçidi, DNS sunucusu gibi bilgiler dağıtılır. Şekil 2.12'de, örnek bir durum denetimli otomatik IP yapılandırması trafiği gösterilmiştir.



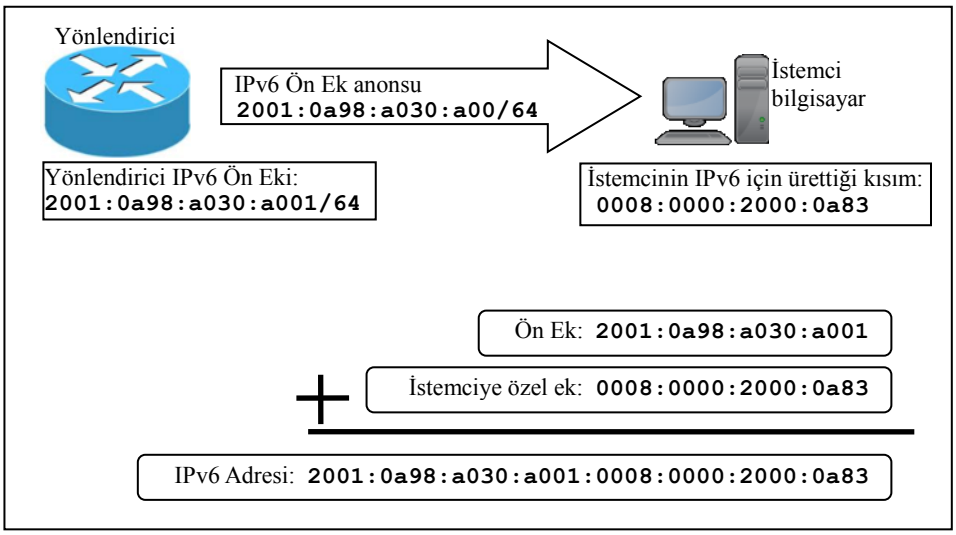

**Şekil 2.12.** Durum denetimli otomatik IP yapılandırması trafiği.

Şekil 2.12'de, 4 farklı DHCP mesajı görülmektedir. Bu mesajların anlamı şu şekildedir:

- DHCP Discover (keşif): Ağa yeni dâhil olan bir istemci ağın tamamına bu mesajı göndererek, kendisine IP verebilecek bir DHCP sunucusu olup olmadığını sorar.
- DHCP Offer (teklif): Ağda bulunan DHCP sunucusu, önceki mesaja cevap olarak, kendisinin IP adresi vermeye yetkili olduğunu belirtir.

- DHCP Request (talep): İstemci, kendisine cevap veren DHCP sunucusunun teklifini kabul eder ve IP yapılandırması bilgilerini ister.
- DHCP Acknowledgement (onay): DHCP sunucusu istemci bilgisayara; IP adresi, alt ağ maskesi, ağ geçidi, DNS sunucusu, NTP sunucusu, TFTP sunucusu, vb. bilgileri gönderir.

Yalnızca IPv6'da kullanılabilen diğer otomatik yapılandırma yöntemi ise, durum denetimsiz otomatik yapılandırmadır. Bu yöntemde ise, önce yönlendirici veya ağ geçitlerinde ağın tanımlaması yapılır. Daha sonra sistem yöneticisi tarafından, ilgili ağa ait olarak belirlenmiş olan "ön ek (prefix)" bilgisinin, cihaz tarafından ağdaki bilgisayarlara (istemciler) anons edilmesi sağlanır. İstemciler bu anonsu alır ve kendi ağını yapılandırır. İstemciler IPv6 için kendi ağ yapılandırmasını yaparken, ilk 64 biti "ön ek" olarak anonstan alır, son 64 biti de kendisi üretir. Şekil 2.13'te durum denetimsiz otomatik yapılandırmanın işleyişi görülmektedir.




**Şekil 2.13.** Durum denetimsiz otomatik IP yapılandırması trafiği.

Bu yöntemde sadece ağa ve internete bağlanılması isteniyorsa, DHCP sunucusu kullanmaya gerek kalmamaktadır. Bu yöntemin bazı sakıncaları da vardır. DHCP sunucusu kullanılmadığı için, hangi bilgisayarın hangi IP adresini aldığı bilgisi tutulamamaktadır. Diğer taraftan, DHCP sunucusu kullanılmazsa, istemci bilgisayarlara NTP sunucusu veya TFTP (Trivial File Transfer Protocol ~ Basit Dosya Transfer

Protokolü) sunucusu gibi bilgileri göndermek mümkün olmamaktadır (Thomson vd., 1998; Droms, 1997).

**Dolaşım:** İstemcilerin farklı IP ağlarında aynı IP adresi ve yetkileri ile dolaşımını sağlamak, özellikle taşınabilir bilgisayarların sayısının artmasından sonra bir ihtiyaç halini almıştır. Bu konu, ilk defa 1996 yılında RFC 2002 ile "IP Mobility Support" başlığında resmi olarak gündeme gelmiştir. IPv6'da bu soruna da çözüm getirilmiştir. IPv6'da mobil istemciler herhangi bir ek protokol veya yönlendirici desteği olmadan bir ağdan diğerine geçiş yapabilirler. Bu geçiş sırasında herhangi bir adres değişikliğine ihtiyaç duyulmamaktadır (Johnson vd., 2004).

**Yeni başlık yapısı:** IP ağlarında her bilgisayarın kendisine özel bir IP adresi olması gerekmektedir. Dolayısıyla IP ağlarında bilgisayarlar, birbirlerinin IP adreslerine veri göndererek haberleşirler. İnternet üzerinden e-posta gönderildiğinde, bir web sayfası görüntülendiğinde, web üzerinden alışveriş yapıldığında veya benzeri işlemlerde, aslında ağ üzerinde gerçekleşen işlem sadece, farklı IP adreslerine sahip olan bilgisayarlar arasında gidip gelen veri trafiğidir.

IP ağlarında, bir verinin bir bilgisayardan başka bir bilgisayara gönderilmesi için, verinin paketlenmesi gerekir. Gerçek hayattaki kargo paketleme işlemine benzetilebilecek olan bu veri paketleme işlemi sırasında gönderilmek istenen verinin üzerine bir başlık bilgisi eklenir. Bu başlıkta; veriyi gönderenin IP adresi, alıcının IP adresi, verinin toplam boyutu, verinin önceliği, kullanılan IP sürümü, vb. bilgiler bulunur.

Bir IP paketinin, kaynak adresten hedefe gidinceye kadar, ağ üzerinde bazen çok sayıda ara yönlendirici veya anahtar cihazlarından geçmesi gerekebilir. Bu cihazlar paket taşıma işlemi yaparken, genellikle IP paketlerindeki başlık bilgisine göre davranış (paketlerin sınıflandırılması veya önceliklendirilmesi gibi) gösterirler. Dolayısıyla IP ağlarında, veri paketlerinin kaynaktan hedefe kadar sağlıklı ve performanslı olarak ulaştırılması konusunda IP başlıkları hayati önem kazanmaktadır.

IPv6'da başlık yapısı, IPv4'e göre oldukça değiştirilmiştir. Özellikle başlık yapısının standart boyutta (IPv4'ün başlık boyutu değişkendir) olması, yönlendiricilerin ve istemcilerin trafik işlem yükünü oldukça azaltmaktadır. IPv4'te yönlendiriciler, başlık içerisindeki başlığın boyutunu belirten değeri okuduktan sonra başlığın boyutunu hesaplamaktadır. Oysa IPv6'da başlık boyutu standart olduğu için bu ilave hesaplama yükü azalmaktadır. IPv6 adresleri IPv4 adresine göre dört kat büyük olmasına rağmen, IPv6 başlığı IPv4 başlığına göre sadece iki kat büyüktür. IPv4 başlığında bulunan, şu anda kullanılmayan ancak ileriye dönük kullanma ihtimali nedeniyle rezerve edilmiş alanlar ve etkin kullanılmayan alanlar kaldırılmış, bunların yerine daha yalın ve işlevsel bir başlık yapısı tasarlanmıştır.

IPv6 başlık yapısındaki bir yenilik de gerektiğinde başlığın genişletilebilir olmasıdır. Bu sayede özel bir durum yoksa oldukça sade bir paket oluşturulmakta ancak ihtiyaç oluşması halinde bazı bilgiler ilave başlıklar halinde pakete eklenebilmektedir. Bu yapı, hem başlığın yalın yapısının bozulmamasını sağlamakta hem de ileriye dönük olarak protokolün esnek olmasını sağlamaktadır (Deering vd., 1998).

Çizelge 2.7’de, IPv4 ile IPv6 protokollerinin bazı önemli farklı noktaları belirtilmiştir (Davies, 2008).

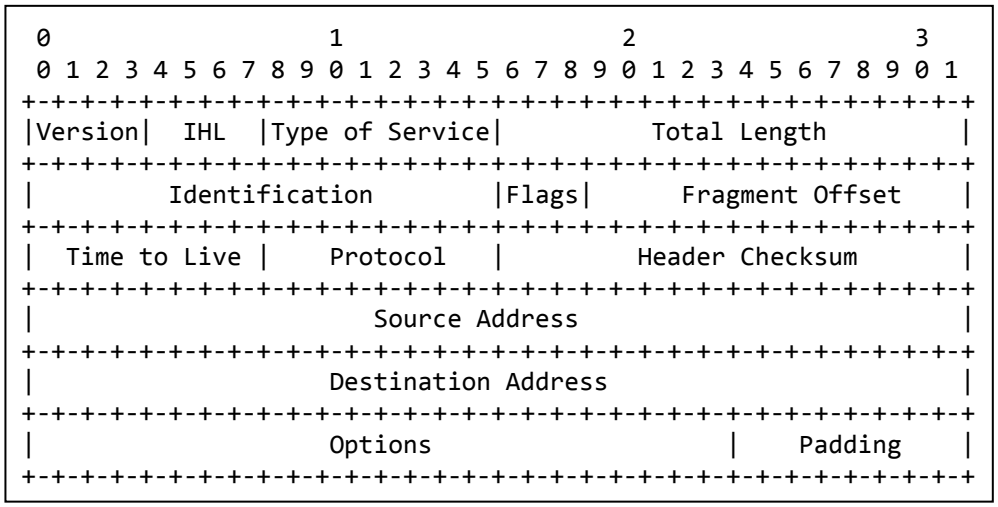
**Çizelge 2.7.** IPv4 ve IPv6 protokollerinin önemli farkları.

| IPv4 | IPv6 |
|---|---|
| Hedef ve kaynak adresleri 32 bittir. (4 bayt) | Hedef ve kaynak adresleri 128 bittir. (16 bayt) |
| IPSec başlık desteği seçimliktir. | IPSec başlığı standarttır. |
| Başlıkta yönlendiricilerin trafik önceliklendirmesi yapabilmesi için akış etiketi yoktur. | Başlıkta yönlendiricilerin trafik önceliklendirmesi yapabilmesi için özel bir akış etiketi alanı vardır. |
| Trafikte parçalama (fragmentation) hem göndericide hem de yol üzerindeki yönlendiricilerde yapılmaktadır. Bu da yönlendirme performansını düşürmektedir. | Trafikte parçalama sadece gönderici tarafından yapılmaktadır. |
| Bağlantı katmanı paket boyutu gerekliliği yoktur ve 576 baytlık paketler halinde yeniden oluşturulmalıdır. | Bağlantı katmanı 1280 bayt paket desteklemelidir ve 1500 baytlık paket olarak yeniden oluşturulabilir. |
| Başlık, özet bilgisi içerir. | Başlık özet bilgisi içermez. |
| Başlık, özel durumlar için seçenekler içerir. | Seçimlik başlık verilerinin tamamı eklenti başlıklarına taşınmıştır. Sadece gerek varsa kullanılır. |
| Bir IPv4 adresinin bağlantı katmanı adresini çözümlemek için ARP (Address Resolution Protocol ~ Adres Çözümleme Protokolü) protokolü kullanır. | ARP yerine çoklu yayın (multicast) ile komşu sorgulama mesajları (Neighbor Solicitation Message – NS) kullanır. |
| Yerel alt ağ grup üyeliği yönetimi için IGMP (Internet Group Management Protocol ~ İnternet Grup Yönetim Protokolü) kullanır. | IGMP, MLD (Multicast Listener Discovery ~ Çokluyayın Dinleyici Keşfi) mesajları ile değiştirilmiştir. |
| En iyi varsayılan ağ geçidini belirlemek için ICMP (Internet Control Message Protocol ~ İnternet Denetim Mesaj Protokolü) yönlendirici keşfi kullanılır ve seçimliktir. | ICMPv4 yönlendirici keşfi yerine, ICMPv6 yönlendirici sorgulama (Router Solicitation) ve yönlendirici duyuru (Router Advertisement) ile getirilmiştir ve gereklidir. |
| Ağdaki tüm istemcilere trafik göndermek için yayın (broadcast) adresi kullanılır. | IPv6 yayın adresi yoktur. Bunun yerine, bağlantı-yerel havuzu tüm-istemciler çoklu yayın adresi kullanılır. |
| IP yapılandırması ya elle yapılmalıdır veya DHCP kullanılmalıdır. | IPv4'teki yöntemlere ilave olarak durum denetimsiz otomatik yapılandırma gelmiştir. |
| DNS'te alan adlarını IP adresine çevirmek için A kaydı kullanılır. | DNS'te alan adlarını IP adresine çevirmek için AAAA kaydı kullanılır. |
| DNS'te IPv4 kayıtlarını alan adlarına çevirmek için IN-ADDR.ARPA üzerinde, işaretçi (PTR) kaydı kullanır. | DNS'te IPv6 kayıtlarını alan adlarına çevirmek için IP6.ARPA üzerinde, işaretçi (PTR) kaydı kullanır. |

### 2.4.1 IPv4 ve IPv6 paketlerinin başlık yapısının karşılaştırılması

IP ağlarında, 2.4.2bir bilgisayardan diğer bir bilgisayara veri gönderilirken, verinin önüne başlık bilgilerinin (gönderenin IP adresi, alıcının IP adresi, verinin önceliği, vb. bilgiler) eklenmesi ile oluşturulan haline "IP paketi" denilir.

"Paket başlığı", paketlerin ağ üzerinde doğru ve performanslı iletilebilmesi için her pakete protokol tarafından eklenen bilgilerdir. IPv4 ile IPv6'nın paket başlık yapısı oldukça farklıdır. Şekil 2.14'te IPv4 paketlerinin başlık yapısı gösterilmiştir.




**Şekil 2.14.** IPv4 paket başlıkları (RFC 791).

IPv4 başlığında 14 adet alan bulunmaktadır. Paket başlığının uzunluğu duruma göre değişmektedir. Paket başlığındaki alanların ne amaçla kullanıldıkları aşağıda belirtilmiştir (Şahin, 2006).

**Sürüm (Version):** İnternet protokolünün sürümünü belirtmektedir. Büyüklüğü dört bittir. IPv4 için değeri ikili sayı sisteminde "0100" olmaktadır.

**IHL (IP Header Length ~ IP Başlık Uzunluğu):** IP başlık uzunluğunu belirtmektedir. Bu bilgiyi taşımak üzere dört bitlik alan ayrılmıştır. En küçük başlık boyutu 20 Byte'tır. Tüm alanlardaki bitlerin kullanılması ile oluşturulabilecek olan en büyük başlık boyutu da 60 Byte'tır.

**Hizmetin Tipi (Type of Service):** Bazı özel uygulamalar tarafından kullanılabilecek bir alandır. Uzunluğu sekiz bitten oluşmaktadır.

**Toplam Uzunluk (Total Length):** Başlık büyüklüğü ve veri boyutunu da sayarak tüm IP paketinin uzunluğunu belirten değerdir. Bu değeri ifade etmek için 16 bit kullanılır.

**Tanımlama (Identification):** Paketlerin ilişkilendirmesini sağlayabilmek için kullanılan 16 bitlik rastgele bir sayıdır.

**Bayraklar (Flags):** Paketlerin parçalara ayrılıp ayrılmadığı bilgisi ve bunların kontrolünü sağlamak için kullanılan üç bitlik bayrak değeridir.

**Parçalanma Başlangıcı (Fragment Offset):** IP veri paketinin başlangıç yerini belirten 13 bit ile ifade edilen alandır.

**Yaşam Süresi (Time to Live):** Yönlendirilme sırasında verinin aktarılacağı en fazla düğüm sayısını belirtmektedir. Bu sayı aşılırsa paket iletilememiş varsayılır ve yok edilir. Bu bilgi başlıkta 8 bit olarak tutulur. Dolayısıyla bir paketin en fazla aktarılabileceği yönlendirici sayısı 255 (0'dan başlandığı için, 256 yerine 255 olabilir) olmaktadır.

**Protokol (Protocol):** IP paketinin içerisinde taşınacak olan üst seviyedeki protokolü belirtir. 8 bitlik uzunluktadır.

**Başlık Özet Kontrolü (Header Checksum):** Verinin, taşıma sırasında herhangi bir bozulmaya uğrayıp uğramadığını kontrol etmek için tutulan alandır, 8 bit uzunluğundadır.

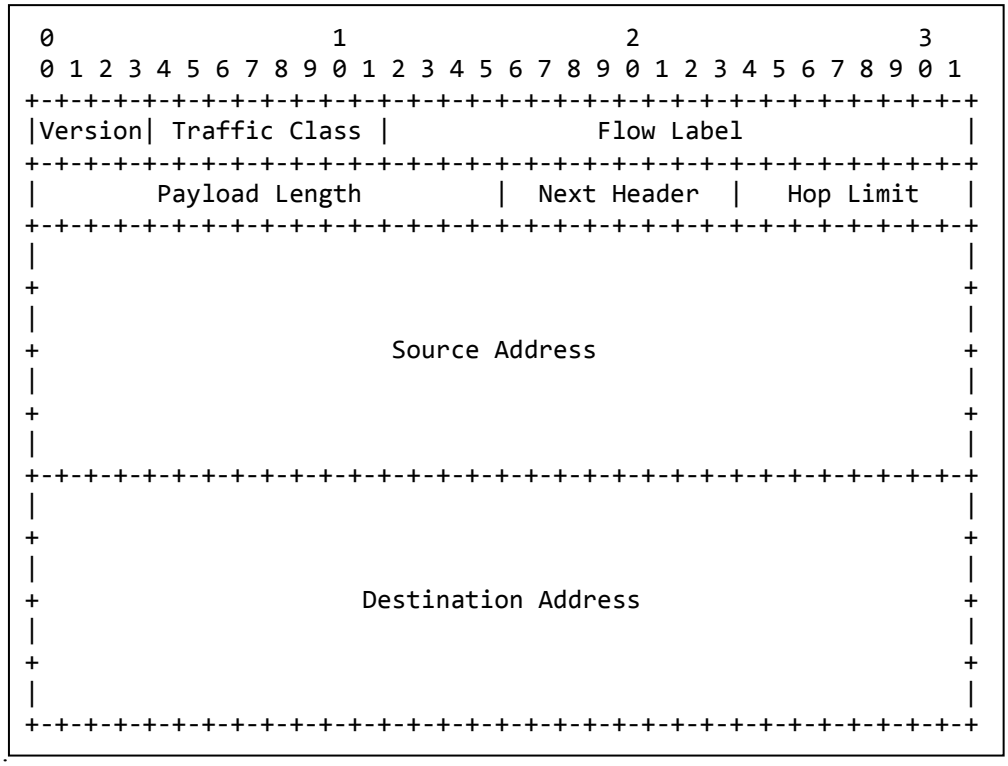
**Kaynak Adres (Source Address):** Veriyi gönderen tarafın IP adresi bilgisini taşıyan alandır. 32 bit uzunluğundadır.

**Hedef Adres (Destination Address):** Veriyi alacak olan tarafın IP adresi bilgisini taşıyan alandır. 32 bit uzunluğundadır.

**Özellikler (Options):** IP başlığına bazı özellikleri eklemek için koyulan bir alandır. Herhangi bir özellik eklenmemiş ise 0 bittir. Ancak eklenen özelliklere göre, 40 Byte'a kadar çıkabilir.

**Dolgu (Padding):** IP paket başlığının 32 bitin katları şeklinde olmasını sağlayan alandır. Boyutu kullanılan başlığa göre değişmektedir.

IPv4 başlığında 14 tane alan bulunmakta iken, Sadeleştirilmiş olan IPv6 başlığında 8 tane alan bulunmaktadır. Paket başlığının uzunluğu IPv4'te olduğu gibi değişken değil, 40 baytlık uzunlukta ve sabittir. Şekil 2.15'te IPv6 paketlerinin başlık yapısı gösterilmiştir. (Şahin, 2006)




**Şekil 2.15.** IPv6 paket başlıkları (RFC 2460 ve 2474).

IPv6 başlığındaki alanların kullanım amaçları aşağıda açıklanmıştır (Şahin, 2006):

**Sürüm (Version):** Bu alan IPv4'teki sürüm alanı ile aynı görevdedir. Protokolün sürümünü belirtir. 4 bit uzunluğundadır. IPv6 için, ikilik sayı sisteminde "0110" (onluk sistemde 6) değerini almaktadır.

**Trafik Sınıfı (Traffic Class):** 8 bitlik bir alandır. IPv4'teki hizmet tipi alanı yerine getirilmiştir. IPv6 paketleri arasındaki değişik sınıf ve öncelikleri belirtme görevini üstlenmektedir.

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

**Veri Uzunluğu (Payload Length):** IPv6 başlığını takip eden tüm paketin uzunluğunu 16 bitlik bir alanda ifade etmektedir. Eğer pakette bir veya birden fazla eklenti başlığı varsa onlarda bu uzunluğa dâhil edilir. IPv4 başlığındaki karşılığı toplam uzunluk alanıdır.

**Sonraki Başlık (Next Header):** 8 bitlik bu alanda IPv6 başlığından hemen sonra gelen başlık çeşidi belirtilmektedir. Bu herhangi bir eklenti başlığı olabilir veya TCP, UDP (User Datagram Protocol ~ Kullanıcı Veri Bloğu Protokolü) gibi daha üst seviyelerden bir protokol olabilir. IPv4'te protokol alanı adıyla geçmektedir.

**Atlama Limiti (Hop Limit):** 8 bitlik bir değerle ifade edilmektedir. Paket her bir düğümden geçtikçe atlama limiti sayısı bir eksiltilmektedir. Bu sayı sıfır olduğu zaman paket çöpe atılmaktadır. IPv4'teki karşılığı TTL (Time To Live ~ Yaşam Süresi) alanıdır.

**Kaynak Adres (Source Address):** Paketin kaynak adresini belirten 128 bitlik alandır.

**Hedef Adres (Destination Address):** Paketin hedef adresini belirten 128 bitlik alandır. Eğer yönlendirici başlığı varsa, hedef adres en son alıcının adresi değildir.

IPv4'teki değişken boyutlu başlık, ağ cihazlarına ilave iş yükü getirmektedir. IPv4 paketlerinin geçtiği her cihazda başlık boyutu yeniden hesaplanmaktadır. IPv6'nın başlık yapısının sade ve sabit boyutlu olması, paket yönlendirmeyi kolaylaştıracağı için, ağ cihazlarının yükünün azalmasını sağlayacaktır. IPv6'da yeniden tasarlanmış olan başlık yapısının avantajları, Başlık 2.4.3'de açıklanmıştır. IPv4 ve IPv6 başlık yapılarının karşılaştırması ise Çizelge 2.8'de verilmiştir.

**Çizelge 2.8.** IPv4 ve IPv6 başlık yapıları karşılaştırması.

| IPv4 Başlık Alanı | IPv6'da Durumu |
|---|---|
| **Version** | Durmaktadır. İçerik olarak, "4" yerine "6" yazmaktadır. |
| **Internet Header Length** | Kaldırılmıştır. Başlık boyutu sabit (40 bayt) olduğundan, IPv4'te başlık boyutunu belirtmek için kullanılan bu alana gerek kalmamıştır. |
| **Type of Service** | Kaldırılmıştır. Trafiği sınıflandırmak için kullanılan bu alanın yerine, IPv6 başlığında, **Traffic Class** alanı vardır. |
| **Total Length** | Paketin toplam boyutunu belirtmek için kullanılan bu alanın yerine, IPv6 başlığında sadece veri kısmının boyutunu belirten, **Payload Length** alanı bulunmaktadır. |
| **Identification** | Kaldırılmıştır. Parçalanmış olarak aktarılan paketlerin sıralanması amacıyla ihtiyaç duyulan bu bilgiler, seçimlik olan "**Fragmentation**" isimli başlık uzantısına yazılmaktadır. |
| **Flags** | |
| **Fragment Offset** | |
| **Time to Live** | Paketin yaşam süresini belirlemek için kullanılan bu alanın yerine, "**Hop Limit**" alanı kullanılmaktadır. |
| **Protocol** | Taşınan verinin protokolünü belirtmek için kullanılan bu alanın yerine, "**Next Header**" alanı kullanılmaktadır. |
| **Header Checksum** | Kaldırılmıştır. Hata denetimi amacıyla başlığın özetini yazmak için kullanılan bu alana gerek kalmamıştır. IPv6'da tüm paketin bit seviyesinde hata denetimi bir alt katmanda yapılmaktadır. |
| **Source Address** | Durmaktadır. 32 bit yerine 128 bit olarak büyütülmüştür. |
| **Destination Address** | Durmaktadır. 32 bit yerine 128 bit olarak büyütülmüştür. |
| **Options** | Kaldırılmıştır. Gerekli olduğunda, IPv6'da uzantılar bölümünde kullanılmaktadır. |
| **Padding** | Kaldırılmıştır. IPv4'te boşluk doldurmak için kullanılan bu alana IPv6'da gerek kalmamıştır. |

### 2.4.3 IPv6 başlık yapısının IPv4 başlık yapısına göre avantajları

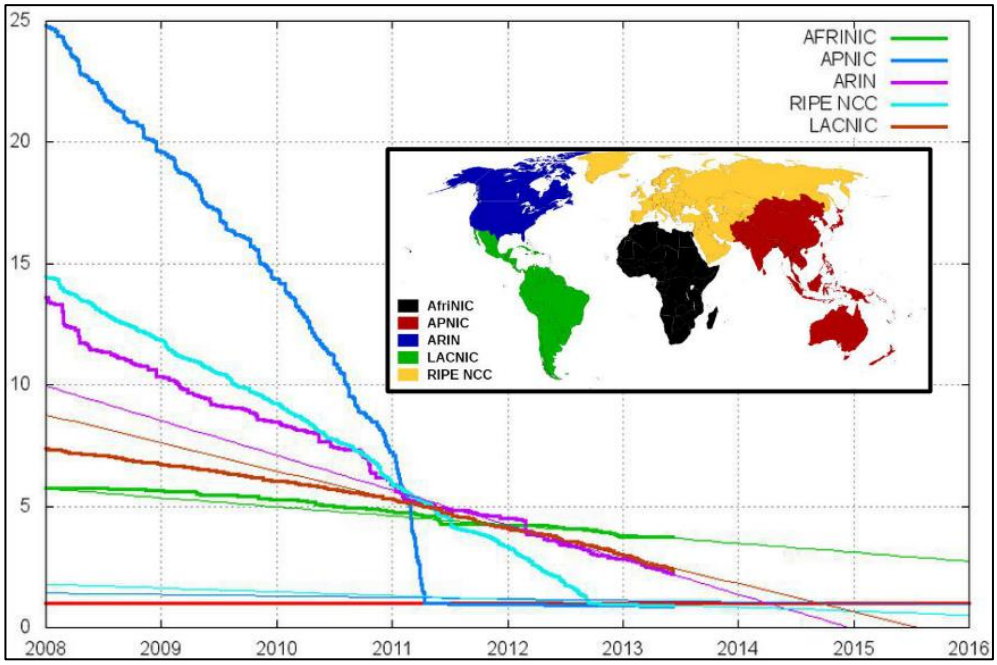
IPv6 paket başlık yapısının IPv4'e göre avantajları şöyledir:

- **Sade olması:** IPv4 başlığında bulunan, ileride kullanma ihtimaliyle konulan ancak kullanılmayan alanlar kaldırılmıştır. IPv6 başlığında, gerçekten ihtiyaç olan alanlar bırakılmıştır. Seçimlik olan başlık seçenekleri ise, eklenti başlıklarına taşınmıştır.
- **Başlık bilgisinin sabit uzunlukta olması:** IPv4 başlığı, kullanılan IP özelliklerine göre, 20-60 bayt arasında değişmektedir. IPv6 başlığı ise, sabit olarak 40 bayt uzunluğundadır. Başlık uzunluğunun sabit olması, ağdaki yönlendiricilerin her bir paket için başlık boyutunu yeniden hesaplama için harcanan işgücünü kaldırmıştır. Bu nedenle, IPv6 paketleri daha performanslı olarak iletilebilmektedir.
- **Başlığa akış etiketleri alanının eklenmesi:** Bu sayede, yönlendiriciler trafik akışındaki paketleri tanımlayabilir ve trafik önceliklendirmesini buna göre yapabilir. Trafik önceliklendirme, paket başlık bilgisindeki "Trafik Sınıfı" ve "Akış Etiketi" alanlarına göre yapıldığından, paketlerin veri kısmı şifrelenmiş dahi olsa, önceliklendirme başarılı olarak yapılabilir. Özellikle akış etiketi özelliği sayesinde, iki uç arasında kurulan bir oturum süresince geçen tüm paketler aynı akış etiketi ile etiketleneceğinden, aktif oturum süresince trafiğin tamamı aynı hizmet önceliklendirmesine tabi tutulabilecektir.
- **Eklenti başlıkları özelliği:** IPv6'da, seçimlik başlık verilerinin tamamı eklenti başlıklarına taşındığından; sadece gerek varsa kullanılır. IPv4'te ise, eklenti başlığı özelliği olmadığından, kullanılsa da kullanılmasa da başlık, özel durumlar için seçenekler içerir. Bu da başlığın gereksiz yere büyümesine neden olur ve performans kaybına sebep olabilir.
- **Sağlama toplamı (checksum) alanının kaldırılması:** IPv4 başlığında, paketin doğru ulaşıp ulaşmadığının denetimi için kullanılan "checksum" alanı, IPv6 başlığında kaldırılmıştır. Hata denetimi için sağlama toplamı hesaplaması işlemi zaten IP üzerinde çalışan diğer protokollerde yapılmaktadır. Bu sayede, IP seviyesinde her iletilen paket için, ağ üzerindeki cihazların yeniden "sağlama toplamı hesaplaması" yapmasından dolayı harcanan işgücü azaltılmıştır.

