T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK-BİLGİSAYAR ANABİLİM DALI
BİLGİSAYAR AĞLARI VE İNTERNET TEKNOLOJİLERİ BİLİM DALI

IPv6 ÜZERİNDEN SES UYGULAMASI VE PAKET ANALİZİ

(Yüksek Lisans Tezi)

Hazırlayan:
Ender CAN

İSTANBUL, 2006

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK-BİLGİSAYAR ANABİLİM DALI
BİLGİSAYAR AĞLARI VE İNTERNET TEKNOLOJİLERİ BİLİM DALI

IPv6 ÜZERİNDEN SES UYGULAMASI VE PAKET ANALİZİ

(Yüksek Lisans Tezi)

Hazırlayan:
Ender CAN
Öğrenci No:
BA2351-001

Danışman:
Yrd. Doç. Dr. Rifat ÇÖLKESEN

İSTANBUL, 2006

IPv6 ÜZERİNDEN SES UYGULAMASI VE PAKET ANALİZİ

Tezi Hazırlayan: Ender CAN

Özet

Bilgisayar ağları ve ağ bileşenlerindeki teknolojik yenilikler son yıllarda noktalar arası veri haberleşme hızları ile paralel bir gelişim süreci içerisine girmesiyle birlikte bu gelişmelere paralel olarak mevcut ağ altyapıları üzerine eklenen yeni teknolojiler, geliştirilen yeni protokoller ve teknikler ile birlikte bilgisayar ağları sadece bilgisayarlar için veri haberleşmesi alanında değil, başka alanlarda da hizmet vermeye başlamışlardır.

Bunlardan en etkileyici olanı ise VoIP ”Voice Over Internet Protocol” olarak karşımıza çıkmaktadır. Aslında VoIP genel olarak mevcut telefon şebekesi ağ mimarisi üzerinde yapılan geliştirme çalışmaları sonucunda ortaya çıkan bir teknolojidir. Önceki zamanlarda anahtar devreli telefon sistemleri üzerinde telefondan telefona ses haberleşmesi sağlanırken günümüzde artık paket devreli sistemler üzerine geçerek tamamen ayrı değerlendirilmesi gereken IP tabanlı altyapılara dönmeye başlanmıştır.

Telefon şebekelerinde kullanılan SS7 sinyalleşmesi ağ yapısı, IP tabanlı ağlar olarak çok daha düşük maliyetli sistemlere dönüşmüş ve bunlar üzerinden ses aktarımı gerçekleşmiştir. Bu değişim süreci kullanıcılara analog hatlardan digital hatlara geçiş olarak yansımış ve gerek ses kalitesi olsun gerek bağlantı süreleri olsun pek çok gelişmeyi beraberindegetirmiştir.

IP ağlarının ses, görüntü ve verileri eşzamanlı olarak aktarmak için tüm bant genişliğini kullanması, Ses trafiği ses paketlerine yüksek öncelik tanıyan kalite denetimli bir IP omurgası üzerinden gönderilebilir olması, Geleneksel ve Yeni Dünya veri hizmetleri aynı altyapı üzerinden verilebilmesi, paket modu ses ve verinin düşük maliyetle aktarılmasını sağlamak için ağ kapasitesi kullanımınının en iyi duruma getirebilir olması ile birlikte bu teknolojik avantajlar, VoIP'nin IP'den bu yana oluşturulan en dikkat çekici iletişim fırsatı olarak karşımıza çıkmasını sağlıyor.

Uluslararası Telekom Birliği (ITU) Gelişme Raporları ve Endüstri araştırmalarından derlenen raporlara gore, Emarketer araştırma firmasının bize sağladığı verilere dayanarak 2005 yılı sonu itibariyle tüm dünyada internet kullanıcı sayısının 1 Milyar'a ulaştığını ve bu kullanım oranının ¼ ünün yani 250 Milyon'unu ev kullanıcısının oluşturduğunu öğrenmekteyiz. [EMarketer,Mayıs 2006]

Yine aynı şekilde şu an da sıklıkla kullanımda olan IPv4 adreslerinin kullanılabilecek olan sayısının (4,3 Milyar) 3/2 sinden fazlasının halen kullanımda olduğunu düşünecek olursak aynı andan kullanılabilecek IP sayısının trilyonları bulacağını bildiğimiz IPv6 ya geçişin önemi artmaktadır. Yaklaşık 20 yıllık bir süreçte birlikte çalıştırılması düşünülen bu iki protokolün IPv4-IPv6 birlikteliğinden sonraki süreç için ciddi yatırımlar,düzenlemeler yapılmaktadır.

Günümüzün bu iki güncel teknolojisinin yapılan bu çalışma ile birlikte, eski nesil IP teknolojisi ile çalıştırılması,gözlemlenmesi, incelenmesi ile birlikte yeni nesil IP teknolojisi olan IPv6 ile entegrasyonu ve paket yapısının incelenmesine çalışılmıştır.