## 2.5 IPv6'nın Günümüzdeki Kullanımı

IPv6'nın çıkışından itibaren oldukça uzun zaman geçmesine ve IPv4 adreslerinin biteceği çok önceden belli olmasına rağmen; IPv6 yaygınlaşamamıştır. Bunun birçok sebebi vardır. IPv6 adresleme yapısının IPv4'e göre daha farklı olması, kurumları uzun süre IPv6 ağına bağlanmaktan alıkoyan nedenlerden birisidir. Diğer taraftan, IPv4 ile uzun süredir kolay bir şekilde çalıştırılan sistemlerin IPv6 ağında sağlıklı çalışıp çalışmayacağının tedirginliği, yatırım maliyetleri, eğitim ihtiyacı, güvenlik açısından yaşanan endişeler gibi nedenler de geçişi yavaşlatmıştır (Yadav A. vd., 2012).

Son 5 adet "**/8**"[1] IPv4 adres aralığı, dünya üzerinde IP dağıtım işlerinden sorumlu olan IANA tarafından, 3 Şubat 2011 tarihinde, 5 adet bölgesel internet kayıtçılarına birer blok olarak verilmiştir. Her bir yerel IP dağıtım yetkilisi, kendilerine atanmış olan ülkelerde son IPv4 bloklarını dağıtmaktadır. Şekil 2.16'da bölgesel internet kayıtçılarının elindeki /8 IPv4 adresi miktarının grafiği gösterilmiştir.

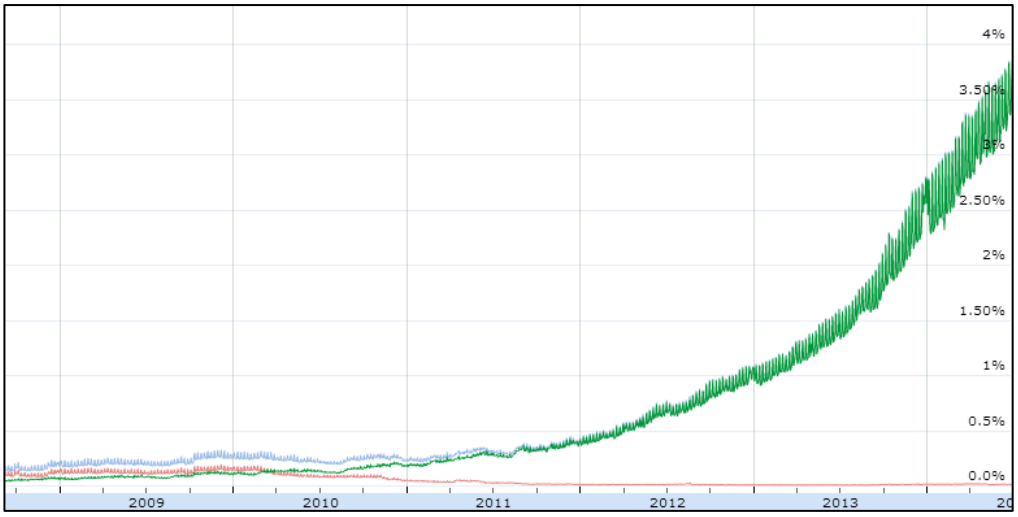



**Şekil 2.16.** Bölgesel internet kayıtçılarının elindeki /8 IPv4 adreslerinin miktarı.

[1] 4 oktetten oluşan IPv4 adreslerinde, ilk oktetin sabit olduğu adres aralıklarına, kısaca /8 denilir. Örneğin: 10.0.0.0 adresinden, 10.255.255.255 adresine kadar kullanılan IP adreslerinin tamamı, 10.0.0.0/8 veya kısaca 10/8 olarak gösterilmektedir. Bu konuda detaylı bilgi, bölüm 2.2.1.1'de verilmiştir.

Bölgesel internet kayıtçılarındaki IPv4 adresleri de hızla tükenmektedir. IPv4 adresi bittiği için IPv4 adresi alamayan, yalnızca IPv6 adresine sahip olan kurumlar, İnternet üzerinde IPv4 kullanan kurumlara normal yollardan bağlanamayacaklardır.

Şekil 2.17'de Google'a IPv6 üzerinden gelen isteklerin istatistiği gösterilmiştir. Google, İnternet üzerinde en yaygın kullanılan arama motorudur. Google'a IPv6 üzerinden gelen isteklerin tamamı, toplam isteklerin ancak **%4** kadarını oluşturmaktadır. Bu da dünya genelinde IPv6 kullanımının yaygınlığı konusunda fikir vermektedir (http://www.google.com/intl/en/ipv6/statistics, 30.06.2014).




**Şekil 2.17.** Google'a IPv6 üzerinden gelen isteklerin istatistiği.

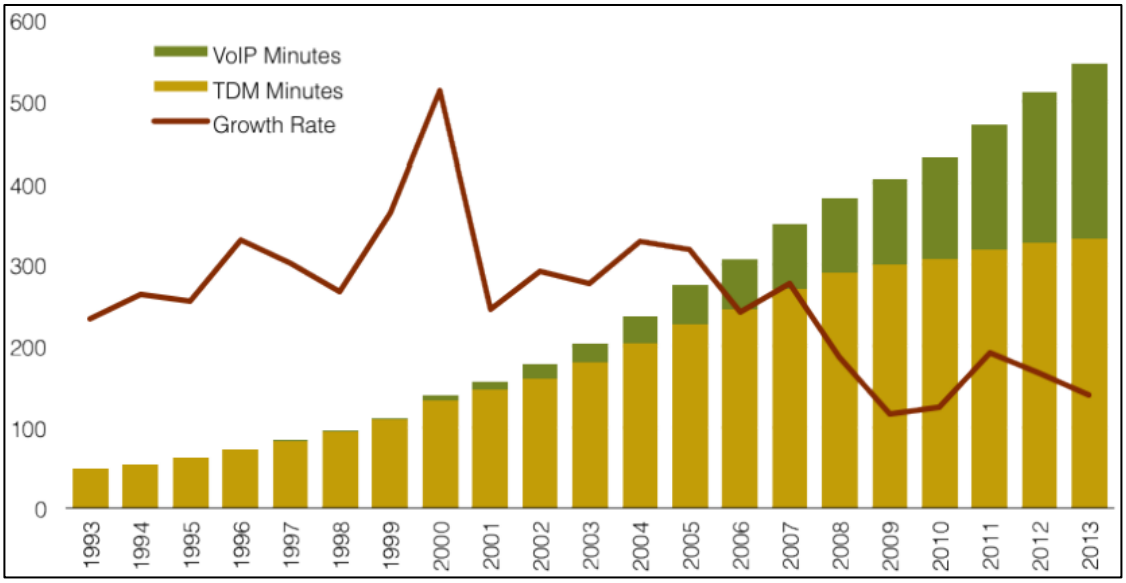
IPv6 adreslerinin kullanımı konusunda, IPv6 adresi alan kurumların sayısı tam doğru bir istatistik sağlamamaktadır. Çünkü kurumlar IPv6 adreslerini teslim alsa bile aktif kullanmıyor olabilirler. Bu nedenle; kullanım istatistikleri, resmi belgelerden daha gerçekçi sonuçlar verebilmektedir.

IPv4 adreslerinin bitiyor olması nedeniyle, IPv6 protokolü kullanımı hızla yaygınlaşacağından, teknik anlamda ağların uygunluğu konusunda çalışılması gerekmektedir. IPv4 ile eskiden beri kullanılmakta olan uygulamaların da IPv6'da yeniden çalıştırılması, yapılandırılması ve test edilmesi gerekmektedir. Bu çalışmada ele alınmış olan, "IPv6 üzerinde ses taşıma" konusunda yapılan uygulamalar, 3. Bölüm'den itibaren açıklanmıştır.

# 3. BÖLÜM: IP ÜZERİNDEN SES TAŞIMA (VOIP) PROTOKOLLERİ

Ses ve video gibi verileri uzak mesafede bir yere ulaştırmak için en hızlı ve güvenli yol, günümüzde veri ağı şebekeleridir. Ev telefonu gibi analog sistemlerde, cep telefonu gibi mobil sistemlerde dahi, aboneden alınan ses sayısala çevrildikten sonra, uzak mesafelere çoğunlukla İnternet Protokolü (IP) üzerinden aktarılmaktadır. Canlı ses iletiminin, veri şebekeleri üzerinden aktarılması, maliyeti çok fazla düşürmektedir. İş yükü açısından bakıldığında ise klasik İnternet trafiğinin yanında, ses trafiği çok küçük kalmakta, dolayısıyla veri şebekelerine getireceği iş yükü ticari açıdan önemli olmamaktadır.

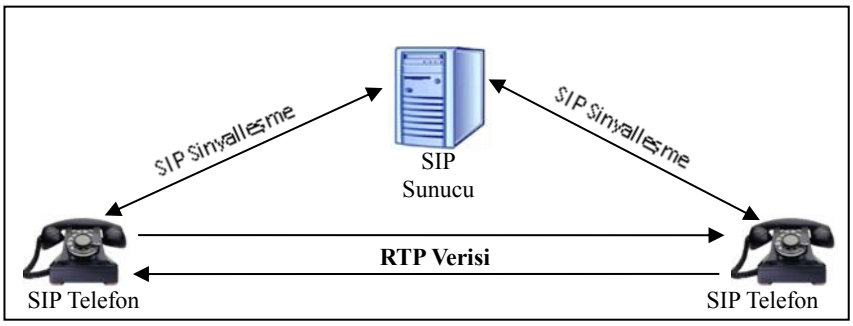
Şekil 3.1'de TeleGeography[1] firması tarafından 2013 yılında yayınlanmış olan, uluslararası telefon görüşme süreleri görülmektedir. Şekilde "*VoIP minutes*" olarak belirtilen değerler, telefon firmaları aracılığıyla ve IP üzerinden yapılan; "*TDM Minutes*" olarak belirtilen değerler ise klasik telefon sistemleri üzerinden yapılan görüşme süreleridir. 2000'li yıllara kadar VoIP çok az kullanılmakta, sonrasında ise hızlı bir yükselişe geçmektedir. Dikey eksenin birimi, "*milyar dakika*" cinsindedir.




**Şekil 3.1.** Uluslararası TDM ve VoIP telefon görüşme süreleri.

[1] TeleGeography, 1989 yılından beri telekomünikasyon alanında pazar payı araştırması yapan; ABD, İngiltere ve Singapur'da ofisleri bulunan bir danışmanlık firmadır (http://www.telegeography.com, Haziran 2014).

IP üzerinden ses ve görüntü taşıma (VoIP ~ Voice Over IP) uygulamalarında, trafiğin kontrolü ve veri paketlerinin iletimi ayrı protokoller ile sağlanır. Ses verisi RTP (Real-Time Transfer Protocol ~ Gerçek Zamanlı Taşıma Protokolü) ile aktarılırken, oturum yönetimi için H.323, SIP, MGCP (Media Gateway Control Protocol ~ Medya Geçidi Denetim Protokolü) gibi protokoller kullanılır. Oturum yönetim işlemlerine sinyalleşme denir. Şekil 3.2'de SIP için, iletişim ve sinyalleşme kullanımı gösterilmiştir. H.323, MGCP, vb. diğer protokollerde de sinyalleşme, benzer şekilde çalışmaktadır.




**Şekil 3.2.** Örnek RTP ve SIP iletişimi gösterimi.

RTP ilk defa IETF tarafından 1996 yılında RFC1889 ile duyurulmuş, daha sonra 2003 yılında RFC3550 ile güncellenmiştir. RTCP (Real-Time Transfer Control Protocol ~ Gerçek Zamanlı Taşıma Denetim Protokolü) ile birlikte çalışmaktadır. RTP gerçek zamanlı veri iletimi ile ilgilenirken; RTCP veri iletimini izler. RTCP sayesinde, paket kaybı olup olmadığı tespit edilir, istatistikler oluşturulur, QoS durumu izlenir. Bir VoIP iletişiminde, biri gidiş biri geliş olmak üzere iki RTP ve bir adet te RTCP oturumu oluşturulur. IP üzerinden ses taşımak için RTP ile beraber en yaygın kullanılan protokoller SIP ve H.323'tür (Schulzrinne vd., 1996; Schulzrinne vd., 2003).

H.323 standardı 1996 yılında ITU-T tarafından yerel ağlarda (LAN) çoklu ortam trafiğini taşımak için geliştirilmiştir. Kısa süre içerisinde WAN'da (Wide Area Network ~ Geniş Alan Ağı) da çok kullanılan bir standart haline gelmiştir. ISDN (Integrated Services Digital Network ~ Bütünleşik Hizmetler Sayısal Ağı) uyumlu olması nedeniyle PSTN (Public Switched Telephone Network ~ Genel Anahtarlamalı Telefon Şebekesi) şebekelerde kullanılmıştır. Protokolün güncel sürümü 2009 yılında yayınlanmıştır.

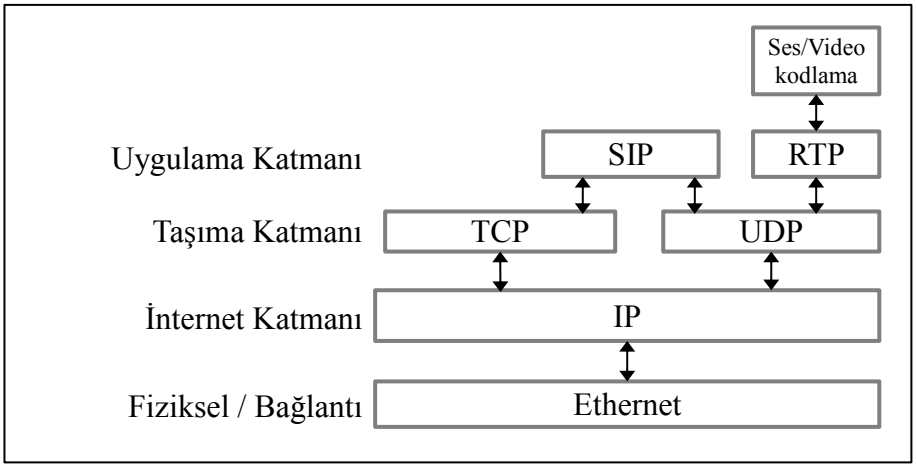
SIP, IETF tarafından geliştirilen ve IP üzerinden iki veya daha fazla uç nokta arasında çağrı kurma, tutma ve sonlandırma işlemleri için kullanılabilen, düz metin içerikli ve şifrelenmemiş bir protokoldür. 1999 yılında RFC 2543 ile yayınlanmıştır. 2002 yılında, RFC 3261 ile güncel sürümünü almıştır. Tıpkı diğer VoIP protokolleri (H.323, MGCP, vb.) gibi paket anahtarlamalı ağlarda sinyalleşme ve oturum yönetimi işlevlerini yerine getirir. Aranılan uç noktanın konumunu, durumunu, ortam yeteneklerini sorgulayarak arayan ve aranılan noktalar arasında çağrı kurulması, çağrıların aktarılması ve sonlandırılması işlemlerini gerçekleştirebilir (Haki, 2007).

SIP, HTTP (Hypertext Transfer Protocol ~ Hareketli Metin Taşıma Protokolü) protokolüne çok benzer düz metin bir protokoldür. Oturum açar, oturum parametrelerini değiştirir, oturumu sonlandırır. Oturumlar IP telefon çağrıları, sunumlar veya konferans şeklinde olabilir, mevcut bir oturuma kullanıcı çağırabilir (Rosenberg vd., 2002).

## 3.1 Oturum Başlatma Protokolü'ne Genel Bakış

SIP ile ilgili ilk taslak çalışma 1997 yılında bir IETF çalışma grubu olan MMUSIC (Multi-Party Multimedia Session Control Working Group) tarafından yapılmıştır. Mart 1999'da ise standart halini almış ve RFC 2543 ile yayınlanmıştır. Daha sonra, 2002 yılında RFC 3261 ile yeniden tanımlanarak güncel halini almıştır.

SIP, uygulama katmanında çalışır. HTTP ve SMTP protokollerine çok benzer düz metin tabanlı bir protokoldür. Ağ üzerindeki iki bilgisayar arasında oturum açmak, oturum parametrelerini değiştirmek, oturumu sonlandırmak gibi işlevleri vardır. Oturumlar; IP telefon çağrıları, çoklu ortam sunumlar, anında mesajlaşma iletileri veya konferans şeklinde olabilir. Mevcut bir oturuma kullanıcı çağırabilir, medya ekleyebilir, çıkarabilir. Şekil 3.3'te, OSI (Open Systems Interconnection ~ Açık Sistemler Ara Bağlantısı) modeli katmanlarında SIP'in yeri görülmektedir. SIP, TCP üzerinde çalışabildiği gibi; kendi hata düzeltme mekanizmaları olması nedeniyle, hata düzeltme mekanizması olmayan UDP üzerinde de çalıştırılabilir (Johnston, 2004).




**Şekil 3.3.** SIP'in katmanlı mimaride gösterimi.

SIP'in düz metin tabanlı olması, protokolün esnekliğini artırmış ve bu nedenle SIP, günümüzde IP Telefonu için en yaygın kullanılan protokol halini almıştır.
Şekil 3.4'te örnek bir SIP iletişim mesajı görülmektedir.

```
      SIP/2.0 200 OK
      Via:  SIP/2.0/UDP  [fe80:0:0:0:6ced:a424:208e:9ec8]:5060;branch=z9hG4bK-363832-
e05a245691d82fdd703ee83f17a81be8;received=fe80::6ced:a424:208e:9ec8%wlan0
      From: "netbook" <sip:netbook@[fe80::221:ff:febd:ce5c]>;tag=456dd488
      To: "netbook" <sip:netbook@[fe80::221:ff:febd:ce5c]>;tag=as5652adf7
      Call-ID: 5667d0a95291e18205c3bd2c7f222c94@0:0:0:0:0:0:0:0
      CSeq: 747 REGISTER
      Server: Asterisk PBX 1.8.3.3-1digium1~natty
      Allow:  INVITE,  ACK,  CANCEL,  OPTIONS,  BYE,  REFER,  SUBSCRIBE,  NOTIFY,  INFO,
PUBLISH
      Supported: replaces, timer
      Expires: 600
      Contact:
<sip:netbook@[fe80:0:0:0:6ced:a424:208e:9ec8]:5060;transport=udp;registering_acc=[fe
80::221:ff:febd:ce5c]>;expires=600
      Date: Tue, 03 May 2011 05:30:39 GMT
      Content-Length: 0
```

**Şekil 3.4.** Örnek SIP iletim mesajı.

SIP, aslında kullanım amacı çok geniş olan bir protokoldür. Temel görevi; ağ üzerinde iki "uç" arasında oturum başlatmak ve yönetmektir. "Uç" adı verilen cihazlar; bilgisayar, telefon makinesi veya SIP destekleyen herhangi bir cihaz olabilir. Protokolün ana sinyalleşme fonksiyonları aşağıda listelenmiştir: (Johnston, 2004)

- Ağ üzerindeki bir uç cihazın yerinin tespiti,
- Çağrı yapılırken, diğer ucun oturumu kabul etmek isteyip istemediğinin öğrenilmesi,

- Oturum kurulmak istendiğinde, iki tarafın desteklediği medya bilgilerinin alış verişi,
- Kurulmuş oturumlardaki medya bilgilerinin değiştirilmesi,
- Kurulmuş medya oturumunun sonlandırılması.

Anında mesajlaşma uygulamalarını kullanabilmek için; SIP fonksiyonları iki ucun bulunabilirlik[1] bilgilerini de kullanabilecek şekilde genişletilmiştir. Bu fonksiyonlar;

- Bulunabilirlik bilgilerini yayınlama ve yükleme,
- Bulunabilirlik bilgilerinin talep edilmesi,
- Bulunabilirlik ve diğer benzeri olaylar ile ilgili bilgilendirme,
- Anında mesajlaşma iletilerinin aktarımı gibi başlıklarla verilebilir (Johnston, 2004).

## 3.2 Oturum Başlatma Protokolü Tercih Nedenleri

SIP ve H.323 protokolleri IP üzerinden gerçek zamanlı ses iletişiminde en yaygın kullanılan protokollerdir. SIP ise özellikle IP Telefon (İnternet Telefonu) sistemlerinde en yaygın kullanılan protokoldür.

SIP ile H.323 arasındaki temel fark; SIP'in HTTP gibi metin tabanlı çalışmasıdır. Oysa H.323 ikili kodlanmış (binary) olarak çalışan bir protokoldür. H.323'ün bu özelliği; daha küçük mesaj boyutu sağlamakta ancak karmaşık bir yapıya sebep olmaktadır. Bu açıdan bakıldığında SIP'in sadeliği; basit betikler ile izlenebilmesine, istatistiklerin rahat çıkarılabilmesine, sorunların daha rahat analiz edilebilmesine olanak sağlamaktadır. SIP protokolünün trafiği, ilave bir araca gerek kalmadan, trafiğin doğrudan kayıt edilmesi ile incelenebilir.

SIP'in H.323'e göre bir diğer farkı, H.323 aslında bir işaretleşme protokolü olmasına rağmen, SIP hem işaretleşme hem de gerçek zamanlı mesajlaşma protokolüdür. SIP'in bu özelliği mobil istemciler, yazılım telefonları, IP telefonları gibi farklı tipte istemcilerde kullanımını daha da çekici hale getirmektedir.

Güvenlik tarafından bakıldığında ise SIP'in esnek güvenlik çözümleri sunduğu

[1] Bulunabilirlik bilgisi (availability information): "çevrim içi / çevrim dışı durumu" , "kişisel rehberdeki kullanıcıların yer bilgileri", vb.

görülmektedir. SIP, birçok güvenlik mekanizması ile çalışacak şekilde tasarlanmıştır. Şifreleme, sertifika tabanlı kimlik doğrulama, güvensiz ara sunucular üzerinden sağlanan iletişimde uçtan uca mesaj bütünlüğü doğrulama gibi özelliklere destek verir. SIP'in bu tarz güvenlik mekanizmalarını geliştirmek gibi bir ihtiyacı da yoktur. Bir İnternet protokolü olduğundan, TLS[1] (Transport Layer Security ~ Taşıma Katmanı Güvenliği) gibi güvenlik protokollerini doğrudan kullanabilir (Johnston, 2004).

Çizelge 3.1'de SIP ile H.323 protokollerinin çağrı özellikleri açısından, bazı önemli farklı noktaları belirtilmiştir (Schulzrinne, 1998).

**Çizelge 3.1.** SIP ile H.323 çağrı özellikleri farkları

| **Çağrı özelliği** | **SIP** | **H.323** | **Açıklama** |
|---|---|---|---|
| Kontrollü transfer | Var | Yok | Hedef abone ile görüştükten sonra, onay verirse, beklemedeki çağrının aktarılması. |
| Çağrı tutma | Var[2] | Yok | Aktif çağrının, başka bir çağrı oluşturmak için bekletmeye alınması. |
| Çağrı park etme | Var | Yok | Aktif çağrının beklemeye alınmasıdır. Park edilmiş çağrıya özel olan bir numara, herhangi bir yerden tuşlanarak faklı yerden de çağrıya devam edilebilir. |
| Çağrı çekme | Var | Yok | Bir aboneye gelen çağrının, başka bir aboneden çekilmesi işlemidir. Çaldığı duyulan, yakındaki bir telefonu açmak için kullanılmaktadır. |

SIP, H.323'e benzer bir hizmet kümesi sağlar ancak çok daha sade olması, zengin genişletilebilirlik desteği ve daha iyi ölçeklenebilir olması gibi avantajları nedeniyle bu çalışmada VoIP protokolleri arasından tercih sebebi olmuştur.

[1] TLS, ağ üzerinden verilerin aktarılması sırasında şifrelenmesini sağlayan bir protokoldür. SSL protokolünün devamıdır. 1999 yılında, RFC 2246 ile 1.0 sürümü duyurulmuştur. 2008 yılında yayınlanan RFC 2008 ile 1.2 sürümünü almıştır.

[2] Session Description Protocol (SDP ~ Oturum Tanımlama Protokolü) sayesinde kullanılabilmektedir. SDP, 2006'da RFC 4566 ile yayınlanmıştır. SIP paketlerinin gövdesinde taşınabilen ve iki uç arasındaki iletişim sırasında uçların yetenekleri ve destekledikleri kodek (medya, codec) biçimlerinin tanımlanmasını sağlayan açık metin biçimli mesajlaşma kullanan bir protokoldür (Handley M., vd., 2006)

## 3.3 Oturum Başlatma Protokolü Bileşenleri

SIP haberleşmesinde farklı uygulamalar kullanılabilmektedir. Eğer az sayıda SIP destekli uç cihazların sesli iletişim sağlaması isteniyorsa, doğrudan bu cihazlar birbirleri ile başka bir donanım veya yazılıma ihtiyaç olmadan bağlanabilirler. Çok sayıda ucun birbiri ile haberleşmesi isteniyorsa, bu tarz durumlarda uçların birbirleri ile sağlıklı haberleşebilmesi için, sunucu sistemleri kullanmak daha kullanışlı olmaktadır.

SIP sistemlerinde temel olarak iki bileşen vardır:

- SIP Kullanıcı Ajanı (SIP User Agent)
- SIP Ağ Sunucusu (SIP Network Server)

**SIP Kullanıcı Ajanı:** Oturum başlatan, cevaplayan ve sonlandıran birimdir. Kendi içerisinde "Kullanıcı Ajanı İstemcisi (User Agent Client)" ve "Kullanıcı Ajanı Sunucusu (User Agent Server)" olmak üzere ikiye ayrılır. İstemci oturum davetini gönderir, sunucu ise oturuma cevap verir. SIP kullanıcı ajanı; herhangi bir bilgisayara yüklü olan SIP destekli yazılım telefonu (soft phone), SIP destekli bir anında mesajlaşma yazılımı, SIP destekli bir IP telefon donanımı (hard phone) veya SIP destekli bir etkileşimli sesli yanıt sistemi (IVR, Interactive Voice Response) olabilir. Bir SIP sunucusuna gerek olmadan, bu tarz cihazlar birbirleri ile haberleşme sağlayabilir. Ancak daha performanslı, düzenli ve kolay haberleşme için, özellikle çok sayıda ucun haberleşmesi isteniyorsa, bir SIP sunucusu kullanmak gerekmektedir.

**SIP Ağ Sunucusu:** Kısaca SIP Sunucusu da denmektedir. Temel görevi, DNS mantığına benzer şekildedir. İsimlerin IP adresine çevrilme görevini üstlenir. Haberleşmek isteyen iki uçtan birisi diğerini aramak istediğinde, önce SIP sunucusuna diğer ucun bilgilerini sorar. SIP sunucusundan aldığı yanıta göre, diğer uç ile kendisi arasında oturum açmaya çalışır. Genelde SIP kullanıcılarının birbirinden ayrılması için, benzersiz alfanümerik isimler kullanılır. Bu adresler de eposta adresleme sistemindeki benzer yapıda, *kullanıcı@alan_adı* şeklindedir. Kolaylık sağlaması için herkesin gerçek eposta adresi de kullanılabilmektedir (Can, 2006).

SIP uygulamalarında kullanılan 3 tip sunucu vardır:

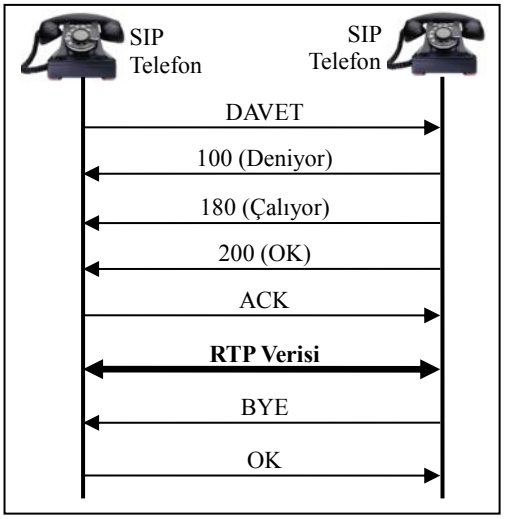
**a. Vekil Sunucusu (Proxy Server):** Bir kullanıcının talebini alıp, o kullanıcının adına başka kullanıcılardan talepte bulunan sunucudur. Kendisine gelen mesajları alır, yorumlar ve diğer uca aktarır. Bu iletişim sırasında, gerekirse mesajların bazı kısımları yeniden düzenlenebilir. Vekil sunucular, kullanıcıların birbirlerini araması konusunda kurallar belirlemek ve uygulamak için de kullanılabilir. Ayrıca, SIP desteklemeyen uçlarla oturum kurabilmek için de kullanılabilmektedir. Vekil sunucusu kullanılan bir sistemdeki oturum kurma aşamaları başlık 3.4 altında açıklanmıştır.

**b. Yönlendirme Sunucusu (Redirect Server):** Bir uçtan gelen SIP talebini alır, bu talebin hedefi olan ucun adresini biliyorsa, arayan uca, hedef ucun adresini göndererek başka bir adrese yönlendirebilir. Vekil sunucunun yaptığı, başkasının yerine talep gönderme işini yönlendirme sunucusu yapmaz. Yönlendirme sunucusu kullanılan bir sistemdeki oturum kurma aşamaları başlık 3.4 altında açıklanmıştır.

**c. Kayıt Sunucusu (Registrar Server):** Kullanıcıların konum (IP adresi gibi) bilgilerinin tutulduğu bir veritabanını barındırır. REGISTER mesajlarını alır ve üzerinde tuttuğu kullanıcıların konum bilgilerini düzenler.

## 3.4 Oturum Başlatma Protokolü İle Oturum Kurulması

Bir kullanıcı diğer bir kullanıcıyı aramak istediğinde, önce karşı tarafa bir davet talebi gönderilir. Bu talep, karşı uç ile oturum başlatılabilmesi için gerekli olan verileri içerir. Aranan tarafın adresi biliniyorsa, SIP sunucuya gerek kalmadan doğrudan davet talebi karşı uca iletilebilir. Aranan tarafın adresi bilinmiyorsa, talep mesajı SIP sunucusuna gönderilir. SIP sunucusu eğer bir vekil sunucusuysa; talebi alır, karşı ucun konum bilgilerini çözümler ve karşı uca talebi kendisi gönderir. Eğer SIP sunucusu bir yönlendirme sunucusu ise, arayana karşı ucun konum bilgisini gönderir. Bu durumda, çağrı başlatmak isteyen uç, karşı uca yeniden davet mesajı göndererek oturumun başlatılmasını sağlar. Şekil 3.5'te SIP sunucu kullanmadan, doğrudan doğruya uçlar arasında yapılan bir SIP oturumunun mesajlaşması gösterilmiştir.




**Şekil 3.5.** SIP sunucu olmadan bir SIP oturumu başlatılması.

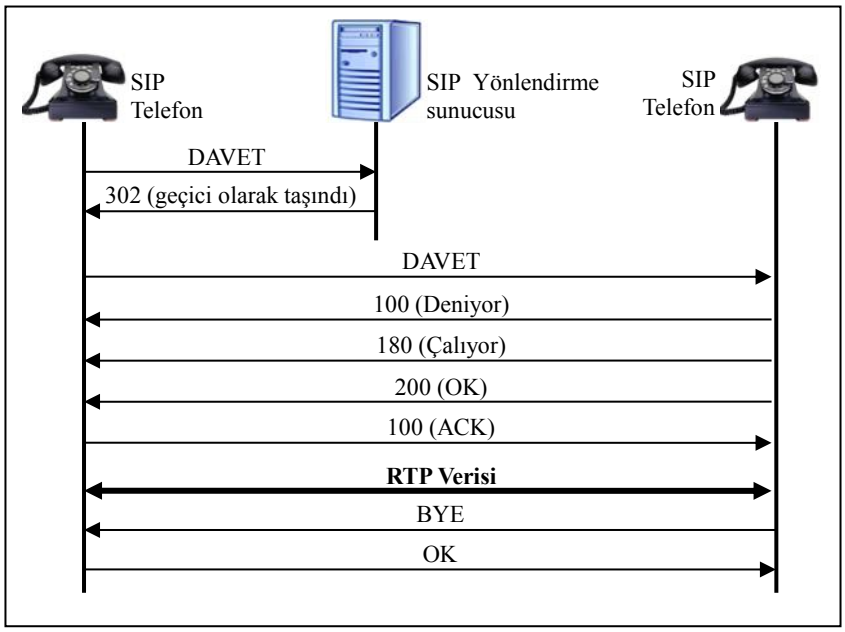
Şekil 3.5'te gösterildiği gibi, SIP sunucusu kullanılmadan kurulan bir oturumun öncesinde bazı özel mesajlar ile iki taraf karşılıklı oturum başlatma işlemi yapmaktadır. Uçtan uca bir SIP oturumunun mesaj detayları Çizelge 3.2'de gösterilmiştir.

**Çizelge 3.2.** Uçtan uca bir SIP oturumunun aşamaları.

| **Aşama** | **Mesaj Kodu** | **Açıklama** |
|---|---|---|
| 1. DAVET | | Arayan uç, diğer uca bir davet gönderir |
| 2. Deniyor | 100 | Aranan uç, arayan uca bilgi içerikli 'Deniyor' yanıtını gönderir. |
| 3. Çalıyor | 180 | Aranan uç çalmaya başladığında 'Çalıyor' yanıtını gönderir |
| 4. Tamam | 200 | Aranan kişi çağrıyı kabul ettiğinde, aranan uç 'OK (Tamam)' yanıtını gönderir |
| 5. Alındı | | Arayan uç 'ACK (Alındı)' yanıtını verir |
| 6. Görüşme | | İki kişi arasında yapılan görüşme, RTP üzerinden veri şeklinde iletilir |
| 7. Sonlandırma | | Bir uç çağrıyı sonlandırdığında, diğer uca 'BYE (Hoşçakal)' talebi gönderilir |
| 8. Tamam | 200 | Karşı uç 'OK (Tamam)' yanıtını verir |

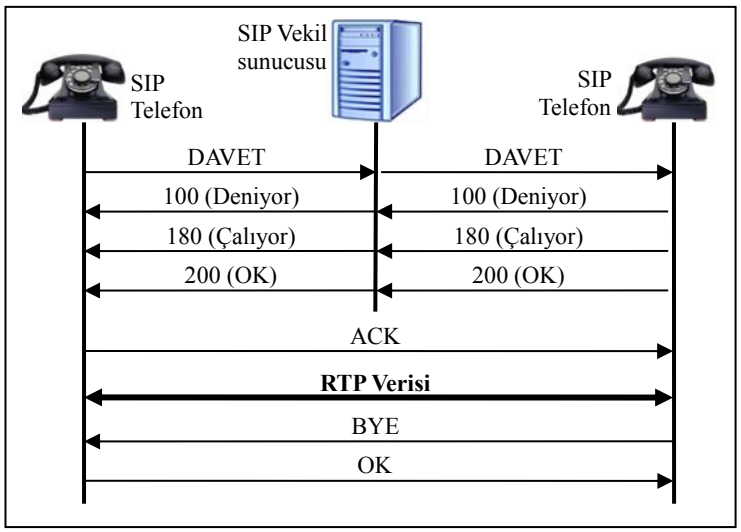
SIP'te, iki uç başka bir sunucuya gerek kalmadan, doğrudan karşılıklı görüşme yapabilir. Ancak uç sayısının çok olması durumunda, her bir ucun diğer uçların adresini bilmesi beklenemez. Bu durumda, yönlendirme sunucusu, görüşme taleplerini yönlendiren bir santral görevi üstlenmektedir. Şekil 3.6'da SIP yönlendirme sunucusu kullanıldığındaki mesajlaşma trafiği gösterilmiştir. Çağrı başlatmak isteyen ucun isteği önce yönlendirme sunucusuna gider, daha sonra bu istek aranan uca yönlendirilir. Bu

şekilde, arayan uç ile diğer uç arasında bir SIP oturumu kurulmuş olur. Bundan sonra tüm görüşme trafiği sunucudan bağımsız olarak iki uç arasında aktarılmaya devam eder.




**Şekil 3.6.** Yönlendirme (redirect) sunucusu kullanılan SIP çağrısı mesajları.

Vekil sunucu kullanılıyorsa, kullanıcıdan gelen talep, vekil tarafından diğer uca iletilir. Aranan uçtan gelen cevaplar da yine vekil sunucu tarafından çağrıyı başlatan uca aktarılır. Bu tarz bir haberleşmenin mesajlaşma trafiği Şekil 3.7'de gösterilmiştir.




**Şekil 3.7.** Vekil sunucusu kullanılan SIP çağrısı mesajları.

## 3.5 Oturum Başlatma Protokolü Mesajları

SIP'in tanımı gereği farklı işlevler için RFC 3261 ile tanımlanmış olan farklı mesaj tipleri kullanılmaktadır. Bu farklı mesaj tiplerine, istek metotları (Request Method) denmektedir. Çizelge 3.3'de SIP iletişimi sırasında sıkça kullanılan istek metotları verilmiştir.

**Çizelge 3.3.** SIP istek metotları.

| İstek Metodu | Açıklama |
|---|---|
| KAYIT (REGISTER) | Bir kullanıcı ajanının, çağrı kabul etmek için kullanacağı ve kendine ait olan IP adresi ile URL'sinin (Tek Biçimli Kaynak Konumlandırıcısı ~ Uniform Resource Locator) bildirilmesi için kullanılır. |
| DAVET (INVITE) | Kullanıcı ajanları arasında yeni bir oturum başlatmak için kullanılır. |
| KABUL (ACK) | (Acknowledge) Mesaj iletiminin onaylanmasını sağlar. |
| İPTAL (CANCEL) | Bekleyen isteği iptal eder. |
| HOŞÇA KAL (BYE) | Aktif oturumun sonlandırılması için kullanılır. |
| SEÇENEKLER (OPTIONS) | Bir çağrı başlatma işlemine girişmeden, arayan kullanıcı ajanının yeteneklerinin istenmesi için kullanılır. |
| GEÇİCİ MESAJ ONAYI (PRACK) | (Provisional Response Acknowledgement) Geçici mesajlara onaylama sistemi eklenerek ağın kararlılığını artırmak için kullanılır. PRACK, geçici mesajlara (1xx) cevap olarak gönderilir. |

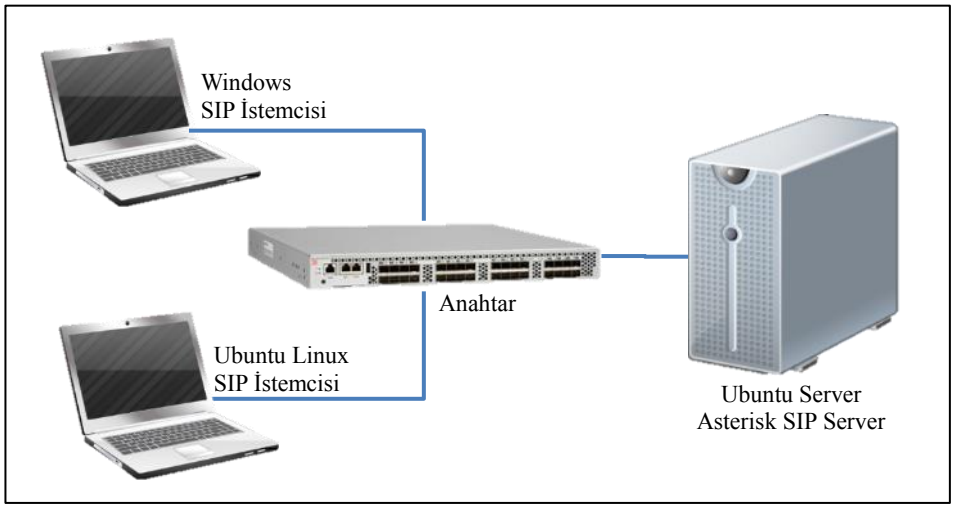
SIP haberleşmesinde, istek metotlarının yanında bir de cevap mesajları vardır. Çizelge 3.4'de SIP haberleşmesinde kullanılan ve RFC 3261 ile tanımlanmış olan cevap mesajı tipleri verilmiştir.

**Çizelge 3.4.** Cevap mesajı tipleri.

| Mesaj Tipi | Açıklama |
|---|---|
| **1xx:** Geçici (provisional) | İstek alındı, işlenmekte |
| **2xx:** Başarılı (success) | İstek alındı, anlaşıldı ve kabul edildi |
| **3xx:** Yeniden yönlendirme (redirection) | Önce sıradaki eylemler tamamlanmalıdır |
| **4xx:** İstemci hatası (client error) | İstekte sözdizim hatası olabilir |
| **5xx:** Sunucu hatası (server error) | Sunucu aktif geçerli isteği yerine getiremedi |
| **6xx:** Genel hata (global failure) | İstek hiçbir sunucu tarafından yerine getirilemedi |

# 4. BÖLÜM: IPV6 AĞINDA SUNUCU-İSTEMCİ MİMARİSİNDE SIP SİSTEMİ UYGULAMASI

Bu uygulama kapsamında tamamen açık kaynak kodlu ve ücretsiz yazılımlar kullanılarak bir SIP iletişim ortamı kurulmuştur. Uygulama ortamında; bir SIP sunucusu ve iki adet SIP istemci yazılımı kurulu bilgisayar kullanılmıştır. IPv4 ve IPv6 protokollerini aynı anda destekleyen bir uygulama ortamı oluşturulduğunda, SIP haberleşmesinin analizi için çalışmalar yapılmıştır. Daha sonra elde edilen bulgular paylaşılmıştır. Şekil 4.1'de uygulama ortamının diyagramı gösterilmiştir.




**Şekil 4.1.** Uygulama bileşenleri.

## 4.1 IPv6 Ağında SIP Uygulama Ortamının Genel Özellikleri

SIP destekli bir iletişim sağlamak için, piyasada hem ücretli hem de ücretsiz çok sayıda yazılım bulunmaktadır. Bu çalışmanın amaçlarından birisi de, "IPv6 üzerinden çalışan uygulanabilir bir SIP iletişim ortamı oluşturmak" olduğundan, özellikle ücretsiz yazılımlar test edilmiştir.

SIP iletişim karakteristiğinin iki protokol üzerinde ayrı ayrı incelenebilmesi için; uygulama ortamının hem IPv4 hem de IPv6 protokolleri ile iletişim kurması sağlanmıştır. Hem IPv4 hem de IPv6 protokollerini aynı anda çalıştırabilen bu tarz sistemlere "ikili yığın (dual stack)" ismi verilmektedir (Gilligan vd., 2000).

Sunucu için işletim sistemi olarak; uyumluluk sorununun az olması nedeniyle, en yaygın GNU/Linux dağıtımlarından olan Ubuntu'nun[1] 64 bitlik 11.04 sürümü tercih edilmiştir. İstemci bilgisayarlar için de farklı işletim sistemlerinde uygulanabilirliği test etmek amacıyla hem Microsoft® Windows 7, hem de Ubuntu Linux kullanılmıştır.

## 4.2 SIP Uygulama Ortamı Yazılımları

Sunucu bilgisayarda Asterisk[2] isimli SIP sunucu yazılımı kullanılmıştır. SIP sunucusu olarak yine açık kaynak kodlu ve ücretsiz olan başka yazılımlar da bulunmaktadır. Ancak gerek yaygın kullanılması nedeniyle daha rahat destek bulunması, gerekse IPv6 desteğinin sorunsuz olması nedeniyle bu uygulamada Asterisk yazılımı tercih edilmiştir. Asterisk kurulumu ve yapılandırması, 4.2.1'de açıklanmıştır.

Uygulama ortamında kullanılmak üzere SIP istemci yazılımı olarak Jitsi[3] isimli yazılım tercih edilmiştir. Yazılımın IPv6 desteği olması, Windows ve Linux üzerinde çalışabilmesi, kullanışlı olması tercih sebebi olmuştur.

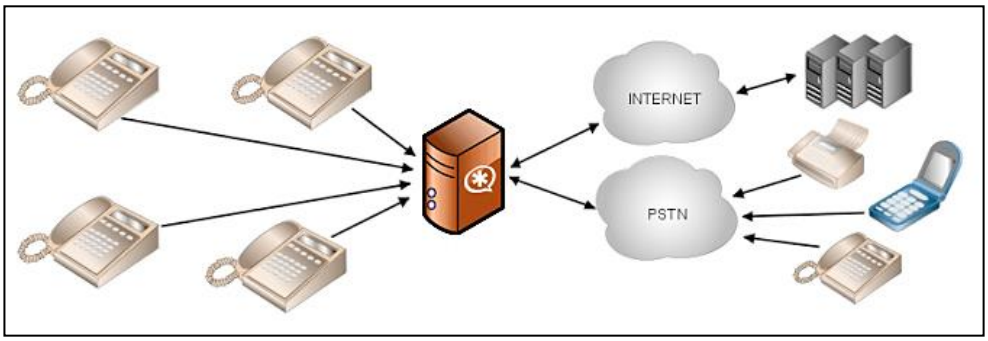
### 4.2.1 Asterisk SIP sunucu yazılımı

Asterisk, açık kaynak kodlu ve ücretsiz bir "tümleşik iletişim sistemi" yazılımdır. Kendi içerisinde SIP destekli "çağrı sunucusu", analog veya sayısal telefon şebekelerine geçiş için kullanılan bir "ses geçidi" sistemi, tanımlı abonelerin birbirlerine sesli mesaj bırakmasını ve istendiğinde mesajların dinlenebilmesini sağlayan "sesli mesaj sistemi", tanımlı abonelerin sesli ve görüntülü konferans yapabilmesini sağlayan "konferans sistemi", arayan kullanıcının tuşlara basarak yönlendirilmesini sağlayan "sesli yanıt sistemi (IVR)" gibi işlemleri üstlenebilen yazılımlardan oluşan bir pakettir.

Şekil 4.2'de Asterisk'in çalışması ile ilgili bir örnek bulunmaktadır. Asterisk, doğrudan SIP abonelerinin iletişimini sağlayabildiği gibi, PSTN (Public Switched Telephone Network ~ Genel Anahtarlamalı Telefon Şebekesi) şebekelerine geçiş için

[1] Ubuntu Linux, http://www.ubuntu.com/ adresinden indirilebilir.
[2] Asterisk, http://www.asterisk.org/ adresinden indirilebilir.
[3] Jitsi, http://jitsi.org/ adresinden indirilebilir.

veya İnternet üzerinden diğer SIP sunucular ile bağlantı sağlamak için de kullanılabilir.




**Şekil 4.2.** Asterisk'in kullanım alanları

PSTN, dünya genelinde kullanılmakta olan devre anahtarlamalı telefon şebekesine verilen isimdir. Önceden tamamen analog olan PSTN şebekesi günümüzde çoğunlukla sayısal hale gelmiştir. Kurumların kendi içerisinde iletişim için kullanılan çağrı sistemlerine de PBX (Private Branch Exchange ~ Özel Telefon Santrali) adı verilir. Klasik telefon yapısını değiştirmeden SIP desteği sağlamak isteyen kurumlarda da Asterisk veya benzeri uygulamalar ile karma yapılar kurulabilmektedir.

Asterisk sunucusunun analog veya sayısal PSTN/PBX şebekelerine bağlanabilmesi için, bilgisayara VoIP kartı denen bir donanım takılması veya ayrı bir ses geçidi kullanmak gerekmektedir. Şekil 4.3'de bir VoIP kartı örneği gösterilmiştir. VoIP kartları bir veya daha fazla sayıda analog veya sayısal port içerebilir. Kart üzerindeki her bir porttan bir telefon cihazına veya bir PBX santrale bağlantı sağlanabilir.

**Şekil 4.3.** VoIP kartı.

#### 4.2.1.1 Asterisk SIP sunucusunun kurulumu

Uygulama ortamında, sunucu bilgisayarda, "2.6.38-8" sürümlü Linux çekirdeği kullanılmıştır. Asterisk'in yüklenmesi için; istenirse kaynak kodundan derlenebileceği gibi, Ubuntu veya Debian gibi bazı dağıtımların içerisinde gelen paket yöneticisinden de kolayca kurulabilir. Uygulama sırasında kolaylık olması için, Asterisk'in yüklenmesi Ubuntu paket yöneticisi içerisinden yapılmıştır.

Ubuntu Linux içerisinde, "`sudo aptitude install asterisk`" komutunu kullanarak Asterisk'in ve bağlı bileşenlerin yüklenmesi kolayca sağlanabilir. Şekil 4.4'te yüklenmiş olan Asterisk paketlerinin listesi görülmektedir.

```
root@cunyor-du:~# aptitude search asterisk | grep "^i"
i   asterisk                        - Open Source Private Branch Exchange (PBX)
i   asterisk-config                 - Configuration files for Asterisk
i   asterisk-core-sounds-en-gsm     - asterisk PBX sound files - English/gsm
i   asterisk-modules                - loadable modules for the Asterisk PBX
i   asterisk-moh-opsound-wav        - asterisk extra sound files - English/wav
i   asterisk-voicemail              - simple voicemail support for the Asterisk
```

**Şekil 4.4.** Yüklenmiş Asterisk paketlerinin listesi.

Asterisk kurulumu tamamlandıktan sonra; yetkili kullanıcı ile sistemde oturum açılmışken, "`asterisk -r`" komutu ile Asterisk servisinin çalışıp çalışmadığı kontrol edilebilir. Şekil 4.5'te, başarılı olarak tamamlanmış bir Asterisk kurulumu sonrasında yapılan test işleminin ekran çıktısı görülmektedir.

```
root@cunyor-du:~# asterisk -r
Asterisk 1.8.4.1-1digium1~natty, Copyright (C) 1999 - 2010 Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 1.8.4.1-1digium1~natty currently running on cunyor-du (pid = 11861)
cunyor-du*CLI>
```

**Şekil 4.5.** Asterisk kurulumunun test edilmesi.

Asterisk'in, kendine ait özel bir komut istemcisi (CLI ~ Command Line Interface ~ Komut Satırı Arabirimi) vardır. Şekil 4.5'te gelen ekran, Asterisk'in komut istemci ekranıdır. Şekil 4.5'in son satırında görülen "`CLI>`" yazısı gelmiyorsa, Asterisk kurulumunda bir sorun olmuş olabilir veya servis çalışmıyor olabilir. "`exit`" komutu kullanılarak, Asterisk'in komut istemcisinden çıkılabilir.

Ubuntu ve Debian işletim sistemlerinde Asterisk servisinin çalışıp çalışmadığı, "`/etc/init.d/asterisk status`" komutu ile kontrol edilebilir. Servisi başlatmak için, "`/etc/init.d/asterisk start`"; servisi durdurmak için de "`/etc/init.d/asterisk stop`" komutları verilebilir. Şekil 4.6'da, Asterisk servisinin başlatılması gösterilmiştir.

```
root@cunyor-du:~# /etc/init.d/asterisk status
 * Asterisk PBX is not running
root@cunyor-du:~# /etc/init.d/asterisk start
Starting Asterisk PBX: asterisk.
root@cunyor-du:~# /etc/init.d/asterisk status
 * Asterisk PBX is running
```

**Şekil 4.6.** Servis denetim komutların işletim ekranı.

#### 4.2.1.2 Asterisk SIP sunucusunun yapılandırması

Varsayılan kurulumda, Asterisk için bir GUI (Graphical User Interface ~ Grafik Kullanıcı Arabirimi) bulunmamaktadır. Tüm yapılandırma işlemleri Linux'ta CLI üzerinden yapılmaktadır. Bu nedenle, öncelikle Linux'un ağ yapılandırması tamamlanmalıdır. Daha sonra uzaktan Asterisk yapılandırmasını düzenlemek amacıyla sunucuya rahat erişebilmek için, Linux'a uzaktan bağlantı olanağı sağlanması, faydalı olacaktır. Bunun için, Ubuntu üzerinde "`sudo apt-get install openssh-server`" komutunu vermek yeterlidir. Bundan sonra, IP adresi üzerinden SSH (Secure Shell ~ Güvenli Kabuk) ile Ubuntu'ya bağlanarak Asterisk yapılandırması düzenlenebilecektir.

Asterisk kurulduğunda varsayılan ayarlarda, SIP iletişimine doğrudan hazırdır. Ancak yine de bazı başlangıç ayarları yapmak gerekmektedir. Uygulama ortamında SIP iletişimi sağlamak için, telefon aboneleri ve abonelerin dâhili numaraları Asterisk üzerinde tanımlanmalıdır.

Asterisk yapılandırmasını değiştirmek (abone eklemek, çıkarmak vb.) için Ubuntu Linux dosya sisteminde "`/etc/asterisk`" klasöründe bulunan dosyaların düzenlenmesi gerekmektedir. Uygulama ortamı için öncelikle iki dosyada düzenleme yapılması gerekmektedir. Bu dosyalar ve görevleri Çizelge 4.1'de belirtilmiştir.

**Çizelge 4.1.** Asterisk'in bazı yapılandırma dosyaları.

| **Dosya adı** | **Dosya görevi** |
|---|---|
| `/etc/asterisk/extension.conf` | Abonelerin, arama planlarının, PBX'ler arası bağlantıların, vb. işlemlerin düzenlendiği dosyadır. |
| `/etc/asterisk/sip.conf` | SIP iletişimi için; TCP ve UDP port numaralarının, IP ayarlarının, kullanılacak kodeklerin, SIP hesaplarının düzenlendiği dosyadır. |

Öncelikle, Asterisk'e IPv6 desteğinin verilmesi gerekmektedir. Bunun için, "`/etc/asterisk/sip.conf`" dosyasında "`udpbindaddr=0.0.0.0`" şeklinde olan satırın bulunarak, bu satırın "`udpbindaddr=::`" şekline getirilmesi gerekmektedir. Burada kullanılan "`::`" işareti, IPv6 ağlarında, tüm IPv6 adresleri anlamına gelmektedir. "`0.0.0.0`" şeklinde olan varsayılan yapılandırma ise, "tüm IPv4 adresleri" anlamına gelmektedir. Asterisk hangi protokolde çalıştırılacaksa, ona göre bu dosyada ilgili değişikliğin yapılması gerekmektedir. Daha sonra, "`/etc/init.d/asterisk restart`" komutu ile, Asterisk sunucusunun yeni ayarları kullanmaya başlaması sağlanmalıdır. Şekil 4.7'de IPv6 yapılandırması tamamlanmış bir Asterisk sunucusu üzerinde `netstat` komutu ile dinlenen portların listelenmesi gösterilmiştir.

```
root@cunyor-du:~# netstat -antulp | grep 5060
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address    Foreign Address     State       PID/Program name
udp6       0      0 :::5060         :::*                            10540/asterisk
```

**Şekil 4.7.** Asterisk tarafından dinlenen IPv6 SIP portu.

Şekil 4.7'de, Asterisk tarafından IPv6 üzerinden dinlenen portlar görülmektedir. Şekil 4.7'nin en alt satırında olan "`udp6`" sözcüğünün sonundaki "6" rakamı, IPv6 üzerinden dinleme yapıldığını belirtmektedir. "`Local Address`" başlığı altındaki "`:::5060`" kısmı, yerel bilgisayardaki tüm IPv6 destekli arabirimler üzerinden "5060" numaralı portun dinlendiğini belirtmektedir. UDP 5060 numaralı port, SIP iletişimi için

kullanılan standart porttur. Sistemde güvenlik duvarı gibi cihazlar veya yazılımlar kullanılıyorsa, SIP istemcilerinin sunucuya bağlanabilmesi için bu portun açık olması gerekmektedir.

Şekil 4.7'de, "`Foreign Address`" başlığının altında ve son satırda görülen "`:::*`" ifadesi, bu bilgisayara IPv6 üzerinden gelen tüm isteklere cevap verileceğini belirtmektedir. Varsayılan kurulum ayarlarına göre, bu şekilde çalışmaktadır. Eğer Asterisk, standart SIP sunucusu olarak kullanılacaksa, istemcilerin bu sunucuya bağlanabilmesi için, tüm IP adreslerinden gelen istekleri dinlemesi uygundur.

Şekil 4.7'de görülen en alttaki satırın görülebiliyor olması, Asterisk sunucusunun SIP portunu IPv6 üzerinden dinleyebildiği anlamına gelmektedir. Yani Asterisk SIP sunucusunun IPv6 yapılandırması sağlıklıdır. Bu aşamada Asterisk sunucusunun yüklü olduğu Ubuntu'ya IPv6 adresi tahsis edilebilir. Şekil 4.8'de, Linux işletim sistemi üzerinde IPv6 adresi ekleme işlemi, IPv6 adresinin doğru kaydedilip kaydedilmediğinin görüntülenmesi ve IPv6 bağlantısının test edilmesi için "ping atma[1]" işlemi gösterilmiştir.

```
cunyor@cunyor-du:~$ sudo ip -6 addr add fc00::1/64 dev wlan0
cunyor@cunyor-du:~$ ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:21:00:bd:ce:5c
          inet addr:192.168.1.8  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::221:ff:febd:ce5c/64 Scope:Link
          inet6 addr: fc00::1/64 Scope:Evrensel
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3274107 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2084891 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3267803311 (3.2 GB)  TX bytes:288840723 (288.8 MB)

cunyor@cunyor-du:~$ ping6 -I wlan0 fc00::1
PING fc00::1(fc00::1) from fc00::1 wlan0: 56 data bytes
64 bytes from fc00::1: icmp_seq=1 ttl=255 time=0.039 ms
64 bytes from fc00::1: icmp_seq=2 ttl=255 time=0.049 ms
```

**Şekil 4.8.** Linux'ta, IPv6 adresi verilmesi ve test edilmesi.

[1] "ping atma" işlemi, ağ üzerindeki bir cihaza ICMP kullanılarak erişilip erişilemediğinin anlaşılması için paket gönderilmesi ve pakete cevap gelip gelmediğine bakılmasıdır. İşletim sisteminin konsolunda, "ping <IP_adresi>" şeklinde komut olarak yazılır. Ping'e cevap gelip gelmediği komutun cevabı olarak ekrana yazılacaktır.

Asterisk sunucusunun `wlan0` isimli ağ arabirimine IPv6 adresi olarak, `fc00::1/64` verilmiştir. fc00 ile başlayan IPv6 adresleri (fc00::/7 ağı) özel bir ağdır ve test amaçlı olarak kurum içi ağlarda kullanmak üzere ayrılmıştır. Aslında uygulama sırasında aynı arabirimde kayıtlı bulunan, `fe80::221:ff:febd:ce5c` (Şekil 4.8'de görülmektedir) şeklindeki IPv6 adresi de kullanılabilirdi. Ancak bu adres işletim sistemi tarafından kendiliğinden oluşturulan uzun isimli bir IPv6 adresi olduğundan, daha kısa isimli olan "fc00::1" IPv6 adresi ile çalışma tercih edilmiştir.

Bu aşamada, hem Ubuntu Linux işletim sisteminin hem de Ubuntu Linux üzerinde çalışan Asterisk SIP sunucusunun IPv6 yapılandırması tamamlanmıştır. Sistem; Asterisk sunucusu üzerinde SIP kullanıcıları oluşturulup, kullanıcılar için birer çağrı numarası tahsis edildiğinde, kullanıcılar SIP üzerinden görüşme yapabilecek hale getirilmiştir. Asterisk üzerinde, uygulamada kullanılmak üzere iki adet kullanıcı tanımlanmıştır. Kullanıcıların sisteme eklenmesi için Şekil 4.9'da görülen satırların "`/etc/asterisk/sip.conf`" dosyasına eklenmesi gerekmektedir.

```
[abone1]
type=friend
host=dynamic
secret=abc123
context=users

[abone2]
type=friend
host=dynamic
secret=abc123
context=users
```

**Şekil 4.9.** Asterisk'e kullanıcı eklemek için yazılması gereken kodlar.

Şekil 4.9'da gösterilen kodlarda köşeli parantezler içinde belirtilen isimler ("abone1" ve "abone2") uygulamada kullanılacak olan hesap isimleridir. "`secret`" ifadesinin yanında yazan "`abc123`" sözcükleri de bu hesaplara ait parolalardır. SIP kullanıcıları hesap ismi ve parolaları ile sistemde oturum açabileceklerdir. Hesapların eklenmesi tamamlandıktan sonra, Asterisk sunucusunun SIP bileşenlerinin yeniden yüklenerek hesapların etkinleştirilmesi gerekmektedir. Şekil 4.10'da SIP bileşenlerinin yeniden yüklenmesi gösterilmiştir.

```
root@cunyor-du:~# asterisk -r
Asterisk 1.8.4.1-1digium1~natty, Copyright (C) 1999 - 2010 Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 1.8.4.1-1digium1~natty currently running on cunyor-du (pid = 12509)
Verbosity is at least 6
cunyor-du*CLI> sip reload
 Reloading SIP
cunyor-du*CLI>
```

**Şekil 4.10.** Asterisk sunucusunun SIP bileşenlerinin yeniden yüklenmesi.

Şekil 4.10'da ilk satırda görülen "`asterisk -r`" ifadesi, Asterisk sunucusunun konsoluna bağlanmak için kullanılmıştır. "`sip reload`" komutu ise SIP bileşenlerinin yeniden yüklenmesi için kullanılmıştır. Bu aşamada SIP hesapları etkinleştirilmiştir.

SIP hesapları da etkinleştirildikten sonra geriye kalan tek işlem, SIP hesapları için birer çağrı numarası tahsis edilmesidir. Bunun için de Şekil 4.11'de gösterilen satırların, "`/etc/asterisk/extensions.conf`" dosyasına eklenmesi gerekmektedir.

```
[users]
exten=>1001,1,Dial(SIP/abone1,20)
exten=>1002,1,Dial(SIP/abone2,20)
```

**Şekil 4.11.** SIP hesaplarına çağrı numarası tahsis edilmesi.

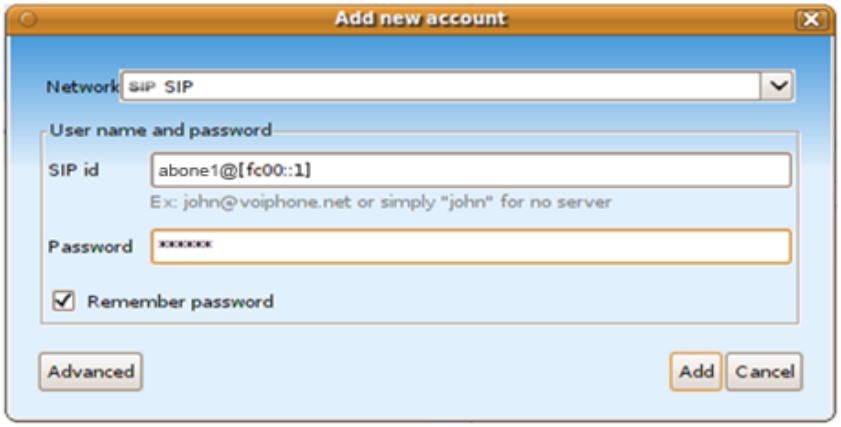
Şekil 4.11'de, "`exten`" komutu ile yeni bir abone (extension) oluşturulmuş, "1001" numarası arandığında, "abone1" isimli SIP hesabının aranması sağlanmıştır. Değişikliklerin etkinleştirilmesi için, Asterisk konsolunda "`dialplan reload`" komutu çalıştırılarak, arama planlarının yeniden yüklenmesi sağlanmalıdır. Bu aşamada, 1001 ve 1002 numaralı "abone1" ve "abone2" kullanıcıları SIP sunucusuna kayıt olduktan sonra, birbirlerini SIP üzerinden çağrı numaraları ile arayabilecektir.

### 4.2.2 SIP istemci yazılımı

Piyasada ücretli veya ücretsiz birçok SIP istemci yazılımı bulunmaktadır. IPv6 desteğinin iyi olması, kullanıcı arabiriminin basit olması, ücretsiz ve açık kaynak kodlu

olması, birçok platformda (Windows, Linux, Mac OSX gibi) çalışabilmesi gibi nedenlerle **Jitsi**[1] isimli yazılım tercih edilmiştir. Bu çalışma yapıldığı sırada Jitsi'nin son sürümü olan "1.0-beta1" sürümü kullanılmıştır.

Hem Ubuntu Linux hem de Microsoft Windows 7 üzerinde Jitsi programı kurularak çalıştırılmıştır. Programın arabirimi, iki işletim sisteminde de aynıdır. Program kurulduktan sonra, Jitsi'ye daha önce Asterisk üzerinde oluşturulan hesapların eklenmesi gerekmektedir. Şekil 4.12'de Jitsi'ye hesap ekleme arabirimi gösterilmiştir.




**Şekil 4.12.** Jitsi'ye SIP hesabı eklenmesi.

Jitsi'ye SIP hesabı eklerken girilmesi gereken örnek bilgiler örnek olarak Çizelge 4.2'de gösterilmiştir. Bilgiler doğru girilmezse, sunucuya bağlanamayabilir.

**Çizelge 4.2.** Jitsi'ye eklenecek SIP hesabı bilgileri.

| **Alan adı** | **Yazılması gereken bilgi** | **Uygulama için örnek** |
|---|---|---|
| Network | Ağın (protokolün) türü | SIP |
| SIP id | SIP hesap adı | abone1@[fc00::1][2] |
| Password | SIP parolası | abc123 |
| Display name | Görüntülenecek olan isim | abone1 |
| Registrar | SIP sunucu adresi | [fc00::1] |
| Authorization name | Yetkilendirme için kullanılacak olan isim | abone1 |

[1] Jitsi, http://jitsi.org/ adresinden indirilebilir.
[2] SIP hesabının yazılış şekli önemlidir. IPv6 sunucusuna bağlanılacaksa, adres köşeli parantezler içerisinde yazılmalıdır.

Eğer Jitsi'ye SIP hesabı ekleme işlemi başarılı olursa, SIP sunucusuna bağlanacak ve Jitsi programının ana penceresinde, yeşil bir işaret ve "Online" yazısı belirecektir. Şekil 4.13'te Jitsi programının ana ekranı gösterilmiştir.


**Şekil 4.13.** Jitsi'nin ana ekranı.

Jitsi kurulumu ve SIP hesabı ekleme işlemleri tamamlandıktan sonra, iki ayrı bilgisayarda bulunan Jitsi yazılımları üzerinden kullanıcılar birbirlerini 1001 ve 1002 şeklinde atanmış olan numaraları ile SIP üzerinden arayabilmektedir.

## 4.3 SIP Sunucusunda Zorlama Testleri Yapılması

Performans incelemesi için açık kaynak kodlu ve ücretsiz bir uygulama olan SIPP[1] isimli uygulama tercih edilmiştir. SIPP'in hem IPv6 desteği olması, hem de Linux üzerinde çalışabilmesi tercih edilme nedenleridir.

SIPP, Linux konsolunda çalışan bir uygulamadır. Temel görevi, SIP trafiği üretmek ve SIP sunucularının performansını test etmektir. Sunucu ve istemci modunda çalışabilmektedir. Sunucu modunda çalıştığında, gerçek bir SIP sunucusu gibi ağı dinler ve SIP mesajlarına cevap verir. İstemci modunda çalıştırıldığında, bir SIP istemcisi (*bu çalışmadaki uygulamada kullanılan Jitsi gibi*) gibi davranır. Bir SIP sunucusuna SIP mesajları gönderebilir. SIPP programı bu özellikleri sayesinde, iki farklı bilgisayara iki

[1] SIPP, http://sipp.sourceforge.net/ adresinden indirilebilir.

farklı özellikte kurularak, istemci-sunucu mimarisinde bir SIP performans testi yapılmasına olanak sağlar. Bu şekilde, SIP sunucusunun veya ağın performansının test edilebilmesi mümkün olmaktadır.

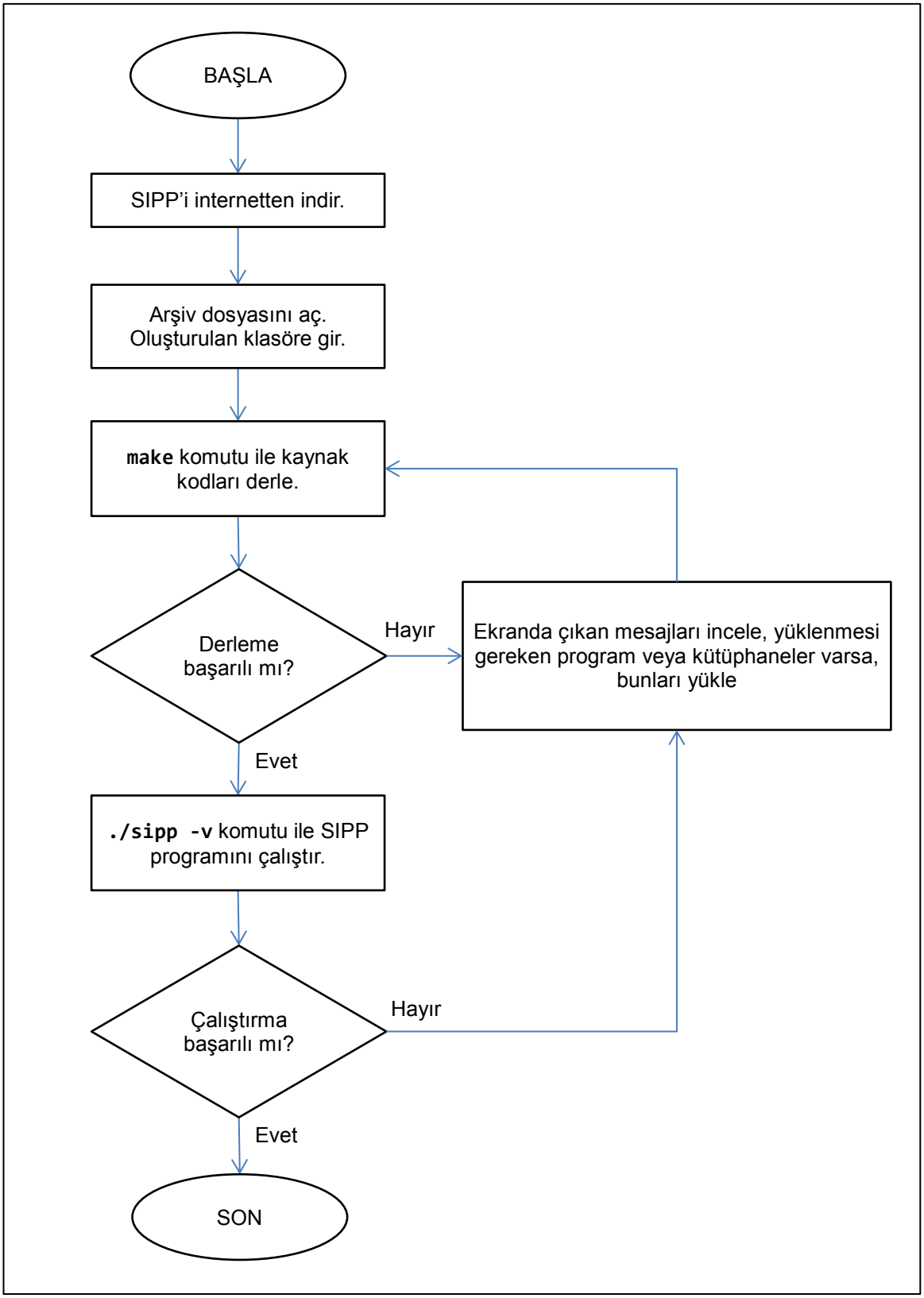
Bu çalışmanın hazırlandığı sırada, SIPP yazılımının kararlı en son 3.2 sürümü bulunmaktadır. Ubuntu Linux'un kendi deposunda ise, bir önceki sürüm olan 3.1 sürümü bulunmaktadır. Bu çalışmada güncel sürümle çalışabilmek için, 3.2 sürümü kullanılmıştır.

SIPP'in tam sürümü, internetten ücretsiz olarak indirilebilir. Kaynak koddan derlemek için indirilen dosya, "`.tar.gz`[1]" uzantısı ile gelmektedir. Kurulum için, önce bu arşiv dosyasının açılması, sonra açılan klasörün içine girerek "`make`[2]" komutu verilerek kaynak koddan derlenmesi gerekmektedir. Bu aşamada bazı dosyaların sistemde eksik olduğunu belirten mesajlar çıkabilir. Bu durumda, Ubuntu'nun deposundan ihtiyaç duyulan paketler[3] kolayca yüklenebilir. "`make`" komutunun sonucu başarılı olursa, aynı klasör içerisinde "`sipp`" adında bir çalıştırılabilir dosya oluşacaktır. Programın çalışıp çalışmadığını test etmek için, "`./sipp -v`" komutu verilebilir. Program düzgün derlenmişse, bu komut sonucunda ekrana, programın sürüm ve lisans bilgilerini veren bir metin gelecektir.

Ubuntu Linux üzerinde SIPP kurulumu sırasındaki işlem basamaklarını ve kontrolleri gösteren bir akış diyagramı Şekil 4.14'te verilmiştir.

---

[1] Genellikle Linux ve Unix tabanlı sistemlerde kullanılan, dosya arşivleme ve sıkıştırma biçimidir.
[2] Linux veya Unix sistemlerinde bir programın kaynak koddan derlenebilmesi için kullanılan komuttur.
[3] SIPP programının, Ubuntu Linux'ta derlenebilmesi için; "make", "gcc", "g++", "libncurses5-dev" paketlerinin yüklü olması gerekmektedir.



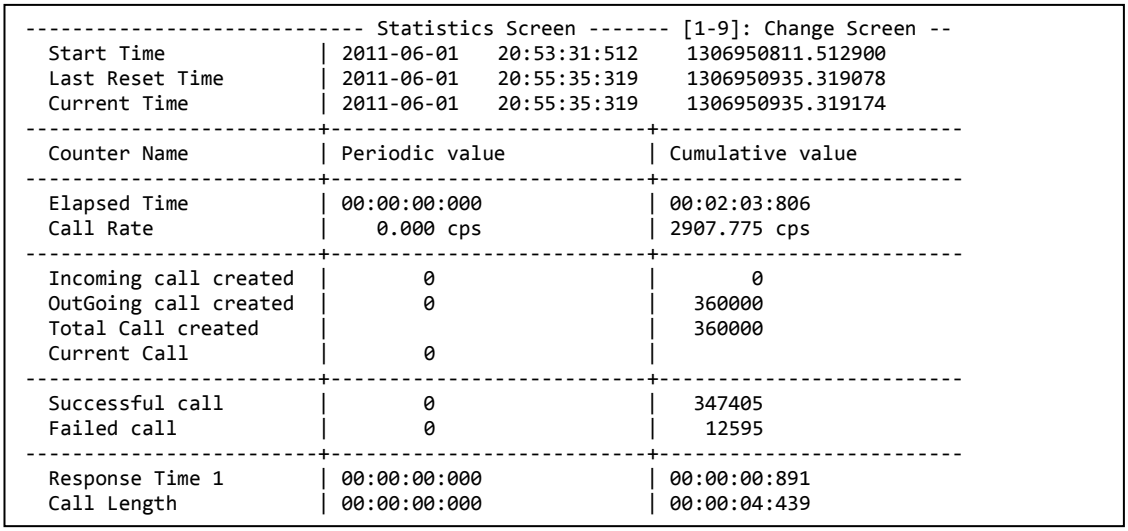

**Şekil 4.14.** SIPP kurulumu işlem basamakları.

Çizelge 4.3'te, SIP sunucusunun performans testini gerçekleştirmek için, SIPP programının kullanımı sırasında ihtiyaç olabilecek olan bazı parametreler verilmiştir.

**Çizelge 4.3.** SIPP programının çok kullanılan parametreleri.

| **Parametre** | **İşlevi** |
|---|---|
| -sn | "uac" ve "uas" olmak üzere iki değer alabilir. **uas**, SIP sunucusu olarak çalıştırmak için kullanılır. **uac**, SIP istemcisi olarak çalıştırmak için kullanılır. |
| -p | TCP veya UDP port numarasını belirtir. Sunucu modunda çalıştırılırsa kullanılır. Hangi portu dinleyeceğini belirtir. |
| -r | Birim sürede başlatılacak olan SIP çağrısı sayısı |
| -rp | Birim sürenin milisaniye cinsinden değeri |
| -m | Toplam başlatılacak olan SIP çağrısı sayısı. Bu değere ulaşınca otomatik olarak testi durdurur. |
| -l | Eş zamanlı yapılacak olan çağrı sayısını belirtir. |
| -bg | Arka planda çalışmasını sağlar. –m değeri ile belirtilen sayıya ulaşınca durur. –m parametresi kullanılmazsa, işlem kesilmezse, sonsuza kadar devam eder. |
| -sleep | Testi başlatmadan önce kaç saniye bekleyeceğini belirtir. Sürüm 3.2'den itibaren kullanılabilir. |
| -f | Gerçek zamanlı istatistik görüntüleme ekranındaki, belirlenen periyotta oluşan olay sayısı değeri için kullanılacak olan periyodu belirler. |
| -t u1 | Tüm çağrıları tek bir UDP oturumundan gönderir. |
| -t un | Tüm çağrılar için ayrı bir UDP oturumu oluşturur. |
| -t t1 | Tüm çağrıları tek bir TCP oturumundan gönderir. |
| -t tn | Tüm çağrılar için ayrı bir TCP oturumu oluşturur. |

SIPP programı ile bir test başlatıldığında, ilk ekran senaryoyu gösteren ekrandır. Gerçek zamanlı istatistikler için, klavyeden "2" tuşuna basmak gerekmektedir. Yeniden senaryo ekranına dönmek için ise klavyeden "1" tuşuna basmak gerekmektedir. Şekil 4.15'de, SIPP programının gerçek zamanlı istatistik ekranı gösterilmektedir.




**Şekil 4.15.** SIPP programının gerçek zamanlı istatistik ekranı.

SIPP programının parametreleri kullanılarak çok sayıda farklı senaryo oluşturulabilmektedir. SIPP programını sunucu modunda başlatmak için; "`./sipp -sn uas -i [::] -p 5060`" şeklindeki komut kullanılabilir. Bu komutta, "`-sn uas`" parametresi ile sunucu modunda çalışacağı belirtilmektedir. Hemen yanında yazan "`-i [::]`" parametresi ile, bu bilgisayar üzerindeki ağ arabirimlerinde yapılandırılmış olan tüm IPv6 adreslerini dinleyeceği belirtilmiştir. Son olarak, "`-p 5060`" parametresi ile 5060 numaralı portu dinlemesi gerektiği belirtilmiştir.

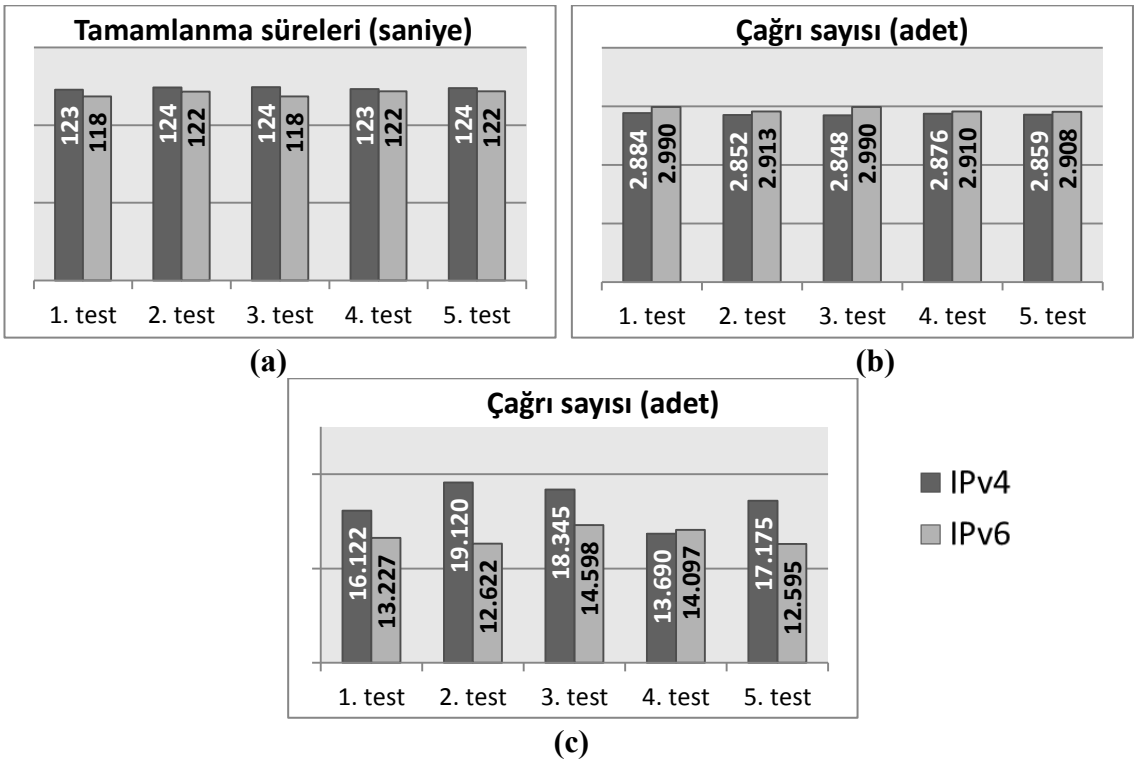
SIPP programını istemci modunda başlatmak için;

```
./sipp -sn uac -r 100 -rp 1000 -m 10000 -sleep 2 -i [fc00::1] [fc00::1]:5060
```

şeklindeki komut kullanılabilir. Bu komutta "`-sn uac`" parametresi, istemci modunda çalışacağını belirtmektedir. "`-r 100`", birim zamanda 100 tane SIP çağrısı başlatması gerektiğini belirtmektedir. "`-rp 1000`", birim zamanın 1000 milisaniye (1 saniye) olduğunu belirtir. "`-m 10000`", toplam başlatılacak çağrı sayısının 10000 olduğunu belirtir. "`-sleep 2`", teste başlamadan önce 2 saniye beklemesi gerektiğini belirtir. "`-i [fc00::1]`", hangi arabirimi kullanarak SIP sunucuya bağlanacağını belirtir. "`[fc00::1]:5060`" hangi SIP sunucusunun hangi portuna bağlanacağını belirtir. Bu ayarlar ile test başlatıldığında, 100 saniye sonrasında 10.000 civarında SIP çağrısı başlatma işlemi tamamlanmış olacaktır. SIPP programı, aktif çağrıların tamamlanması için bir süre daha bekledikten sonra istatistikleri gösterecek ve kapanacaktır.

Bu çalışmadaki SIPP ile performans testi uygulaması kapsamında, hem IPv4 üzerinden hem de IPv6 üzerinden aynı donanım ve yazılım ortamında SIPP programı ile testler yapılmıştır. Test kapsamında, saniyede 6.000 çağrı olmak üzere toplamda 360.000 çağrı yapılması sağlanmıştır. Bu çağrıların yapılması 60 saniye gibi bir sürede tamamlanmıştır. Saniyede 6.000'den fazla SIP çağrısı başlatıldığında, kullanılan bilgisayarın işlemcisinin donanımsal olarak yetersiz kaldığı görülmüş, bu nedenle bu değer 6.000'den fazla artırılmamıştır. Saniyede 100-200 gibi görece düşük miktarlarda çağrı başlatıldığında ise, kaynak ihtiyacı çok düşük olduğundan ölçümler sağlıklı olamamıştır.

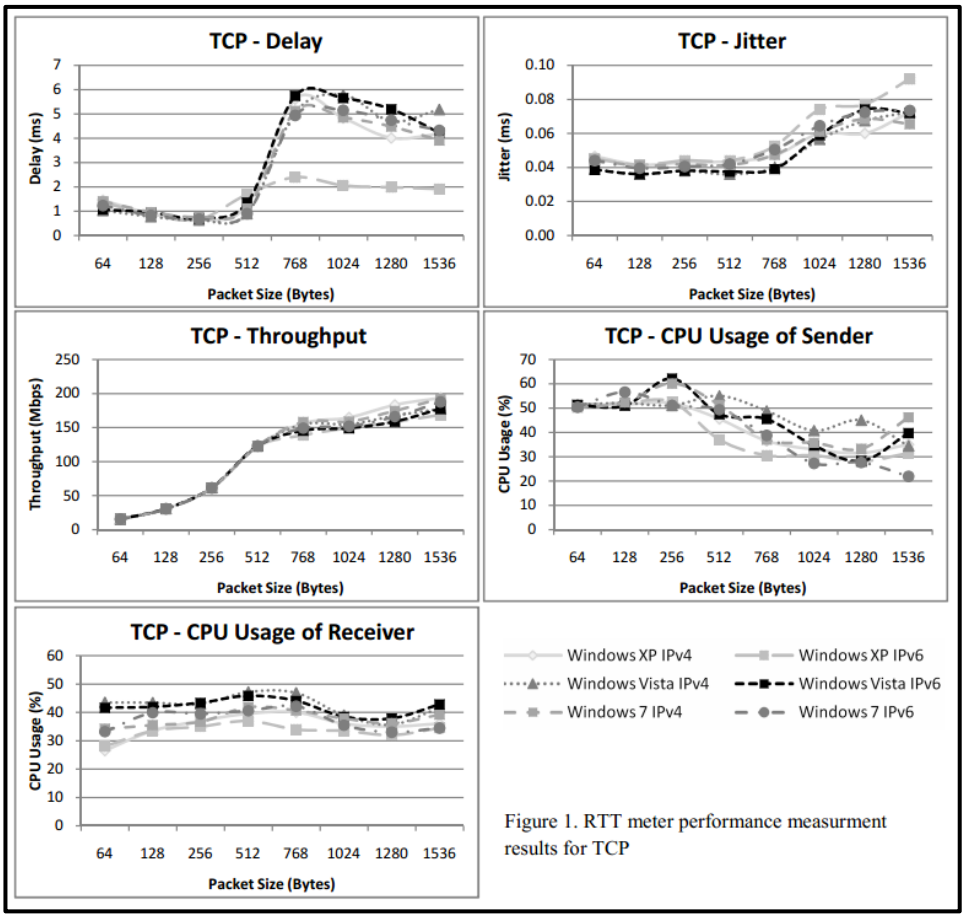
Test ortamında 100Mb/s bant genişliğine sahip bir ağ ve oldukça güçlü donanımlar kullanılmasına rağmen, aynı anda yapılan çağrı sayısı artırıldıkça, donanım kaynaklarının bu yükü taşımak konusunda yetersiz geldiği ve kararlı olmayan veriler elde edildiği görülmüştür. Şekil 4.16'da bu testlerin sonuçlarında elde edilen verilerin grafikleri görülmektedir.




**Şekil 4.16.** Testlerde elde edilen verilerin grafikleri
**(a)** Testlerin tamamlanma süreleri
**(b)** "1" saniyede tamamlanan ortalama çağrı sayıları
**(c)** Başarısız çağrı sayıları.

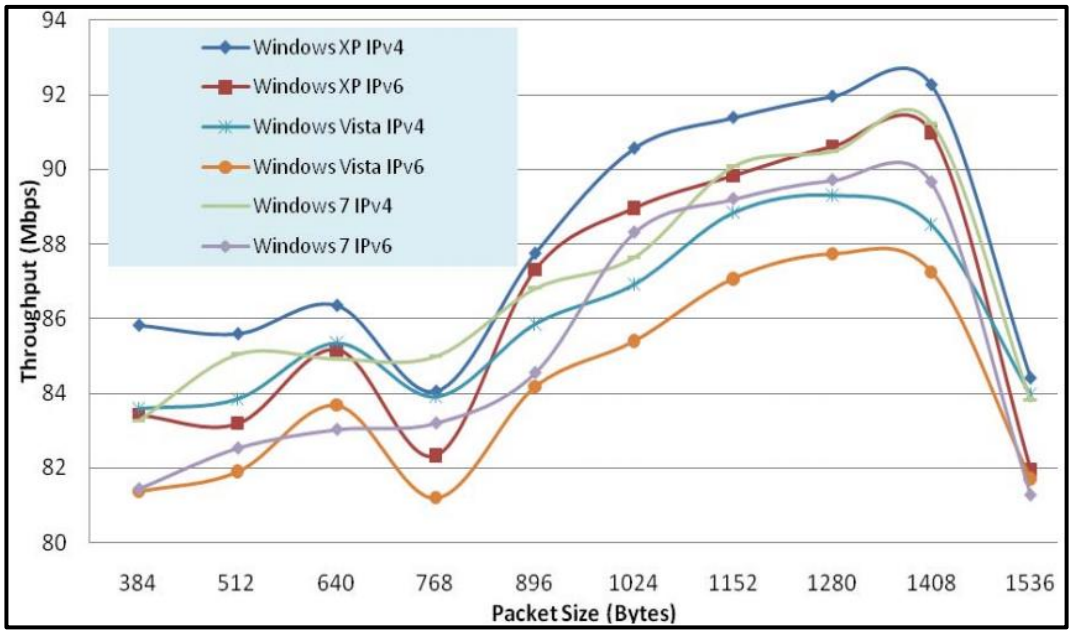
Şekil 4.16'daki grafikler incelendiğinde; testlerin tamamlanma süresi açısından, IPv6'nın performansının IPv4'e göre ortalama %2,7 daha iyi olduğu görülmektedir. Benzer şekilde; 1 saniyede tamamlanan ortalama çağrı sayıları açısından, IPv6 %2,7 daha iyi sonuç vermiştir. Başarısız çağrı sayıları isimli grafikte, IPv6 üzerinden yapılan testlerde, başarısız çağrı sayılarının IPv4'e göre %25,8 daha az olduğu görülmektedir.

Test verilerine göre SIP protokolü açısından; IPv6, IPv4'e göre daha performanslı çalışmaktadır. Ancak test sırasındaki kısıtlar mutlaka göz önünde bulundurulmalıdır. Bu testler sırasında da aynı donanım ve yazılım bileşenleri üzerinde uygulamalar yapılmıştır. Trafik verisi olarak sadece SIP paketleri kullanılmıştır. Diğer taraftan; kullanılan bilgisayarların donanımsal kaynakları, işletim sistemi sürümü, ağ kartının sürücüleri, gönderilen paket boyutu, IP üzerinde taşınan protokol, vb. etkenlerin değişik olduğu durumlarda mutlaka farklı sonuçlar çıkacaktır. Başka çalışmalarda; farklı işletim sistemleri üzerinde yapılan IPv4 ve IPv6 performans testlerine bakıldığında, oldukça farklı sonuçlar görülebilmektedir. Şekil 4.17'de Balen J. ve arkadaşları tarafından 2012 yılında yayınlanmış olan grafiklerde, Windows işletim sisteminin farklı sürümlerinde, IPv4 ve IPv6 protokollerinde ve farklı paket boyutlarında yapılan trafiklerin sonucunda elde edilen veriler gösterilmiştir. "Gecikme" (Delay) grafiğine bakıldığında; Windows XP için IPv6'da gecikme değerleri 2ms civarındayken, IPv4'te gecikme değerlerinin 4-6ms civarında olduğu görülmektedir. Windows XP'de IPv6 protokolü, "*gecikme süresi*" açısından, IPv4'e göre %100-%200 civarında daha performanslı gözükmektedir. Ancak aynı veriler Windows XP'den bir sonraki işletim sistemi olan Windows Vista'da ise birbirine çok yakın seyretmektedir (Balen J. vd., 2012).




**Şekil 4.17.** Balen J., vd. tarafından 2012 yılında yayınlanan test verileri (Balen J., vd., 2012).

Farklı uygulama ve test ortamlarında bu testler tekrarlanırsa, daha farklı sonuçlar da elde edilebilecektir. İşletim sisteminin kendisi, kaç bitlik işletim sistemi kullanıldığı, işletim sisteminin optimizasyonu, kullanılan donanımın performansı, ağın performansı ve benzeri birçok parametre bu uygulamanın sonuçlarında etkili olmaktadır. Narayan S., vd. tarafından 2010 yılında yayınlanan makalede, Windows XP işletim sisteminde IPv4 ve IPv6 ile yapılan performans testlerinde; bant genişliği açısından IPv4, IPv6'ya göre ~%2,17 daha performanslı olduğu belirtilmiştir. (Narayan S., vd., 2010) Oysa Şekil 4.17'de görülen ve Balen J. ve arkadaşları tarafından yayınlanan grafikte, bant genişliği açısından Windows XP işletim sisteminde, iki protokolün performansının da hemen hemen aynı olduğu görülmektedir. Şekil 4.18'de Narayan S. ve arkadaşları tarafından yayınlanan test verileri gösterilmiştir.




**Şekil 4.18.** Narayan S., vd., tarafından 2010 yılında yayınlanan test verileri (Narayan S., vd., 2010).

Aynı yerel ağ içerisinde SIP üzerinden çok sayıda çağrı yaparak uygulanan zorlama testleri sonrasında; IPv6'nın IPv4'ten daha hızlı çalışabileceği görülmüştür. Ancak aynı anda yapılan çağrı sayısının çok fazla artırılması durumunda, bu çalışmanın konusu dışında olan kısıtlar (*işletim sistemine, donanıma, vb. bağlı olan*) söz konusu olmaktadır. Bu nedenle, farklı bir test çalışması yapmak üzere, test laboratuvarı yeniden düzenlenmiş, protokollerin çalışmasına etki eden faktörler mümkün olduğunca azaltılmaya çalışılmıştır. Düzenlenen test ortamında yapılan çalışmalar hakkında detaylı bilgi 5. Bölümde verilmiştir.

# 5. BÖLÜM: IPV4 VE IPV6 ÜZERİNDE VOIP UYGULAMASI

İnternet Protokolü'nde sürüm 6'ya geçilmesinin getirilerinden birisi, NAT işlemine gerek kalmamasından dolayı, ağ üzerinden ses taşıma işlemlerinde kolaylık sağlamasıdır. Ancak VoIP uygulamalarında tek sorun NAT değildir. VoIP ve video konferans gibi canlı görüşmeler "zaman-kritik" olduğundan, hata kabul toleransı çok azdır. Ağdaki 2 saniyelik gecikme; bir web sayfasının yüklenmesi konusunda rahatsız edici değildir. Ancak aynı gecikme süresi bir telefon görüşmesi için kabul edilebilir sınırların dışında kalabilmektedir.

Ağ üzerinden canlı iletişim sırasında görüşmenin kalitesine etki eden; ağın yük durumu, kullanılan donanımlar, yazılımlar, protokoller, kodekler, vb. şeklinde pek çok faktör bulunmaktadır. Bu şekilde çok sayıda değişkenin etki ettiği bir sistemde sağlıklı bir karşılaştırma veya inceleme yapabilmek oldukça zordur. Çalışmanın bu aşamasında, IPv4 ve IPv6 üzerinden SIP ve RTP protokolleri kullanılarak ses iletişimi yapılmış ve çıkan sonuçlar değerlendirilmiştir. Değerlendirmenin sağlıklı olabilmesi için de performansa etki eden birtakım değişkenlerin sabitlenmesi sağlanmıştır.

R.Yasinovskyy ve arkadaşları tarafından 2009 yılında yapılan çalışmada; 100Mb/s bant genişliği olan IPv4 ve IPv6 destekli bir ağ üzerinde bir yandan ses iletişimi yaparken, diğer taraftan da ağdaki veri trafiğinin miktarını kontrollü olarak artırmaya yönelik uygulama yapılmıştır. Yine aynı çalışmada, VoIP performansının IPv4 ve IPv6 açısından kalitesine dair incelemeler sunulmuştur (Yasinovskyy vd., 2009).

Bu çalışmada ise öncekilerden farklı olarak; ortamdaki değişkenlerin ölçülen değerlere etkisini azaltmak konusunda geliştirmeler yapılmıştır. Bant genişliği 10Mb/s olacak şekilde ayarlanmış, kullanılan tüm bilgisayarların işletim sistemleri ve diğer yazılımlar aynı olacak şekilde seçilmiş, sıkıştırmasız bir kodek seçilmiş, farklı iki ağ mimarisinde testler yapılmış, her bir görüşme süresi 10 dakikanın üzerinde tutulmuş, sesli ve sessiz ayrı ayrı testler yapılmıştır.

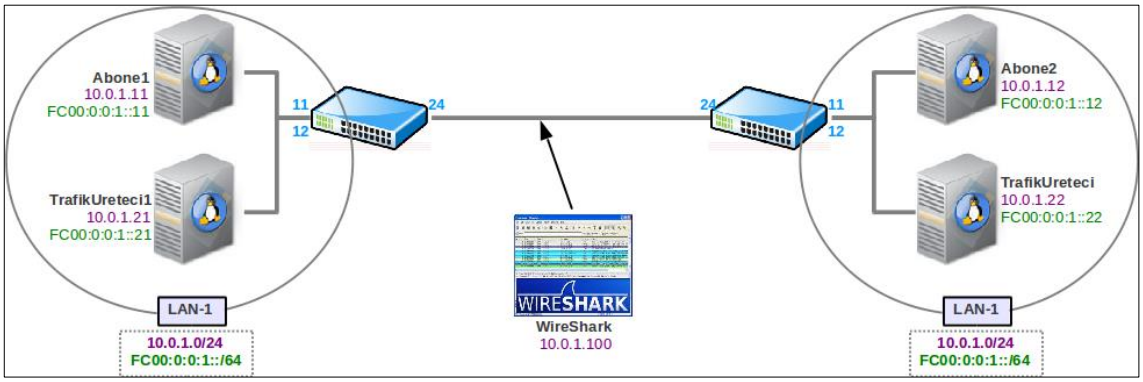
## 5.1 Test Ortamı

Ağ üzerinden ses taşıma uygulamaları hem yerel ağlarda (LAN) hem de uzak mesafe ağlarında (WAN) kullanılmaktadır. Yerel ağlarda ses taşıma konusunda çok fazla sorun bulunmamaktadır. Yerel ağlarda, yönlendirme ihtiyacı ya yoktur ya da WAN'a göre çok daha azdır. Ayrıca yerel ağlarda; bant genişliği yetersizliği sorunu olmamakta, tüm ağ donanımı kontrol altında olduğu için; istenilen ağ topolojileri uygulanabilmekte ve istenilen protokoller kullanılabilmektedir. VoIP uygulamalarında asıl sorun, WAN uygulamalarında ortaya çıkmaktadır. WAN uygulamalarında, ağın yönetimi LAN uygulamalarında olduğu kadar esnek olamamaktadır.

Bu uygulamadaki test ortamında, bir üst paragrafta belirtilmiş olan WAN uygulamalarındaki zor şartlara benzer bir laboratuvar ortamı oluşturulmuştur. Cihazlar arasındaki bant genişliği 10Mb/s olacak şekilde sınırlandırılmıştır. Bu ağ üzerinde, farklı seviyelerde trafik oluşturarak bu bant genişliği istenilen oranlarda daha da sıkıştırılmış ve İnternet protokolünün iki farklı sürümünün bu ortamda VoIP trafiği üzerine etkisi incelenmiştir. Test ortamı olarak; özel bir laboratuvar oluşturulmuş ve testler burada yapılmıştır. Şekil 5.1'de test için kurulmuş olan laboratuvar ortamı görülmektedir.

**Şekil 5.1.** Bu çalışmada kullanılan laboratuvarın fotoğrafı.

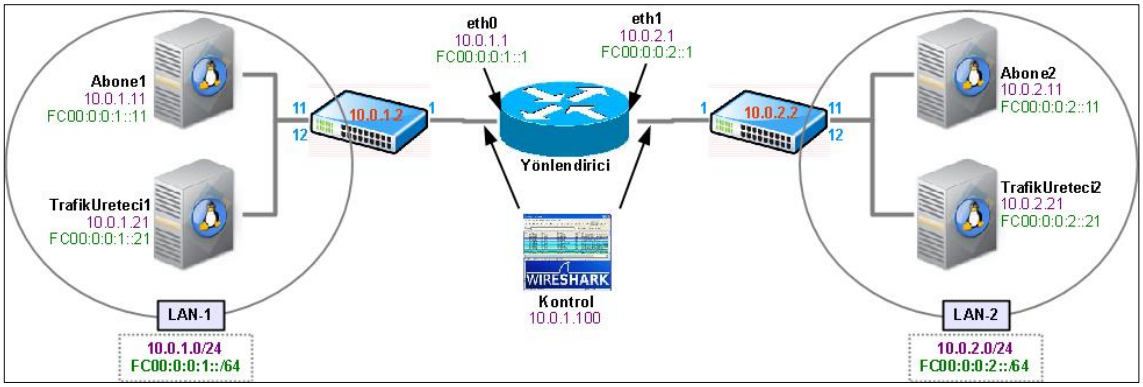
Uygulama kapsamında iki farklı ağ mimarisi kullanılmıştır. IPv4 ve IPv6 protokollerinin VoIP performansına etkisini görebilmek için; öncelikle bu protokoller yönlendirmeli ve yönlendirmesiz iki ayrı ağ üzerinde uygulanmış ve sonuçlar incelenmiştir. Daha sonra gerçek hayata daha uygun olduğu için, yönlendirmeli ağa karar verilmiş ve testler yönlendirmeli ağ üzerinde devam ettirilmiştir. Şekil 5.2'de test ortamında kullanılan yönlendirmesiz ağın diyagramı verilmiştir.




**Şekil 5.2.** Yönlendirmesiz IPv4 ve IPv6 üzerinde VoIP incelemesi mimarisi.

Yönlendirmesiz ağda, tüm trafik aynı ağ üzerinde gerçekleşmektedir. Cihazlar arasında iletişim, OSI modeline göre 2. katmanda sağlanmaktadır. Bu durum, aslında 3. katman protokolü olan İnternet Protokolü'nün sağlıklı olarak test edilmesini engellemektedir. Ancak yönlendirmesiz ağlarda gerçekleşen durumu incelemek için, böyle bir ağ uygulaması da yapılmıştır.

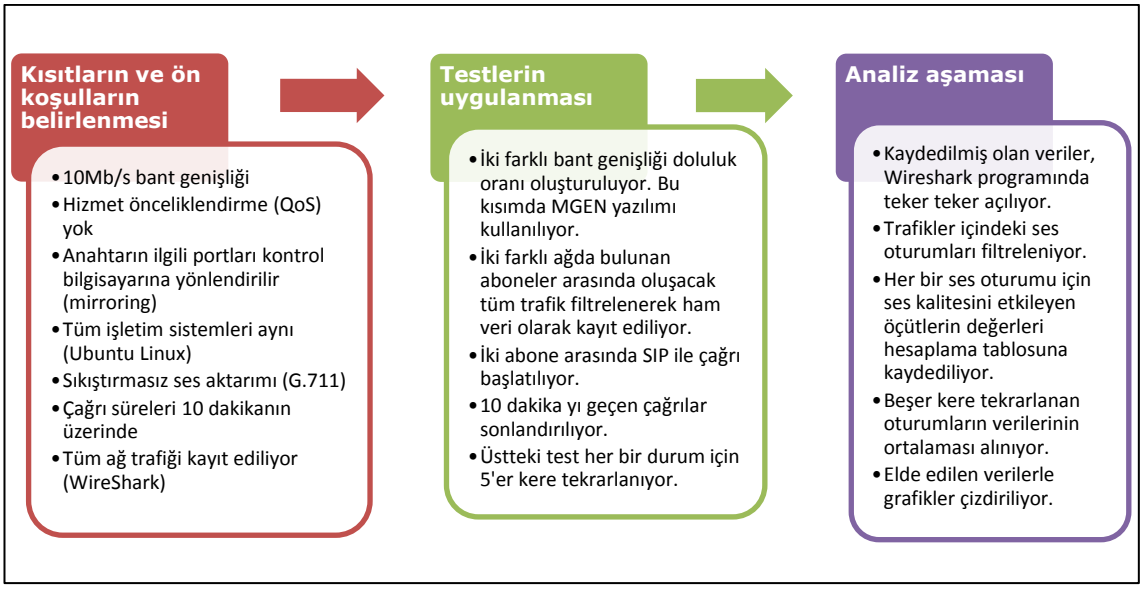
Şekil 5.3'te ise yönlendirmeli ağın diyagramı görülmektedir. Bu uygulamada, iki farklı ağ oluşturulmuş, ağların her ikisinde de IPv4 ve IPv6 çalışır hale getirilmiş, ağların diyagramda görülen yönlendirici üzerinden birbiri ile iletişimi sağlanmış ve iki ağ arasında IPv4 ve IPv6 üzerinden ses iletişimi yapılmıştır.




**Şekil 5.3.** Yönlendirmeli IPv4 ve IPv6 üzerinde VoIP incelemesi mimarisi.

Şekil 5.2 ve Şekil 5.3 üzerinde görülen bilgisayarların yanında verilmiş olan "`10.0.1.`" ile başlayan ifadeler bilgisayarın IPv4 adresini belirtirken, "`FC00:0:0:`" ile başlayan ifadeler her bilgisayarın IPv6 adresini belirtmektedir. Abone1 ve Abone2 bilgisayarları, test sırasında karşılıklı VoIP görüşmesi yapmak için kullanılmıştır. Bu sırada, TrafikUreteci1 ve TrafikUreteci2 bilgisayarları arasında da istenilen miktarlarda özel trafik oluşturulmuştur. Bu sayede; iki ağ arasındaki bant genişliği daraltılarak iletişim zorlaştırılmış ve iki farklı protokoldeki durum incelenmiştir. Şekilde "Wireshark" yazısı ile belirtilen bilgisayar, "kontrol" bilgisayarıdır. Testler sırasındaki tüm trafiğin ham veri olarak kaydedilmesi ve daha sonra kaydedilmiş verinin analizinin yapılması amacı ile kullanılmaktadır.

Uygulamada; ilave trafik oluşturarak bant genişliğini daraltmak amacı ile -*Abone bilgisayarlarının haricinde*- iki ayrı bilgisayar daha kullanılmıştır. Bu şekilde bir uygulama yapılmasının sebebi; Abone1 ve Abone2 bilgisayarlarına mümkün olduğunca az yük yüklemektir. Abone1 ve Abone2 bilgisayarlarında -değerleri etkilememesi için- zorunlu yazılımlar dışında başka hiçbir yazılım çalıştırılmamıştır. Testler sırasında uygulanan 3 aşamalı iş akışı, Şekil 5.4'te gösterilmiştir.




**Şekil 5.4.** Testler sırasında uygulanan iş akışı.

### 5.1.1 Test ortamında kullanılan donanım ve yazılımlar

**Bilgisayarlar:**

Tüm bilgisayarların donanım özellikleri aynı olup aşağıda listelenmiştir:

- Bilgisayar: HP® Compaq™ 6300 Pro MT PC
- Ana bellek: 4GB
- Sabit Disk: 500 GB
- Mikroişlemci: Intel® Core™ i5-3470 @3,2GHz CPU
- Ağ Bağdaştırıcısı: Intel® 82579LM Gigabit Ethernet
- Yönlendiricide kullanılan ikinci ağ bağdaştırıcısı: 3Com® 3C905C-TX

**Anahtarlar:**

Ağdaki anahtarların her ikisinin de modeli, HP® Procurve™ 2610'dur. Anahtarların yazılım sürümleri: `R.11.72` şeklindedir.

**Kullanılan Yazılımlar:**

Tüm bilgisayarların işletim sistemleri aynıdır. `Ubuntu GNU/Linux Desktop Edition 12.10 (64 bit)` işletim sistemi kullanılmıştır. Abone1 ve Abone2 bilgisayarlarının sesli görüşme yapabilmesi için LinPhone yazılımının `3.5.2` sürümü

kullanılmıştır. Bant genişliğini daraltma amacıyla, TrafikUreteci1 ve TrafikUreteci2 bilgisayarları arasında arka plan trafiği oluşturma işlemi için MGEN isimli yazılımın `5.02` sürümü kullanılmıştır. Anahtar üzerinden geçen trafiğin kaydedilmesi, VoIP oturumu verilerinin elde edilmesi, bazı analizlerin yapılması gibi amaçlarla Wireshark isimli yazılımın `1.8.2` sürümü kullanılmıştır. Elde edilen trafik verilerinin grafiklerini çizmek için, Libreoffice Calc yazılımından faydalanılmıştır.

## 5.2 Laboratuvarda Yapılan Özelleştirmeler

Test uygulaması için kurulan laboratuvarda kullanılan cihazlarda ve yazılımlarda, istenen koşulları oluşturmak üzere bir takım özelleştirmeler yapılmıştır. Aşağıda bu özelleştirmeler belirtilmiştir.

### 5.2.1 İşletim sistemleri

Bilgisayarlara Ubuntu Linux işletim sistemleri yüklendikten sonra, işletim sistemlerinin orijinal deposundan son güncellemeleri yapılması sağlanmıştır. Laboratuvar uygulamasında ihtiyaç duyulan uygulamalar dışında, gerekli olmayan programların kaldırılması veya başlangıçta çalıştırılmaması sağlanmıştır.

Yönlendirici olarak çalışacak olan bilgisayarın IPv4 ve IPv6 ağlarında yönlendirme yapabilmesi için, `/etc/sysctl.conf` dosyasında düzenleme yapılmıştır. Dosyada yönlendirme yapılandırmasının olduğu satırlar, Şekil 5.5'te gösterilmiştir. Şekil 5.5'te koyu olarak görülmekte olan satırlar, IPv4 ve IPv6 yönlendirmelerinin etkinleştirilebilmesi için düzenlenmiş olan satırlardır. Bahse konu satırlardaki eşitliklerin sağ tarafındaki değerin "1" olması, yönlendirme yapılacağı anlamına gelmektedir. Değerin "0" olması veya satırın devre dışı bırakılması, yönlendirme yapılmayacağı anlamına gelmektedir.

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
net.ipv6.conf.all.forwarding=1
```

**Şekil 5.5.** Linux'ta IPv4 ve IPv6 yönlendirme yapılandırması.

İşletim sistemlerinin IP yapılandırması, laboratuvar kullanımına uygun olarak sağlanmıştır. Tüm işletim sistemleri birbirleri ile IPv4 ve IPv6 üzerinden görüşebilmektedirler. İşletim sistemlerine tahsis edilen IPv4 ve IPv6 adresleri Şekil 5.3 üzerinde görülmektedir.

### 5.2.2 Anahtar yapılandırması

Laboratuvar ortamında iki tane anahtar (switch) kullanılmıştır. Anahtarların ikisi de ayrı birer ağa bağlanmış ve bu iki ağ bir yönlendirici üzerinden yönlendirilmiştir. Yapılan testler sırasında elde edilen ham verilerin kaydedilmesi için, anahtarın üzerinden port aynalama (port mirroring) ismi verilen işlem yapılmıştır. Bu işlem, anahtarın yönlendiriciye bağlı olan portundaki tüm trafiğin bir başka portuna (kontrol bilgisayarının portu) aynalanmasını sağlamış ve aktif trafiğe müdahale etmeden pasif olarak trafiğin koklanmasını (sniffing) sağlamıştır.

Yine anahtarlar üzerinde yapılan bir başka işlem de anahtarın ilgili portlarının 10Mb/s olarak çalışacak şekilde ayarlanmasıdır. Bu sayede, WAN bağlantılarına benzer bir ortam oluşturulmaya çalışılmıştır.

Anahtarlar üzerinde OSI modeline göre 2. katmandan daha yukarıda bir servis (yönlendirme, erişim denetim listesi, hizmet önceliklendirme, vb.) çalıştırılmadığı için, anahtarlarda IPv4 veya IPv6 ile ilgili özel bir yapılandırma yapılmamıştır. Anahtarlar üzerinde IP ile ilgili olarak düzenlenen tek yapılandırma, anahtara uzaktan bağlanıp yönetebilmek için bir IP adresi tahsis edilmesidir. Şekil 5.6'da, test laboratuvarında kullanılan anahtarlarda düzenlenmiş olan yapılandırmalar verilmiştir.

**LAN-1 Anahtarı**

```
hostname "testLAB-LAN1"
mirror-port 2
interface 1
   speed-duplex auto-10
exit
interface 2
   name "IZLEME-PORTU"
exit
interface 11
   speed-duplex auto-10
exit
interface 12
   speed-duplex auto-10
exit
interface 24
   speed-duplex auto-10
exit
ip default-gateway 10.0.1.1
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-28
   ip address 10.0.1.2 255.255.255.0
   exit
interface 1,24
   monitor
   exit
ip ssh
```

**LAN-2 Anahtarı**

```
hostname "testLAB-LAN2"
interface 1
   speed-duplex auto-10
exit
interface 11
   speed-duplex auto-10
exit
interface 12
   speed-duplex auto-10
exit
ip default-gateway 10.0.2.1
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-28
   ip address 10.0.2.2 255.255.255.0
   exit
ip ssh
```

**Şekil 5.6.** Test laboratuvarı anahtarlarının yapılandırmaları.

### 5.2.3 MGEN ile trafik oluşturma

MGEN yazılımı, açık kaynak kodlu ve ücretsiz bir yazılımdır. Görevi ise istenen özelliklerde bir ağ trafiğini oluşturmak ve ağdaki başka bir bilgisayara göndermektir. Programın en önemli özelliği, tamamen özelleştirilebilir bir trafik oluşturmaya izin vermesidir. Betik kullanmaya imkân vermesi sayesinde, belirli bir süre boyunca ihtiyaç duyulan trafiğin her aşaması detaylı olarak tarif edilebilmektedir. Program ile oluşturulacak olan trafiği tanımlamak için, özel bir betik dili bulunmaktadır. Şekil 5.7'de MGEN ile kullanılabilecek basit bir betik örneği verilmiştir. Çizelge 5.1'de ise betikteki komutların açıklaması verilmiştir.

| | |
|---|---|
| **1. satır** | **0.0 ON 1 UDP DST 10.2.1.9/4000 PERIODIC [10.0 1024] TOS 0x10** |
| **2. satır:** | **10.0 OFF 1** |

**Şekil 5.7.** Örnek bir MGEN betiği.

**Çizelge 5.1.** Örnek MGEN betiğindeki komutların açıklaması.

| **Komut** | **Açıklaması** |
|---|---|
| `0.0 ON 1` | 0. saniyede "1" numaralı trafiği başlat<br>(satırın devamında trafiği tanımlıyor) |
| `UDP` | Trafiğin protokolü UDP olsun |
| `DST 10.2.1.9/4000` | Trafiğin gideceği hedef IP adresi 10.2.1.9 ve portu da 4000 olsun |
| `PERIODIC` | Trafik periyodik olarak devam etsin |
| `[10.0 1024]` | 1 saniyede 10 tane 1024 Baytlık trafik gönderilsin. |
| `TOS 0x10` | IPv4 başlığı için bir eklemedir, hizmet önceliklendirmesi yapmak istenirse, kullanılabilir. |
| `10.0 OFF 1` | 10. saniyede, "1" numarası ile tanımlanmış olan trafiği durdur. |

Bu çalışma kapsamında gerçekleştirilen uygulamada, çok özelleştirilmiş trafiğe ihtiyaç duyulmadığından, Şekil 5.7'de gösterilmiş olan betik kullanılmıştır. Farklı seviyelerde trafik oluşturmak için, örnek betik içerisindeki "[10.0 1024]" şeklindeki kısımda düzenlemeler yapılması yeterli olmuştur.

MGEN ile kullanılacak olan betik yazılıp kaydedildikten sonra, trafiği başlatmak için, MGEN programına parametre olarak betiğin isminin verilmesi yeterlidir. Örneğin, ismi "`trafik1.txt`" şeklinde olan bir betik yazıldıysa, bu betiği kullanarak trafik üretmek için, "`mgen input trafik1.txt`" şeklinde bir komut verilmesi yeterlidir.

### 5.2.4 Kodek seçimi

Ses, analog bir büyüklüktür. Analog bir veriyi bilgisayar ağı üzerinden (sayısal ortamdan) bir yere aktarmak için, sayısala dönüştürmek gerekir. Kodeklerin görevi, ses ve görüntü aktarımında trafiğin iki tarafında bu dönüştürme işlemlerini sağlıklı bir şekilde yapmaktır. Kodekler, kullanılan haberleşme programına bağlıdırlar. Programın desteklemediği bir kodek kullanılamaz. Ayrıca, haberleşmenin iki tarafındaki abonelerin aynı kodeği kullanması gerekmektedir.

Farklı uygulamalar için farklı kodekler kullanışlı olabileceğinden, çok fazla sayıda kodek bulunmaktadır. Örneğin; bant genişliği sorunu olmayan yerel ağlarda sıkıştırmasız kodekler tercih edilirken; bant genişliği düşük olan özellikle WAN'larda, sıkıştırma yapan kodekler tercih edilebilmektedir.

Bu çalışma kapsamında gerçekleştirilen uygulamada, abonelerin SIP üzerinden sesli görüşme yapabilmesi için, “Linphone” yazılımı ve “G.711” ses kodeği tercih edilmiş ve kullanılmıştır. Aşağıda Linphone yazılımının tercih nedenleri belirtilmiştir:

- Ücretsiz ve açık kaynak kodlu bir uygulama olması
- Çok sayıda kodek desteklemesi
- SIP ile sorunsuz çalışması
- IPv4 ve IPv6 desteğinin sorunsuz olması
- Windows ve Linux sürümlerinin bulunması
- Adres defteri, geçmiş çağrı kayıtları, çağrı derecelendirmesi, vb. özellikler

Linphone yazılımı ilk kurulduğunda; varsayılan ses kodeği, “Speex” olarak seçili gelmektedir. Bu kodek, VBR (Variable Bit Rate ~ Değişken Bit Oranı) olarak çalıştığı için tercih edilmemiştir. VBR terimi, bir verinin aktarılması sırasında oturum oluşturulduktan sonra, aktarılan veriye bağlı olarak işgal edilen bant genişliğinin değişebileceği anlamına gelmektedir. Alternatif olarak, CBR (Constant Bit Rate ~ Sabit Bit Oranı) seçeneği de kullanılabilmektedir. CBR özellikli bir veri aktarımı sırasında kullanılan bant genişliği, oturum süresince değişmemekte, hatta kullanılacak olan bant genişliği önceden bilinmektedir.

Speex kodeğinin VBR özellikli olması, gerçek hayatta ses iletişiminde oldukça iyi sonuçlar vermektedir. Çünkü ses yoğunluğu azaldığında bant genişliğini düşürerek ağ kullanımını optimize etmektedir. Ancak VBR özellikli bir kodeğin kullanılması bu çalışma kapsamındaki testler için uygun görülmemiştir. Çünkü çalışmanın amacı; kodekleri karşılaştırmak değil, protokolleri karşılaştırmaktır. Bu nedenle, protokoller arasındaki farklılıkları incelerken, sonuçlarda etkisi olan diğer tüm kriterlerin mümkün olduğunca sabit olması tercih edilmiştir. Bu nedenle bu çalışmadaki uygulama kapsamında, CBR özellikli olan G.711a isimli kodek kullanılmıştır.

G.711 kodeği, ITU-T tarafından 1972 yılında yayınlanmış bir standarttır. Önceleri sadece telefon şebekelerinde kullanılmış olmasına rağmen, günümüzde hemen hemen tüm VoIP sistemlerinde desteklenmektedir. IP üzerinden faks taşıma gibi

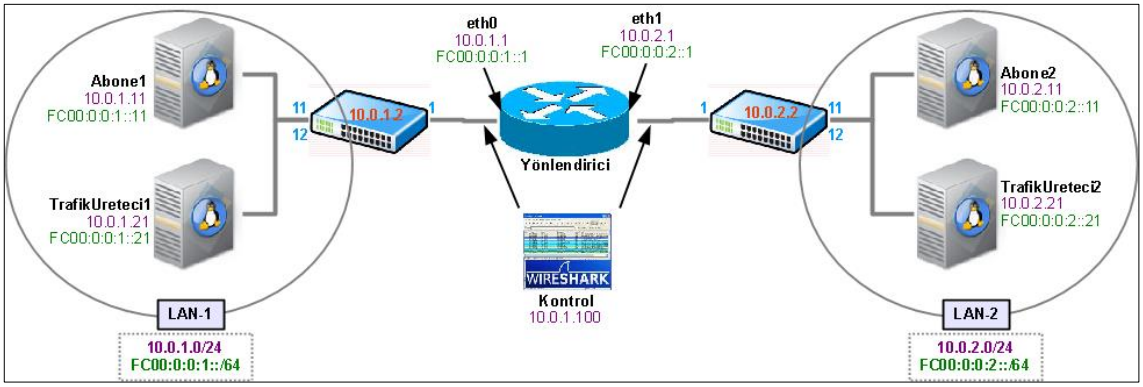
işlemlerde de kullanılmaktadır.

G.711 kodeği; analog sesi sayısala çevirirken, 300Hz ve 3400Hz frekans aralığındaki sesleri alarak 8KHz'de (1 saniyede 8.000 tane) örnekleme yapar. Her bir örneklemede 8 bitlik kodlama kullanır. Bu iki verinin çarpımı da 1 saniyedeki toplam örnek boyutunu verir. Yani G.711 kodeğinin teorik olarak bant genişliği 64Kb/s (8 KHz x 8 bit) olmaktadır. Ancak uygulamada pakete eklenen başlık bilgileri, hata kontrolü, vb. nedenlerle harcadığı bant genişliği biraz artmaktadır. Aşağıda, G.711 kodeğinin bu çalışma açısından avantajları sıralanmıştır (ITU-T, 1972):

- Açık kaynak kodlu ve ücretsizdir.
- CBR özelliklidir. Aktardığı veri miktarı sesin yoğunluğuna göre değişmez.
- Yaygın kullanılması nedeniyle hemen her platform tarafından desteklenmektedir.
- Sıkıştırma yapmadığı için; kodlama ve kod açma işlemlerinde, donanım kaynaklarını çok az kullanmakta, sisteme az yük bindirmektedir.

## 5.3 Laboratuvarda Yapılan Testler

Laboratuvarda 10Mb/s bant genişliğine sahip bir ağ üzerinde, bir yandan SIP ve RTP protokolleri ile ses haberleşmesi yapılırken, diğer taraftan da ağdaki yük durumu kademeli olarak artırılmış ve stres altında IPv4 ile IPv6 protokollerinin ses görüşmesine olan etkileri incelenmiştir. Şekil 5.8'de bu çalışma için oluşturulan laboratuvar ortamının ağ haritası gösterilmiştir.




**Şekil 5.8.** Laboratuvar ortamı.

Laboratuvardaki tüm bilgisayarlara Ubuntu Linux işletim sistemi yüklenmiştir. Uygulamada faydalanılan tüm yazılımların açık kaynak kodlu ve ücretsiz yazılımlar olmasına özen gösterilmiştir. Ağdaki tüm cihazlar hem IPv4 hem de IPv6 ile çalışabilecek şekilde yapılandırılmıştır. Şekil 5.8 üzerinde tüm cihazların isimleri ile IPv4 ve IPv6 adresleri görülmektedir.

Abone1 ve Abone2 bilgisayarları Linphone yazılımı üzerinden birbirleriyle SIP/RTP görüşmesi yapabilmektedirler. Bu iki bilgisayar, uzak mesafe ağı (WAN) üzerinden birbirine bağlı iki ayrı ağı temsil etmektedir. Bu nedenle, ağdaki anahtarların tüm portları 10Mb/s bant genişliğinde çalışacak şekilde yapılandırılmıştır. "Kontrol" isimli bilgisayar ise iki ağ arasındaki tüm trafiği kaydetmek ve daha sonra analiz etmek amacı ile kullanılmaktadır. Trafiği kaydetmek ve analiz etmek için Wireshark isimli yazılım kullanılmıştır. Wireshark, normal kullanımda tüm ağ verisini kaydettiğinden, sadece ses trafiğinin kaydedilmesi için filtre kullanılması gerekmektedir. Uygulamada Wireshark ile kullanılan filtreler aşağıda gösterilmiştir:

- **IPv4 için:** `host 10.0.1.11 and host 10.0.2.11`
- **IPv6 için:** `host FC00:0:0:1::11 and host FC00:0:0:2::11`

Ses haberleşmesi sırasında TrafikUreteci1 ve TrafikUreteci2 isimli bilgisayarlar arasında da MGEN yazılımı ile trafik üretilmiştir. Farklı kademelerde üretilen bu trafik sırasında toplam fiziksel bant genişliğinin (10Mb/s) sıkıştırılarak, ses haberleşmesinin zorlaşması sağlanmıştır. MGEN ile üretilen trafik miktarının diğer uçta gözlenmesi için, "`vnstat -l`" komutu kullanılmıştır.

## 5.4 Uygulanan Test Türleri

Laboratuvar ortamı kurulup çalıştırıldıktan sonra, çok sayıda farklı test uygulamaları yapılmıştır. Aşağıda bu uygulamalar açıklanmıştır.

**Yönlendirmeli ve yönlendirmesiz trafik testleri:** IP'nin yönlendirilebilir bir protokol olması nedeniyle, IP trafiği yönlendirilerek iki farklı ağ arasındaki trafik incelenmiştir. Ancak, yönlendirme işleminden kaynaklanan fark oluşup oluşmadığını görmek için, yönlendirici olmayan bir ağda ayrı bir test uygulaması daha yapılmıştır.

**IPv4 ve IPv6 protokol testleri:** Uygulamanın en önemli amacı, IPv4 ve IPv6 protokollerinin stres altında ses trafiği açısından incelenmesidir. Bu nedenle tüm testler her iki protokolde de uygulanmıştır.

**Sesli ve sessiz test uygulamaları:** Uygulamada kullanılan G.711 kodeği, teoride ses yoğunluğundan bağımsız olarak bant genişliği işgal etmektedir. Ancak uygulamada ses yoğunluğunun trafiğe etkisini görebilmek amacı ile sesli ve sessiz olmak üzere tüm testler tekrarlanmıştır. Sesli ve sessiz testlerin uygulanması için, bilgisayara mikrofon takılmış ve sökülmüş, bu iki durumdaki veriler de işlenmiştir.

**Farklı bant genişliklerinde test uygulamaları:** MGEN ile oluşturulan trafiğin farklı seviyeleri için; hem IPv4 hem de IPv6 protokollerinde testler uygulanmıştır. Toplam 10Mb/s olan bant genişliği MGEN ile 4Mb/s, 8Mb/s, 9Mb/s doldurularak testler uygulanmıştır. Yapılan testler, Çizelge 5.2'de gösterilmiştir.

**Çizelge 5.2.** Uygulanan test türleri.

| | | Bant genişliği doluluk miktarları | | |
|---|---|---|---|---|
| | | 4Mb/s | 8Mb/s | 9Mb/s |
| IPv4 | Sesli | ✓ | ✓ | ✓ |
| | Sessiz | ✓ | ✓ | ✓ |
| IPv6 | Sesli | ✓ | ✓ | ✓ |
| | Sessiz | ✓ | ✓ | ✓ |

Çizelge 5.2'de gösterilmiş olan test uygulamalarında sağlıklı ve kararlı sonuç alınabilmesi için her bir testteki çağrı süresi 10'ar dakika tutulmuş ve her bir test 5'er kere tekrarlanmıştır. Testler sırasında bilgisayarlara veya bilgisayar ağına herhangi bir yük getirecek uygulamaların çalışmıyor olmasına dikkat edilmiştir.

## 5.5 Çağrı Kalitesini Etkileyen Değişkenler

IP üzerinden yapılan bir çağrı sırasında, bu çağrının kalitesine etki eden birçok değişken vardır. Bu ölçümler yapılırken; sesin, konuşmacının ağzından çıktığı andan, dinleyicinin kulağına gidişine kadar olan sürecin tamamı göz önünde

bulundurulmaktadır. Aşağıda bu değişkenlerin bazıları sıralanmıştır:

- Bant genişliği (10Mbps, 100Mbps, 1Gbps, vb.)
- Ağ bağlantısının full duplex / half duplex olması durumu
- Tek yönlü / çift yönlü ses aktarımı
- Ortamdaki manyetik gürültüler
- Kullanılan ses kodeği (G.711, Speex, vb.)
- Mikrofon ve hoparlör kalitesi
- Ağ arabirim kartının kalitesi, sürücü yazılımları
- İşletim sisteminin özellikleri
- Bilgisayarın donanımlarının kapasiteleri, vb. şeklinde, çağrı kalitesine etki eden birçok değişken sıralanabilir.

IPv4 ve IPv6 protokollerinin ses taşıma üzerinde etkisini sağlıklı bir şekilde inceleyebilmek için, kullanılan protokol haricindeki diğer değişkenlerin çağrıya etkisini azaltmak için çalışmalar yapılmış ve mümkün olduğunca sabit kalmaları sağlanmıştır. Yukarıdaki listede belirtilen etkenlerden, "ortamdaki manyetik gürültüler" haricinde sıralanmış olanların tamamı kontrol altında tutulmuştur.

## 5.6 Performans Değerlendirme Kriterleri

VoIP uygulamalarında, normalde WWW trafiğinde hissedilmeyen gecikmeler ciddi sorun oluşturabilmektedir. Özellikle de aşağıdaki 3 ölçüt oldukça önem arz etmektedir:

- **Gecikme (Latency/Delay):** Temel olarak; sesin konuşmacının ağzından çıktığı andan, dinleyicinin kulağına kadar geçen süreyi ifade eder.
- **Seğirme (Jitter):** Ardışık olarak aktarılan paketlerdeki gecikme süreleri arasındaki farka, jitter ismi verilmektedir. **Gecikme varyasyonu** ya da **sapma** olarak ta ifade edilebilmektedir.
- **Paket Kaybı (Packet Loss):** Veri hattı boyunca herhangi bir nedenle bazı paketlerin karşı uca aktarılamaması durumudur. Bu değişkenler hakkında detaylı bilgi aşağıda verilmiştir.

### 5.6.1 Gecikme

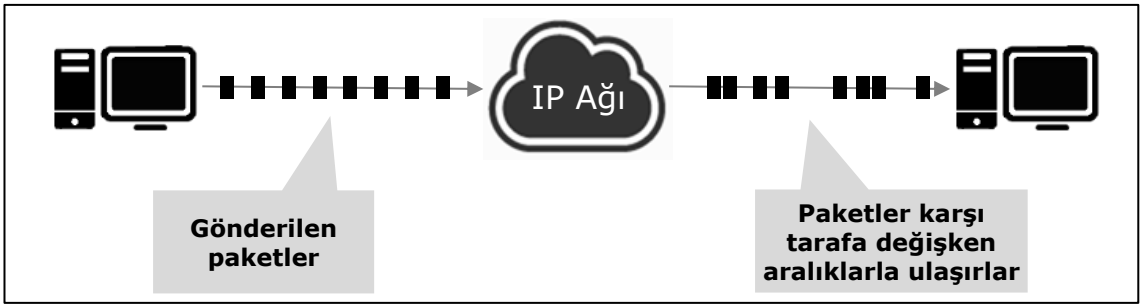
Sesin konuşmacının ağzından, dinleyicinin kulağına gelinceye kadar farklı aşamalarda yaşanan gecikmelerin toplamına denmektedir. Sesin aktarılması sürecinde birçok farklı ortamdan ve işlemden geçmesi nedeniyle, farklı aşamalarda farklı gecikme tipleri bulunmaktadır. Temel olarak üç tip gecikme bulunmaktadır, bunlar:

- **Yayılım Gecikmesi (Propagation Delay):** Fiber optik kablolarda ışığın; bakır kablolarda ise elektrik işaretinin ilerlemesi için geçen süredir.
- **Yayınlama Gecikmesi (Serialization Delay):** Bir bit veya baytın ağ arabirimi üzerine koyulması için harcanan süreyi ifade eder. Diğer gecikmelerin yanında kayda alınmayacak kadar küçük bir değerdir.
- **İşleme Gecikmesi (Handling/Processing Delay):** Paketin herhangi bir aşamada işlenmesi ile ilgili tüm gecikmeleri (paketleme, sıkıştırma, anahtarlama...) kapsar.

Sesli iletişiminde kabul edilebilir gecikme değerleri konusunda kesin bir sınır çizmek zordur. Farklı insanların, problem kabul toleransı farklı seviyelerde olabilmektedir. Bu nedenle; ITU-T tarafından 2003 yılında yayınlanan G.114 numaralı referansta bu konuda bir tavsiye belirtilmiştir. Bu referans belgesine göre; ağızdan kulağa kadar, tek yönde kabul edilebilen maksimum gecikme 150ms'den az olmalıdır. Tercih edilen seviye ise 100ms'den daha düşük değerlerdir. Gecikme 400 milisaniyeyi aştığında ise kabul edilemez seviyededir (ITU-T, 2003).

### 5.6.2 Seğirme

Canlı ses görüşmesinin kaliteli bir şekilde yapılabilmesi için, ardışık aktarılan paketlerin gecikme süreleri birbirine yakın olmalıdır. İdealde ise tüm gecikme miktarları aynı olmalıdır. Ancak gecikmesiz bir veri aktarımı mümkün olmadığı gibi, tüm paketlerdeki gecikmelerin de aynı seviyede olması mümkün değildir. Ardışık olarak aktarılan paketlerdeki gecikme süreleri arasındaki farka; seğirme (jitter) ismi verilmektedir. Şekil 5.9'da seğirmenin paketler üzerindeki etkisi temsili olarak gösterilmiştir.




**Şekil 5.9.** Seğirmenin temsili gösterimi.

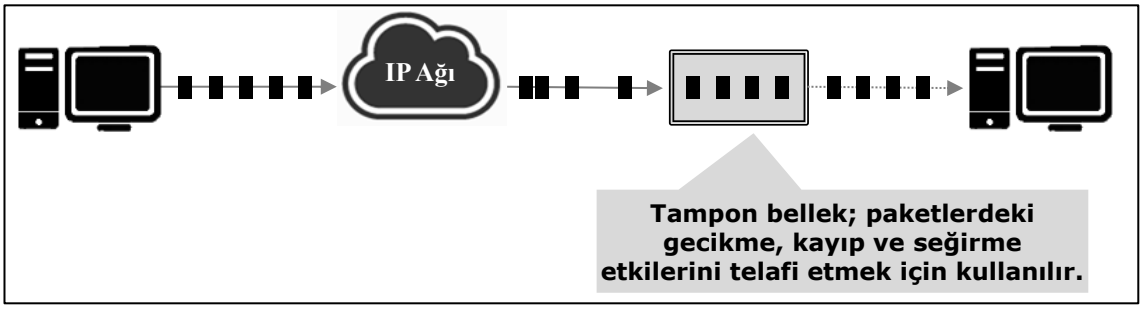
Seğirme; "paketlerin ağdaki yönlendiricilerin kuyruğunda bekleme sürelerinin farklı olması", "paketlerin farklı yollardan hedefe gidebilmesi", "ağda hizmet önceliklendirmesi olmaması" gibi nedenlerle oluşabilmektedir. VoIP iletişimi yapmak üzere tasarlanan donanım ve yazılımlarda gecikme farklılıklarını dengelemek üzere bir tampon bellek kullanılabilmektedir. Tampon bellek büyütüldükçe, seğirme azalmakta ancak paketlerin gecikme miktarı artmaktadır. (Manousos, vd., 2005)

### 5.6.3 Paket kayıpları

Ağ üzerinde iki bilgisayar arasında veri aktarımı sırasında; kaynaktan çıkan verilerin bazılarının, herhangi bir nedenle karşı uca ulaşamaması durumudur. Genellikle yoğun veya parazitli hatlarda yaşanır. Hat yoğun olduğunda ağın stresi artar ve paketler bozulmaya başlar. Bu duruma "paketlerin düşmesi" adı verilmektedir.

Paket kaybı, gerçek hayattaki veri trafiklerinde sıkça karşılaşılan bir durumdur. Veri aktarım sistemlerinin kendi içinde hata tespit/düzeltme mekanizmalarının olması nedeniyle, genellikle hissedilir bir etkisi olmamaktadır. Örneğin TCP, tüm paketlerin hedefe ulaştığını garanti edebilmektedir. Bu tarz protokollerde, aktarılan verinin hedefe tam olarak ulaşıp ulaşamadığının anlaşılabilmesi için; bir bütünü oluşturan tüm paketler numaralandırılmakta, karşı uca gönderilen paketler tampon bellekte biriktirilmekte ve verinin tamamı karşıya ulaştıktan sonra ilgili veri işlenebilmektedir. Karşıya ulaşamayan kayıp paketler yeniden iletilebildiğinden, çoğunlukla veri kaybı olmamakta ancak uygulamada bu durumun etkisi "yavaş iletişim" şeklinde hissedilebilmektedir. Kayıp oranları yükseldikçe iletişim daha da yavaşlamaktadır. Veri aktarımında tampon

belleğin yeri, temsili olarak Şekil 5.10'da gösterilmiştir.

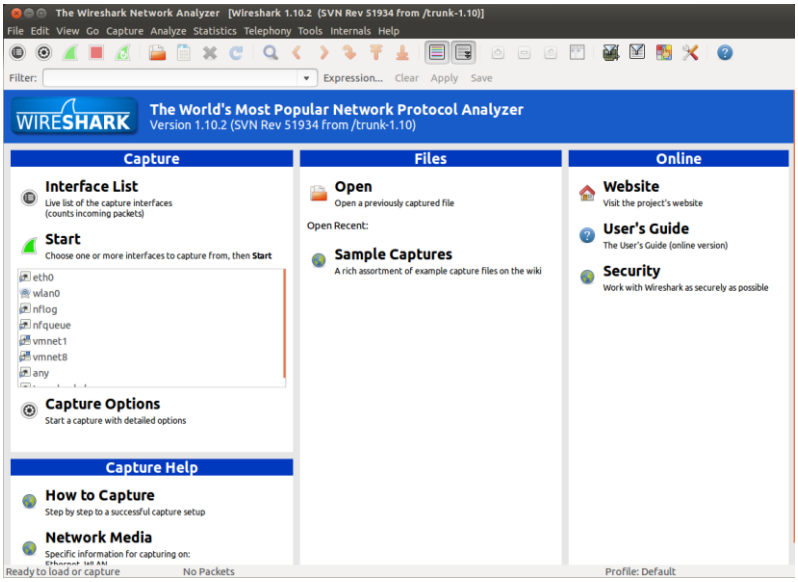



**Şekil 5.10.** Tampon belleğin temsili gösterimi.

Canlı ses haberleşmesi gibi anlık iletişimlerde, tampon bellek boyutunun artırılması, doğrudan ses iletişiminin gecikmesine ve kabul edilemez beklemelere sebep olabilmektedir. Bu nedenle ses haberleşmesinde kullanılan protokoller genellikle; hata düzeltme mekanizması olmayan UDP protokolü üzerinde çalışmaktadır. İki uç arasında; anında ve doğru sırada aktarılması gereken bir trafik söz konusu ise, kaybolan paketlerin yeniden gönderilmesi çok anlamlı olmamaktadır. Mikrofondan bir sözcük söylendiğinde; sözcüğün başındaki sese denk gelen paket kaybolmuşsa, ilgili paketin hemen yeniden gönderilmesi ve karşı tarafta yeniden seslendirilmesi, sözcüğün sonunda normalde olmaması gereken bir sesin çıkmasına sebep olabilir. Bu nedenle VoIP haberleşmesinde, kaybolan paketlerin yeniden gönderilmesi tercih edilmemektedir.

## 5.7 Ses Trafiklerinin Kayıt Edilmesi ve Ölçümlerin Yapılması

Ağ üzerinden gerçekleştirilen veri trafiğini dinlemek için kullanılan programlara "network sniffer (ağ koklayıcı, ağ dinleyici)" denmektedir. Bu çalışmada oluşturulan trafikleri kayıt etmek ve incelemek için, ücretsiz bir program olan "Wireshark" tercih edilmiştir. Wireshark; bir bilgisayarın ağ arabiriminden geçen tüm verileri kayıt edebilmekte, bu verileri süzebilmekte, trafik oturumlarını bütün olarak analiz edebilmektedir. Şekil 5.11'de, Wireshark'ın başlangıç ekranı görüntüsü verilmiştir.




**Şekil 5.11.** Wireshark programının başlangıç ekranı.

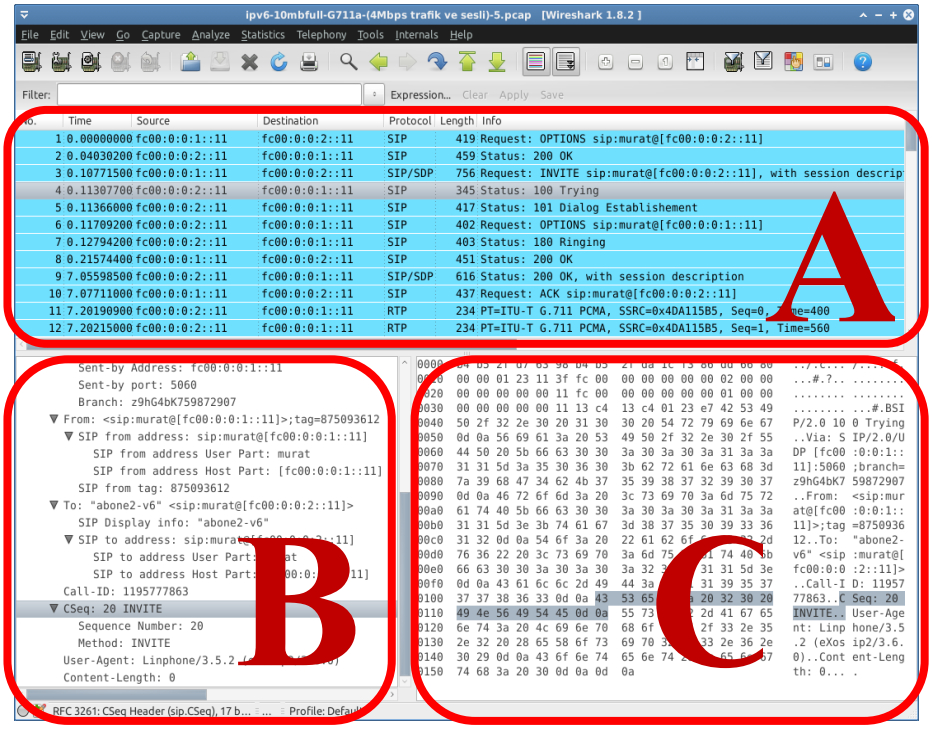
Çalışmamız sırasında; iki bilgisayar arasında yapılan ses trafikleri Wireshark ile kayıt edilmiştir. Daha sonra bu trafik verileri içerisindeki SIP+RTP ses oturumları yine Wireshark içerisinde hazır gelen VoIP modülü vasıtasıyla analiz edilmiştir. Çizelge 5.3'te Wireshark'ta ölçülen değerlerin açıklamaları verilmiştir.

**Çizelge 5.3.** Wireshark'ta ölçülen değerler.

| **Değer** | **Açıklama** |
|---|---|
| Delta | Bir paket ile kendisinden bir önceki paketin ulaşım süresi farkı. |
| Max Delta[1] | Oturum boyunca görülen en büyük Delta değeri. |
| Max Jitter | Her bir paket için hesaplanan seğirme değerlerinden en büyük olanı. |
| Mean Jitter | Hesaplanan tüm seğirme değerlerinin aritmetik ortalamasıdır. |
| Lost Packets | Oturum boyunca, hedefe ulaşamayan paketlerin oranı. |

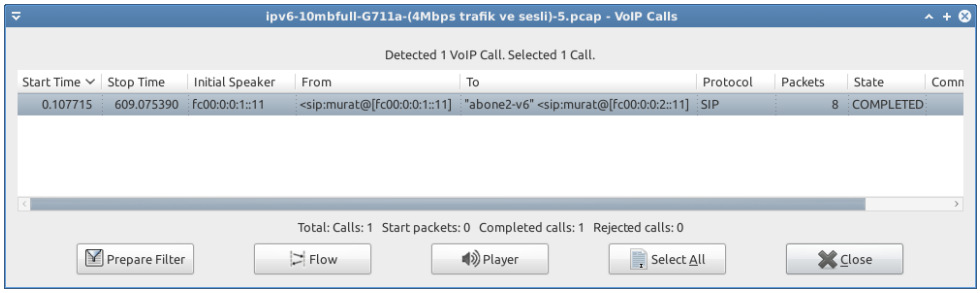
Şekil 5.12'de, Wireshark'ta kaydedilmiş bir ses oturumuna ait paketler görülmektedir. Programın ekranı temel olarak üçe bölünmüştür. "A" harfi ile belirtilen üst bölümde, o anda incelenen trafiğin paketlerinin satırlar halinde listesi bulunmaktadır. Kayıt edilen oturumun ilk paketi ilk sıradaki pakettir. Herhangi bir paketin (satırın) üstüne tıklandığında; şekilde "B" harfi ile belirtilen bölmede paketin başlık bilgileri, "C" harfi ile belirtilen bölmede ise paketin veri kısmının içeriği görülmektedir.

[1] Wireshark'tan alınan "max delta" değerleri; kayıp veya bozuk paketlerde, 10 kata kadar yüksek çıkabilmektedir. Bu nedenle; az miktardaki bozuk paketlerdeki değerler ortalamaya dâhil edilmemiştir.




**Şekil 5.12**. WireShark'ta bir SIP paketinin incelenmesi.

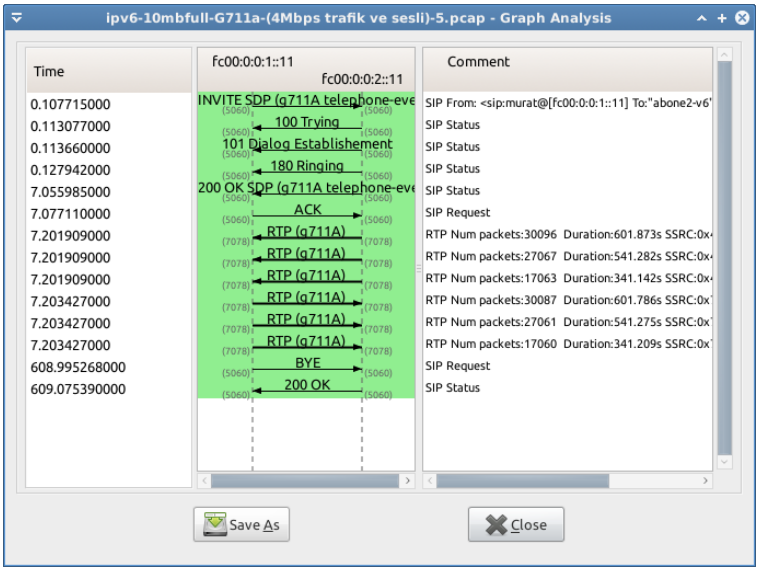
Paketler, bireysel olarak ya da ses oturumu bütünü olarak ta incelenebilmektedir. Şekil 5.13'de, bir trafik verisindeki ses paketlerinin Wireshark tarafından ayrıştırılarak bütün bir sesli görüşme oturumunun program tarafından tanındığı görülmektedir. Bu ekranda, ses oturumunun başlama ve bitiş zamanları, kaynak ve hedef bilgisayar bilgileri, kullanılan protokol bilgisi, oturum içerisindeki toplam paket sayısı, oturumun durumu (tamamlanmış, devam ediyor, reddedildi, vb.) gibi bilgiler görülmektedir.




**Şekil 5.13.** Wireshark'ın ses oturumları penceresi.

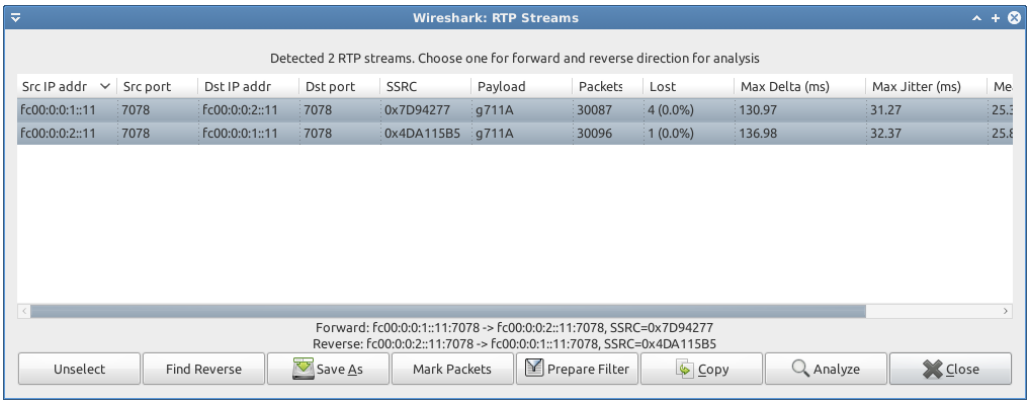
Şekil 5.13'te görülen "Player" düğmesiyle, ses oturumu yeniden dinlenebilmektedir. "Flow" düğmesiyle, "akış" (flow) şeklinde görülebilmektedir. Şekil

5.14'te örnek oturum akışı görülmektedir. SIP'e ait "INVITE" mesajı ile başlatılan oturum, karşı tarafın kabul etmesiyle devam etmekte ve RTP protokolü üzerinden ses akışı sürdürülmektedir. Son olarak, "BYE" mesajı ile oturumun bitirilmesi sağlanmıştır.




**Şekil 5.14.** WireShark'ta bir SIP oturumunun incelenmesi.

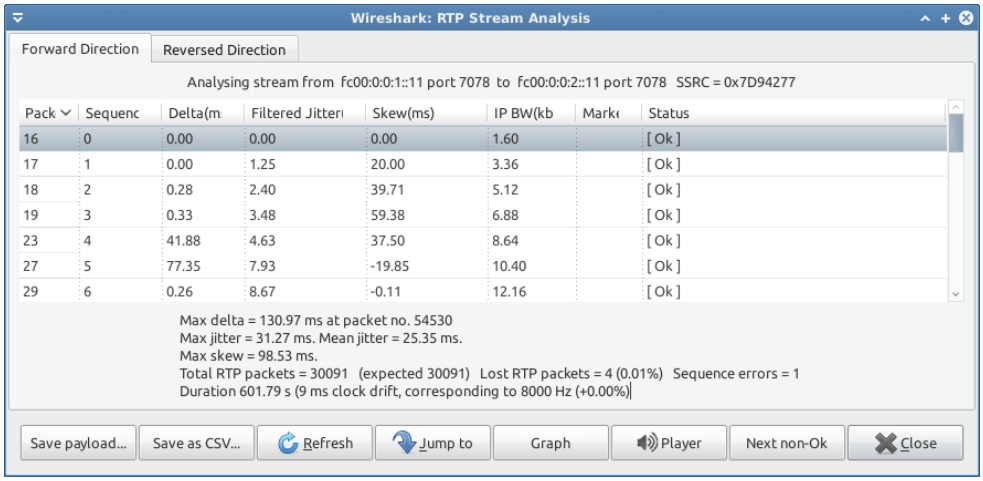
Sesli görüşme sırasında aktarılan seslerin incelenebilmesi için; RTP oturumu analiz edilmelidir. Şekil 5.15'te, Wireshark'ta kayıt edilmiş olan, iki yönlü bir RTP oturumunun özeti görülmektedir.




**Şekil 5.15.** WireShark'ta bir RTP oturumunun görüntülenmesi.

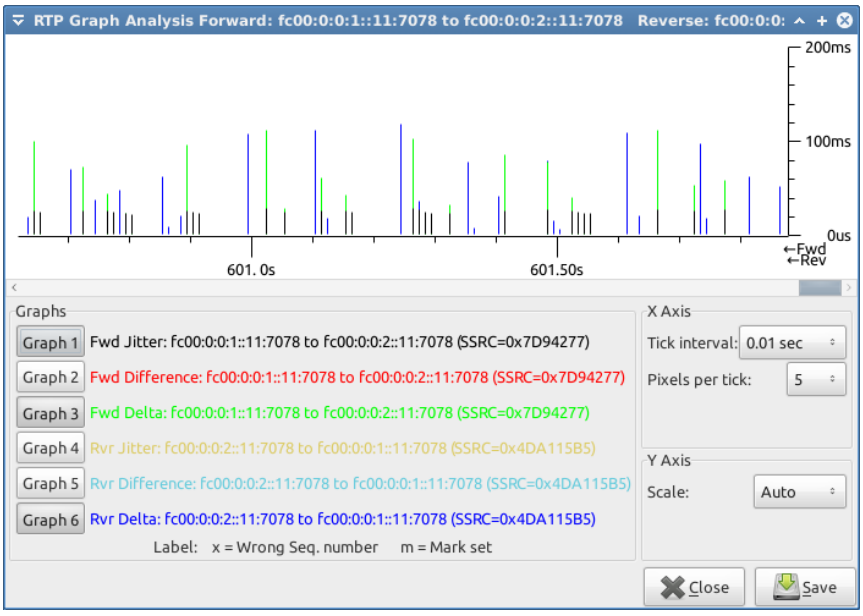
Şekil 5.15'teki "Analyze" düğmesine tıklandığında; bu RTP oturumunun analizi yapılmakta, ilgili verileri hesaplamaktadır. Şekil 5.16'da RTP oturumunda ölçülen ve

hesaplanan değerler gösterilmiştir. IPv4 ve IPv6'nın etkisinin incelenmesi için kullanılacak veriler (*delta, max delta, jitter, max jitter, lost packet*) bu ekrandan alınabilmektedir. İlgili RTP oturumu içerisindeki her bir paket alt alta listelenmekte ve her bir paket için ölçülen ve hesaplanan değerler ekranda gösterilmektedir.




**Şekil 5.16.** WireShark'ta RTP oturumu analizi.

Şekil 5.16'daki "Graph" düğmesiyle, her bir RTP paketi ile ilgili değerler grafik halinde görülebilmektedir. Şekil 5.17'de RTP oturumu grafik analizi gösterilmiştir. Oturumun herhangi bir anındaki değer grafik üzerinde görülebilmektedir.




**Şekil 5.17.** WireShark'ta RTP oturumu grafik analizi.

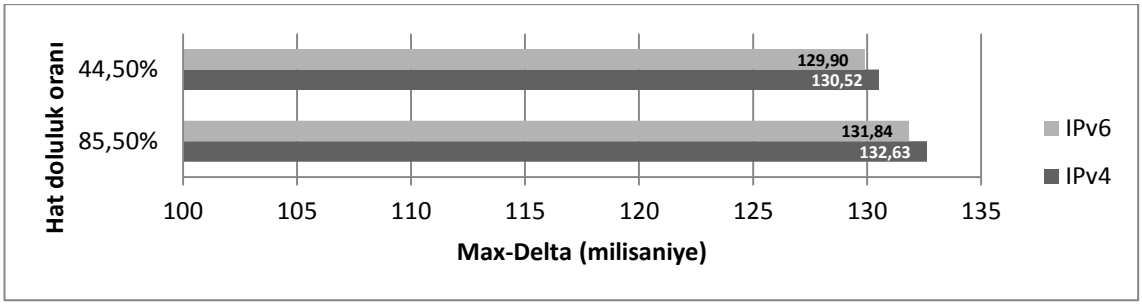
## 5.8 Ölçülen Veriler

Testler sırasındaki kayıtlarda, bant genişliği doluluğu arttıkça kayıp paket oranı artmaktadır. Ses trafiğinde IPv4 ve IPv6 etkilerini inceleyebilmek için; hattın iki farklı doluluk durumunda yapılan trafiklerle ilgili veriler burada paylaşılmıştır. Çizelge 5.4'te uygulama sırasında kaydedilen veriler kullanılarak ölçülen ve hesaplanan veriler gösterilmiştir.

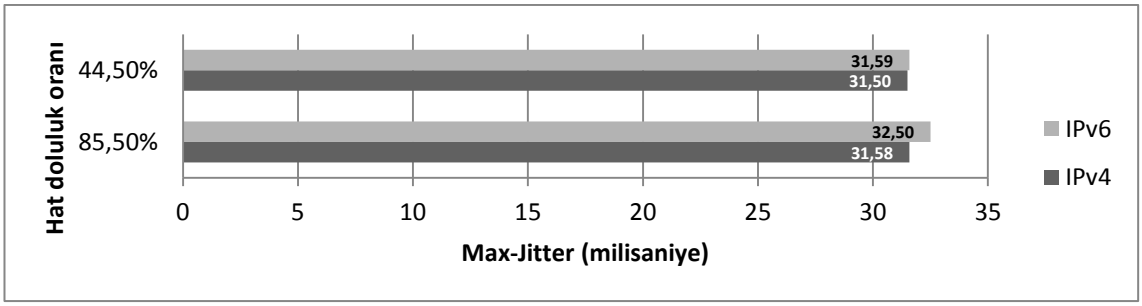
**Çizelge 5.4.** Ölçülen ve hesaplanan veriler.

| Hat doluluğu | IP sürümü | Çağrı kayıt no | Süre (sn) | Azami delta (sn) | Azami seğirme (sn) | Ortalama seğirme (sn) | Kayıp paketler |
|---|---|---|---|---|---|---|---|
| %44,5 | 4 | 1 | 603,30 | 128,22 | 31,54 | 24,45 | %0,00 |
| | | 2 | 603,49 | 128,90 | 31,75 | 24,57 | %0,18 |
| | | 3 | 603,04 | 129,34 | 31,23 | 24,48 | %0,57 |
| | | 4 | 604,37 | 136,56 | 31,95 | 24,64 | %0,00 |
| | | 5 | 604,53 | 129,58 | 31,04 | 24,80 | %0,18 |
| | | Ortalama | 603,75 | 130,52 | 31,50 | 24,59 | %0,19 |
| | 6 | 1 | 602,34 | 128,18 | 32,12 | 24,93 | %0,02 |
| | | 2 | 612,70 | 128,56 | 31,18 | 25,05 | %0,02 |
| | | 3 | 602,12 | 131,58 | 31,22 | 25,24 | %0,00 |
| | | 4 | 601,59 | 130,88 | 31,41 | 25,29 | %0,00 |
| | | 5 | 625,20 | 130,30 | 32,02 | 25,49 | %0,00 |
| | | Ortalama | 608,79 | 129,90 | 31,59 | 25,20 | %0,01 |
| %85,5 | 4 | 1 | 601,66 | 134,42 | 32,25 | 20,21 | %5,44 |
| | | 2 | 622,32 | 136,62 | 31,60 | 20,39 | %0,00 |
| | | 3 | 600,96 | 128,65 | 31,88 | 20,04 | %0,30 |
| | | 4 | 600,67 | 127,01 | 31,30 | 19,53 | %0,69 |
| | | 5 | 601,51 | 136,46 | 30,89 | 20,02 | %1,59 |
| | | Ortalama | 605,42 | 132,63 | 31,58 | 20,04 | %1,60 |
| | 6 | 1 | 615,60 | 135,12 | 31,90 | 24,48 | %0,88 |
| | | 2 | 601,95 | 128,44 | 31,59 | 23,83 | %0,50 |
| | | 3 | 620,02 | 128,71 | 34,24 | 24,43 | %0,08 |
| | | 4 | 608,80 | 137,08 | 32,74 | 25,06 | %0,01 |
| | | 5 | 605,06 | 129,86 | 32,02 | 24,98 | %0,02 |
| | | Ortalama | 610,29 | 131,84 | 32,50 | 24,56 | %0,30 |

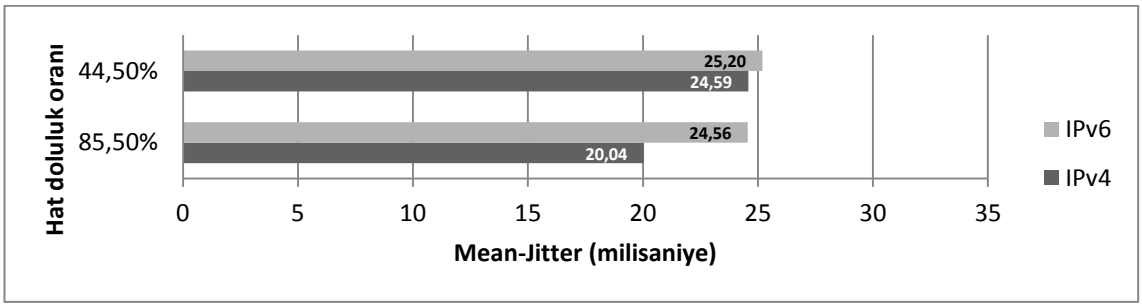
Çizelge 5.4'te verilmiş olan ortalama değerler ile çizilen grafikler Şekil 5.18, Şekil 5.19, Şekil 5.20 ve Şekil 5.21'de verilmiştir.




**Şekil 5.18.** IPv6 ve IPv4 için azami delta grafiği.



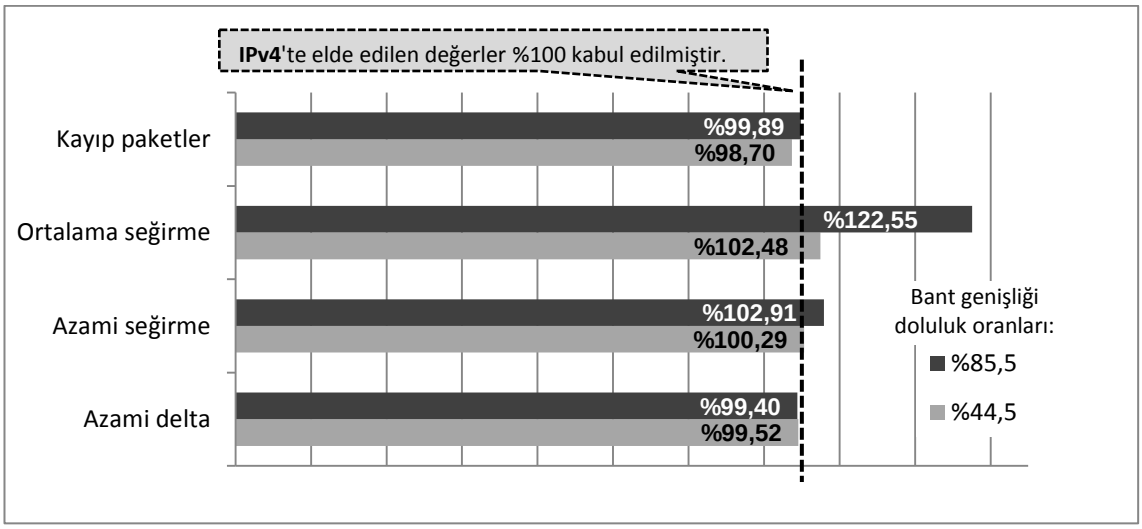

**Şekil 5.19.** IPv6 ve IPv4 için azami seğirme grafiği.




**Şekil 5.20.** IPv6 ve IPv4 için ortalama seğirme grafiği.


**Şekil 5.21.** IPv6 ve IPv4 için paket kayıpları grafiği.

Çizelge 5.4'teki değerlerde, IPv4 ve IPv6 arasında bir kıyaslama yapılabilmesi için, IPv4 kullanıldığı durumdaki değerler norm (%100) kabul edilmiştir. Daha sonra, IPv6 kullanıldığındaki değerler IPv4 değerlerine oranlanarak, tüm değerler aynı grafik üzerinde toplanmış ve elde edilen grafik Şekil 5.22'de gösterilmiştir. Grafikte verilmiş olan; sesin kalitesine etki eden bu değişkenlerin idealde "0" olması gerekmektedir. Dolayısıyla grafik üzerinde "**küçük**" olan değerler daha "**iyi**" olarak okunmalıdır.




**Şekil 5.22.** IPv4 değerlerine kıyasla IPv6 değerlerinin oranları.

## 5.9 Bulgular

Test laboratuvarında yapılan çalışmalarda kaydedilen trafiklere ait değerlerden elde edilen bulgular aşağıda sıralanmıştır.

**i.** Kayıp paket miktarlarının, protokole bağlı olarak büyük değişiklik göstermediği, ancak IPv6'da kayıpların her durumda daha az olduğu görülmüştür. Ağda trafik yükünün az olduğu durumda, IPv6'nın başarımı IPv4'e göre %1,3 daha iyi fazladır. Arka plan trafik yükü artırıldığında, IPv6'daki kayıplar da artmaktadır.

**ii.** Seğirme (jitter) açısından diğer değişkenlere kıyasla oldukça büyük farklılık vardır. IPv6'da ortalama seğirme her durumda IPv4'e göre daha fazladır. Ancak özellikle ağ yükü arttığında, IPv6'da, IPv4'e göre %22,55 kadar daha fazla seğirme görülmüştür.

**iii.** Azami delta (*iki ardışık paket arasındaki en fazla zaman farkı*) değerlerinin her durumda IPv6'da %0,005 civarında daha iyi olduğu görülmüştür. Ağdaki trafik yükü arttığında, protokolden bağımsız olarak azami delta değerinde %0,015 civarında artış olmuştur.

**iv.** Azami seğirme değerleri, ağda trafik az iken her iki protokolde çok yakın çıkmıştır. Arka plan trafik miktarı arttırıldığında ise IPv6'nın azami seğirme değeri, IPv4'tekine göre %2,91 fazla olmuştur.

**v.** İletim hattının doluluğu arttıkça, IPv6 üzerinde yapılan VoIP trafiklerinde seğirmeye bağlı hatalar IPv4'e göre daha hızlı artmaktadır.

## 5.10 Bulguların Değerlendirilmesi

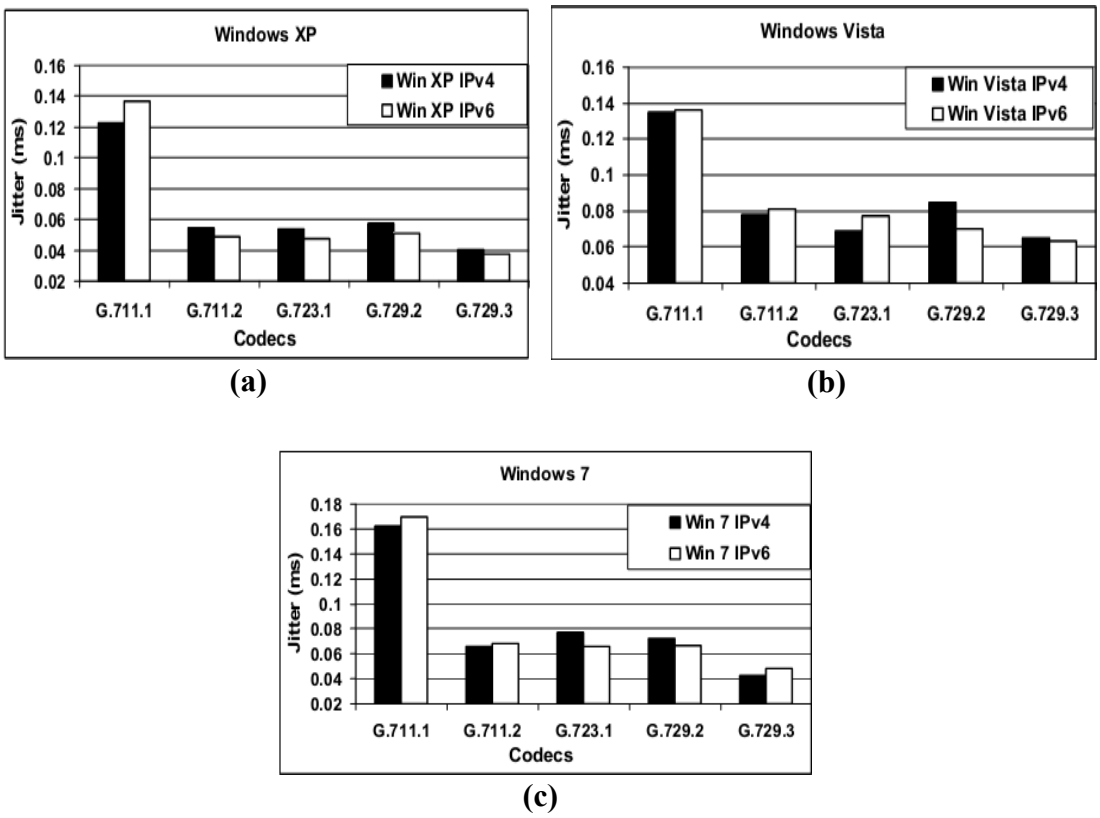
IP ağlarında, canlı iletişim trafiklerinin TCP yerine UDP üzerinden sağlanması performans ve işlevsellik açısından verimli olmakta, ancak bir sorunu da beraberinde getirmektedir. TCP, yapısı gereği oturum temelli bir protokol olduğundan, bir oturum süresince aktarılan tüm veriler "bütün" olarak değerlendirilir. Bu sayede oturum kurulduktan sonra, oturum kapatılana kadar olan tüm trafik daha kolay aktarılmaktadır. Trafiği yoğun olan bir ağda hem TCP hem de UDP trafiği varsa, öncelikle UDP trafiği sorun yaşamaktadır. Çünkü her bir TCP oturumu için; gönderilen her paketin karşı uca ulaşıp ulaşmadığı kontrol edilmekte, problem varsa yeniden gönderilmektedir. Bunun sebep olduğu gecikme çok az olduğundan, TCP trafiğinde önemsenmeyecek kadar küçük olmaktadır. UDP'de ise -*TCP'nin tersine*- oturum denetimi bulunmamaktadır. Yerel ağlarda, bant genişlikleri çok yüksek olabildiğinden, performans açısından TCP/UDP trafikleri arasındaki farklar hissedilebilecek oranda olmamaktadır. Ancak WAN bağlantılarında ve diğer bant genişliği düşük olan ağlarda, herhangi bir önceliklendirme yapılmamış ise UDP trafiklerinde kayıplar ve performans sorunları artabilmektedir.

Bu çalışmada elde edilen bulgular sonucunda; VoIP trafiği için IPv4 ve IPv6 ağlarında genel anlamda performans açısından farkın, önemsenmeyecek kadar az olduğu görülmüştür. Seğirme değerleri haricindeki (*seğirme değerinin fazla olduğu durum, sonraki paragrafta ele alınmıştır*) tüm ölçütlerde IPv4 ve IPv6 arasındaki

performans farkı en fazla %2-3 seviyesindedir. Trafik şekillendirme[1] yapılmayan ağlarda, bu tarz sonuçlar gayet normaldir. Bu sonuç, önceki çalışmalarla da uyumludur. 2009 yılında R. Yasinovskyy ve arkadaşları tarafından yayınlanan "*VoIP Call Performance Over IPv6 During HTTP and Bittorrent Downloads (HTTP ve Bittorrent ile dosya indirme işlemi sırasında IPv6 üzerinden yapılan VoIP çağrılarının performansı)*" isimli çalışmada; VoIP performansının IPv4 ve IPv6'da çalıştırılmasına göre önemsenmeyecek derecede fark olduğu belirtilmiştir. Yine R. Yasinovskyy ve arkadaşları tarafından 2009 yılında yayınlanan "*Impact of IPSec and 6to4 on VoIP Quality over IPv6 (IPSec ve 6to4'un IPv6 üzerinde VoIP kalitesine etkisi)*" isimli çalışmada, çok yoğun olmayan ağ trafiklerinin, VoIP üzerindeki etkisinin minimal olduğu belirtilmiştir (Yasinovskyy vd., 2009).

Ölçümler sonucunda; VoIP kalitesini etkileyen değişkenlerden seğirme'nin IPv6'da (iletim hattının doluluğu arttığında) IPv4'e göre %22,55 daha fazla olduğu görülmüştür. Şekil 5.20'ye bakıldığında, grafikteki 4 değerden 3 tanesinin birbirine çok yakın olduğu, IPv4'ün yüksek bant genişliği durumunda daha düşük değerde olduğu görülmektedir. Şekil 5.22'deki grafikte; IPv4 değerleri %100 kabul edildiği ve IPv6 değerleri de IPv4 değerlerine oranla çizdirilmiş olduğu için, IPv6 değerleri yüksek çıkmış gibi görülmektedir. Daha önce yapılmış çalışmalara bakıldığında, testler sırasında kullanılmış olan G.711 kodek için IPv4'ün seğirme değerlerinin genellikle IPv6'ya göre daha az olduğu görülmüştür.
Şekil **5.23**'te, H.Sathu vd. tarafından 2012 yılında yayınlanan grafikler gösterilmiştir (Sathu vd., 2012).

[1] Bilgisayar ağlarında trafiğin farklı koşullara göre (önem, aciliyet, protokol türü, IP adresi, vb.) sınıflandırılması ve kurallar (önceliklendirme, kısıtlama, engelleme, iletim hattının belirli kısmını tahsis etme, vb.) uygulanması işlemlerine genel olarak "*trafik şekillendirme*" denmektedir.




**Şekil 5.23.** İşletim sistemi, kodek ve IP sürümüne göre seğirme karşılaştırması (a) Windows XP; (b) Windows Vista; (c) Windows 7 (Sathu vd., 2012).

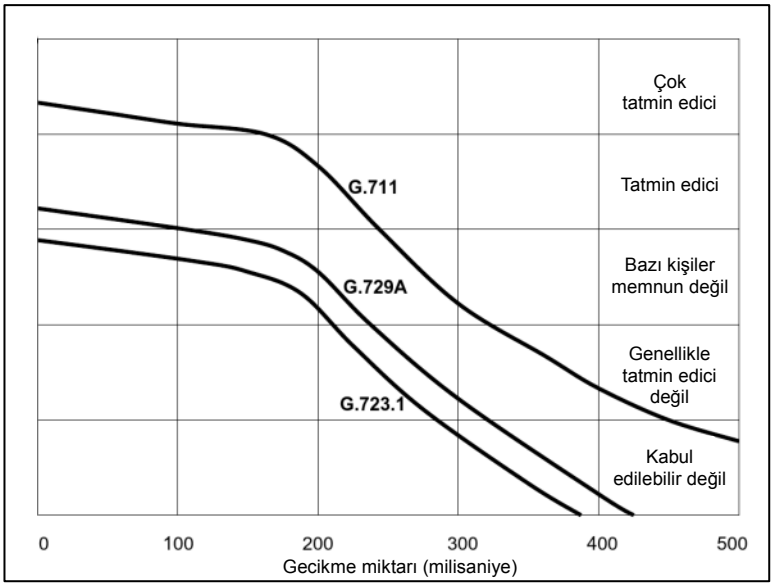
Şekil **5.23**'te verilmiş olan grafiklere bakıldığında; "işletim sistemi", "kullanılan kodek" ve "IP sürümü" gibi ölçütlerin herhangi bir tanesini temel alıp diğerlerini yok varsayarak karşılaştırma yapmanın mümkün olmadığı görülmektedir. Herhangi bir kodek, farklı işletim sistemlerinde veya farklı protokol sürümlerinde farklı sonuçlar verebilmektedir. Benzer şekilde; IP'nin 4 veya 6 sürümü, farklı işletim sistemlerinde veya farklı kodekler ile kullanıldığında farklı sonuçlar verebilmektedir.

H.Sathu vd. tarafından yapılan çalışmanın, bu çalışma ile benzer bir sonucu da G.711 kodek kullanımında, Windows'un 3 ayrı sürümünde de IPv4'ün IPv6'ya göre

daha az seğirme değeri vermesidir. Bu çalışmada yapılan testler sonucunda da IPv4'te seğirme değerlerinin daha az olduğu görülmüştür. Bu durum, "*G.711 kodek kullanıldığında IPv4 kullanılması gerektiği*" şeklinde yorumlanmamalı, farklılıkların uygulamada hissedilmeyecek seviyelerde olduğu unutulmamalıdır.

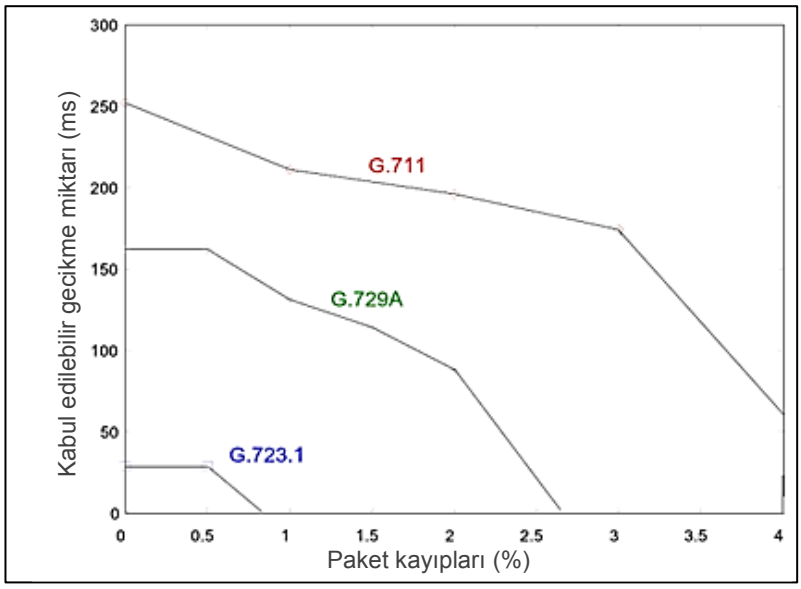
Kayıp paket miktarları açısından iki protokol arasındaki farkın, en fazla %1,3 kadar olduğu görülmüştür. UDP üzerinden yapılan VoIP uygulamasında bu kayıp paketlerin telafisi olmamaktadır. VoIP'te kayıp paket oranı arttıkça, karşı tarafa iletilen sesin kalitesi bozulmaktadır. Trafiklerdeki kayıp paket değerleri bu açıdan önemlidir.

S.Na ve S.Yoo tarafından 2002 yılında yapılmış olan çalışmada; G.711 kodek için, 250ms üzerindeki gecikmelerin insanlar tarafından problem olarak algılanmaya başlandığı belirtilmiştir. Şekil 5.24'te, ilgili çalışmada belirtilen tolerans seviyelerinin grafiği verilmiştir (Na S., vd., 2002).




**Şekil 5.24.** Gecikme miktarına bağlı memnuniyet seviyeleri (Na vd., 2002).

Şekil 5.25'te paket kayıplarının miktarına göre kabul edilebilir gecikme seviyeleri gösterilmiştir. Şekillerde problemlere tolerans açısından en dayanıklı kodek olarak G.711 görülmektedir. Bunun sebebi, kodeğin sıkıştırmasız olmasıdır.




**Şekil 5.25.** Paket kaybı miktarına bağlı kabul edilebilir gecikme değerleri (Na vd., 2002).

Bu çalışma kapsamında IPv4 ve IPv6 protokolleri ile yapılan testlerde, paket kayıplarının en fazla olduğu durum, IPv4 kullanıldığında ve yoğun arka plan trafiği olduğunda %1,6 civarında ölçülmüştür. Paket kaybı oranları açısından, IPv4 ve IPv6 arasındaki en fazla fark %1,3 civarındadır. Azami delta değerlerine bakıldığında; 129,90ms ile 132,63ms arasında olduğu, dolayısıyla kabul edilebilir seviyede olduğu görülmüştür. Bu verilerin ışığında, G.711 kodek ile VoIP uygulaması açısından IPv6 ve IPv4 protokolleri arasında kişiler tarafından hissedilir seviyede bir fark görülmeyeceği söylenebilir.

# 6. BÖLÜM: SONUÇLAR VE ÖNERİLER

IPv4 protokolü, kullanılabilir IP adresleri tükendiğinden, ömrünün sonuna gelmiştir. Artık IP'nin hangi sürümünün kullanılacağı tercihe bağlı bir durum değildir. Günümüzde üretilen hemen hemen tüm donanımlar, yazılımlar, işletim sistemleri IPv6 desteklemektedir. Zamanla tüm kurumsal ve kişisel uygulamaların da IPv6 üzerinde çalıştırılacak şekilde yapılandırılması gerekmektedir.

Bu çalışma kapsamında; IPv4 üzerinden yapılmakta olan VoIP uygulamalarının, IPv6'ya geçişi konusunda ne gibi farklılıklar olduğunu, IPv4 ve IPv6 protokollerinde yapılan VoIP uygulamaları sırasında performans açısından fark olup olmadığını anlamaya yönelik testler ve analizler yapılmıştır. VoIP uygulamaları, ağ üzerine fazla yük bindirmeyen ancak gerçek zamanlı aktarım gerektirdiği için çevresel değişkenlerin etkilerine karşı hassas olan uygulamalardır. VoIP uygulamalarının başarımının değerlendirilmesinde, kullanılan IP sürümünün tek başına çok etkili olmadığı görülmüştür. Kullanılan işletim sistemi, tercih edilen kodek, iletim hattının kapasitesi ve hat yoğunluğu gibi birçok değişken VoIP başarımında etkili olmaktadır. Bu değişkenlerin kontrol edilebilmesi, doğrudan VoIP kalitesini etkilemektedir. Analizler sonucunda; özellikle ağdaki trafik yükünün az olduğu durumda, kayıp paketler ve gecikme açısından IPv4 ve IPv6 arasında kayda değer bir fark olmadığı (*%1'den daha az*) görülmüştür. Bu tez kapsamında yapılan çalışma neticesinde elde edilen bulguların önceki çalışmalarla uygun olduğu gözlenmiştir.

Trafik şekillendirme yapılmayan ağlarda, iletim hattının doluluğu arttığında VoIP uygulamalarında sorunların arttığı görülmüştür. Bu nedenle, ses ve diğer verilerin aynı ağ ortamında aktarıldığı uygulamalarda, VoIP trafiğine öncelik verilmesinin önemli olduğu belirlenmiştir. Yapılan testler sırasında tercih edilmiş olan G.711 kodek, sıkıştırmasız olduğu için iletim hattını en yoğun kullanan kodeklerden birisidir. Bir ses görüşmesi, G.711 kodek ile 80Kb/s civarında bant genişliği tüketmektedir. VoIP için ihtiyaç duyulan toplam bant genişliği; aynı iletim hattı üzerinden eş zamanlı yapılacak olan sesli görüşme sayısı kadar artmaktadır. İletim kapasitesi az olan bir ağ üzerinde, eş zamanlı olarak çok sayıda sesli görüşme yapılan uygulamalarda, veri sıkıştırma özelliği

olan bir kodek tercih edilmesi faydalı olabilmektedir. Ancak sıkıştırmalı kodeklerin de ağ üzerindeki sorunlara hassasiyeti fazla olduğundan, her platform için "*doğru kodek*" farklı olabilmektedir. IPv6'nın VoIP açısından bir avantajı da NAT kullanılmamasına gerek kalmamasıdır. Bu sayede, sanal IP adreslerini gerçek IP adresine dönüştürmeye gerek kalmadan, her cihaz doğrudan kendi gerçek IP adresleri ile haberleşebilmektedir. Bu özellik, VoIP uygulamalarında da fayda sağlamaktadır. NAT yapılmadığında; IP adres dönüşümleri için harcanan zaman ve IP dönüşümü için kullanılan aracı sistemlere gerek kalmaması açısından yararlı olmaktadır.

**Öneriler**

IPv6'ya geçiş süreci boyunca, iki protokolün karşılaştırılması konusunda araştırıcılar ve uygulayıcılar için daima yapılabilecek çalışmalar olacaktır. Bu çalışmada sadece VoIP açısından testler yapılmıştır. IPv4'te çalıştırılmakta olan diğer uygulamalar da IPv6 açısından incelenebilir. Çok sayıda yönlendirici üzerinden aktarılan trafiklerde bu çalışmadakine benzer testler yapılarak sonuçlar karşılaştırılabilir. Farklı kodekler, farklı işletim sistemleri gibi değişik şartlarda testler yapılabilir. Ağ üzerinden gerçek zamanlı ses taşıma konusunda önemli konulardan birisi olan "trafik şekillendirme" üzerine de çalışmalar yapılabilir. Farklı algoritmalarla veya farklı sistemlerle yapılan trafik şekillendirme uygulamalarının VoIP açısından başarımının karşılaştırılması ya da yeni algoritmalar geliştirilmesi mümkündür.

# KAYNAKLAR


Balen, J., Martinovic, G., Hocenski, Z., "Network Performance Evaluation Of Latest Windows Operating Systems", **The 20th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2012)**, 2012.

Can, E., "IPv6 Üzerinden Ses Uygulaması ve Paket Analizi", Yüksek Lisans, ***Beykent Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 2006.

Davies, J., "Understanding IPv6", ***Microsoft Press***, ABD, 2008.

Deering, S., Hinden, R., "Internet Protocol, Version 6 (IPv6) Specification", ***IETF RFC*** 2460, 1998.

Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., Carney, M., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", ***IETF RFC 3315***, 2003.

Droms, R., "Dynamic Host Configuration Protocol", ***IETF RFC 1531***, 1993.

Droms, R., "Dynamic Host Configuration Protocol", ***IETF RFC 2131***, 1997.

Geesey, D., "Guide for Federal Agencies Transitioning to IPv6", ***Juniper Networks***, 2006.

Gilligan, R., Nordmark E., "Transition Mechanisms for IPv6 Hosts and Routers", ***IETF RFC 2893***, 2000.

"Google IPv6 Statistics", http://www.google.com/intl/en/ipv6/statistics/, 2011.

"Guidelines for 64-bit Global Identifier (EUI-64™)", ***IEEE***, 2003.

Haki, E.H., "İnternet Protokolü Üzerinden Ses İletiminde Hizmet Kalitesinin Analizi", Yüksek Lisans, ***Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 2007.

Handley, M., Jacobson, V., Perkins, C., "SDP: Session Description Protocol", ***IETF RFC 4566***, 2006.

Hinden, R., Deering, S., "IP Version 6 Addressing Architecture", ***IETF RFC 4291***, 2006.

Holdrege, M., Srisuresh, P., "Protocol Complications with the IP Network Address Translator", ***IETF RFC 3027***, 2001.

IANA, "IPv4 Address Space Registry", http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml, 2012.

IBM, Kurumsal Web Sitesi, http://www.ibm.com/ibm/tr/tr, 2011.

"Internet Protocol - Darpa Internet Program Protocol Specification", ***IETF RFC 791***, 1981.

ISC, "Internet Host Count History", http://www.isc.org/solutions/survey/history, Haziran 2011.

ITU, "Pulse Code Modulation (PCM) Of Voice Frequencies – ITU-T Recommendation G.711", 1972.

ITU, "One-way transmission time – ITU-T Recommendation G.114", 2003.

Johnson, D., Perkins C., Arkko, J., "Mobility Support in IPv6", ***IETF RFC 3775***, 2004.

Johnston, A.B., "Understanding the Session Initiation Protocol Second Edition", ***Artech House***, Boston (Londra), 2004.

"Kamu Kurumları için IPv6'ya Geçiş Planı", ***Resmi Gazete (Sayı: 27779)***, 2010.

Lawrence, E.H., "The Second Internet", ***InfoWeapons***, Filipinler, 2010.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G., Wolff, S., "A Brief History of the Internet", ***ACM SIGCOMM Computer Communication Review,*** *39(5):22-31*, 2009.

Loshin, P., "IPv6: Theory, Protocol, and Practice", ***Morgan Kaufmann Publishers***, San Francisco (ABD), 2004.

Manousos, M., Apostolacos, S., Grammatikakis, I., Kagklis, D., Sykas, E., "Voice-Quality Monitoring and Control for VoIP", **IEEE**, 2005.

Mockapetris, P., "Domain Names - Concepts and Facilities", ***IETF RFC 1034***, 1987a.

Mockapetris, P., "Domain Names - Implementation and Specification", ***IETF RFC 1035***, 1987b.

Mustell E.J., "Internet Protocol Version 6 the Next Generation", Yüksek Lisans, ***Marquette University Department of Mathematics, Statistics and Computer Science***, Milwaukee (Wisconsin), 2009.

Na S., Yoo S., "Allowable Propagation Delay for VoIP Calls of Acceptable Quality", "**Advanced Internet Services and Applications, First International Workshop, AISA 2002, Seoul, Korea, August 1-2",** 2002.

Narayan, S., Shi, Y., "TCP/UDP Network Performance Analysis of Windows Operating Systems with IPv4 and IPv6", **2nd International Conference on Signal Processing Systems (ICSPS)**, V2:219-222, 2010.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, "SIP: Session Initiation Protocol", ***IETF RFC 3261***, 2002.

Sağıroğlu Ş., Bektaş, O., Soysal, M., "Güvenlik Penceresinden IPv4/IPv6 Karşılaştırılması", ***3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı (ISCTurkey)***, Ankara, 2008.

Sathu, H., Shah, M.A., "Performance Comparison of VoIP Codecs on Multiple Operating Systems using IPv4 and IPv6", **International Journal of e-Education, e-Business, e-Management and e-Learning**, 2012.

Schulzrinne, H., casner, S., Frederick, R., Jacobson, V., "RTP: A Transport Protocol for Real-Time Applications", ***IETF RFC 1889***, 1996.

Schulzrinne, H., casner, S., Frederick, R., Jacobson, V., "RTP: A Transport Protocol for Real-Time Applications", ***IETF RFC 3550***, 2003.

Schulzrinne, H., Rosenberg, J., "A Comparison of SIP and H.323 for Internet Telephony", ***Proceedings of the 8th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 98)***, Cambridge, UK, 1998.

Silvestre, B.A., Silva, C.A.F., "IPv6 Deployment in Wireless Networks", **Instituto Politecnico de Leiria**, 2011.

Şahin M., "IPv6 Sistem Geçişi", Yüksek Lisans, ***İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 2006.

Thomson, S., Narten, T., "IPv6 Stateless Address Autoconfiguration", ***IETF RFC 2462***, 1998.

"Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi", http://www.ipv6.net.tr/, 2012.

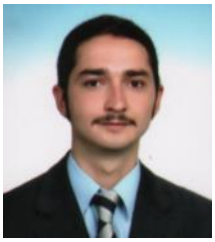
Wikipedia, "IPv4 address exhaustion" http://en.wikipedia.org/wiki/IPv4_address_exhaustion, 2011.

Yadav A., Abad P., Shah H., Kaul A., "IPv6 protocol adoption in the U.S.: Why is it so slow?", **University of Colorado**, 2012.

Yasinovskyy R., Wijesinha A.L., Karne R.K., Khaksari G., "A Comparison of VoIP Performance on IPv6 and IPv4 Networks", **IEEE 978-1-4244-3806-8/09**, 2009.

Yasinovskyy R., Wijesinha A.L., Karne R.K., "VoIP Call Performance over IPv6 during HTTP and Bittorrent Downloads", **ISCA PDCCS**, 2009.

# ÖZGEÇMİŞ



**Kişisel Bilgiler**

Adı Soyadı : Murat ÖZALP
Doğum Yeri ve Tarihi : Kahramanmaraş, 01.04.1979

**Eğitim Durumu**

Lisans Öğrenimi : Sakarya Üniversitesi, Teknik Eğitim Fakültesi, Elektronik ve Bilgisayar Öğretmenliği (2005)
Bildiği Yabancı Diller : İngilizce
Bilimsel Faaliyetleri :

**İş Deneyimi**

Stajlar : Türkiye Vagon Fabrikası A.Ş (Sakarya)
Sakarya Endüstri Meslek Lisesi (öğretmenlik stajı)
Projeler :
Çalıştığı Kurumlar : 1) Sakarya Üniversitesi, Bilgi İşlem Dairesi Başkanlığı (1997-2008)
2) Bilecik Şeyh Edebali Üniversitesi, Bilgi İşlem Daire Başkanlığı (2008-)

**İletişim**

Adres : Bilecik Şeyh Edebali Üniversitesi, Bilgi İşlem Daire Başkanlığı Gülümbe Kampüsü, BİLECİK
Tel: : 0228.2141111
E-Posta Adresi : murat.ozalp@bilecik.edu.tr

**Tarih: / /**

**İmza**

**Renkli Çıktı**

- Sayfa 43 - **Şekil 2.16.** Bölgesel internet kayıtçılarının elindeki /8 IPv4 adreslerinin miktarı
- Sayfa 45 - **Şekil 3.1.** Uluslararası TDM ve VoIP telefon görüşme süreleri
- Sayfa 76 - **Şekil 5.1.** Bu çalışmada kullanılan laboratuvarın fotoğrafı.
- Sayfa 74 - **Şekil 4.18.** Narayan S., vd., tarafından 2010 yılında yayınlanan test verileri
-