Anahtar Sözcükler: VoIP, IPv6, IPv4, H.323, H.225, SIP, RTP, SDP, RTCP..

VOICE OVER IPv6 APPLICATION AND PACKET ANALYSIS

Ender CAN

Abstract

Technological innovation on computer network and net components field has entered a parallel advancement process with the data transfer between points.
However, as the parallel of the advancements; new technologies has edited to the present network system and by the developing new protocols and techniques, computer networks have started to serve not only data communication for computer field but also another fields.

The most impressive of them is VoIP "voice over internet protocol", which is a technology has emerged from the result of development process on current telephone network architecture. At earlier times of voice transfer technology development, the voice were transferred between telephone endpoints, by key circuit telephone system. Now, voice transfer is based on IP based substructere that depend on pocked circuit system.

SS7 signal network structure as IP floored network convert into low costs and voice transfer started to be based on SS7.. This transformation process users and as result, they started to pass from analogue lines to digital lines and it brought voice quality and long connection duration.

As a result of development and innovations on telekom technology, VoIP as started to enter our lives by the squeezing protocols and equipments which are developed for network. Since Ip networks are able to use bandwidth for transferring voice, image and data,synchronously, since Voice traffic can be sent on IP structures, which gives high priority to the voice package and since old and new generation data services can be given at the same substructure package mode may bring the most suitable point in order to transfer voice and data at the lowest cost.

According to the report that has gathered from national telecom association development reports and industrial researches and according to the data has been provided by

E market research firm: at the end of the 2005 the number of the internet users on the all over the world reached 1 billion, 25 % of it , 250 million of them are home users. (E market, May 2005)

IPv4 can provide 4,3 billion addresses and currently and 2/3 of it is already being used. Since we know that IPv6 can provide us more than billion, passing to IPv6 has become an obligation.For aproximately 20 years, both IPv4 and IPv6 will be used to together, therefore, during that period and especially at the end ot this period, period serious investments and regulations must be carried out.

In this thesis, working of two contemporary techniques with old generation IP network technology and integration these old techniques to the new IPv6 technologies are observed and examined and predictions are made about future processes.

Keywords: VoIP, IPv6, IPv4, H.323, H.225, SIP, RTP, SDP, RTCP..

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

KISALTMALAR

ACF: ADMISSION CONFIRM
Giriş Onay Mesajı

ARQ: ADMISSION REQUEST
Giriş Kabul İsteği

ARP: ADRESS RESOLUTION PROTOCOL
Adres Çözümleme Protokolü

ATM: ASYNCHRONOUS TRANSFER MODE
Asenkron Transfer Modu

CELP: CODE EXCITED LINEAR PREDICTION
Kod Çıkışlı Doğrusal Tahmin

CODEC: CODING DECODING
Kodlama – Çözme

CSRC: CONTRIBUTING SOURCE IDENTIFIER
Ek Kaynak Tanımlayıcısı

DSP: DIGITAL SIGNAL PROCESSING
Sayısal İşaret İşleme

FTP: FILE TRANSFER PROTOCOL
Dosya Transfer Protokolü

GK: GATEKEEPER
Ağ Kapı Sorumlusu

GW: GATEWAY
Ağ Geçidi

HTML: HYPER TEXT MARKUP LANGUAGE
Hiper Metin Oluşturma Dili

HTTP: HYPER TEXT TRANSFER PROTOCOL
Hiper Metin Transfer Protokolü

ICMP: INTERNET CONTROL MESSAGING PROTOCOL
İinternet Kontrol Mesaj Protokolü

IETF: INTERNET ENGINEERING TASK FORCE
İnternet Mühendisliği Geliştirme Birliği

IKE: INTERNET KEY EXCHANGE
İnternet Anahtar Değişimi

IN: INTELLIGENT NETWORK
Akıllı Ağ

IP: INTERNET PROTOCOL
İnternet Protokolü

IPng INTERNET PROTOCOL NEXT GENERATION
İnternet Protokol Gelecek Nesil

ISDN: INTEGRATED SERVICES DIGITAL NETWORK
Tümleşik Servisler Sayısal Ağı

ISO: INTERNATIONAL STANDARDS ORGANIZATION
Uluslar Arası Standartlar Organizasyonu

ITU: INTERNATIONAL TELECOMMUNICATIONS UNION
Uluslar Arası Telekomünikasyon Birliği

IPSec: INTERNET PROTOCOL SECURITY
İnternet Protokol Guvenlik

JPEG: JOINT PICTURE EXPERTS GROUP
Birleşik Resim Uzmanları Grubu

LAN: LOCAL AREA NETWORK
Yerel Alan Ağı

LEC: LOCAL EXCHANGE CARRIER
Yerel Santral Taşıyıcısı

MCU: MULTI POINT CONTROL UNIT
Çoklu Nokta Kontrol Birimi

MGC: MEDIA GATEWAY CONTROLLER
Medya Geçidi Kontrolorü

MGCP: MEDIA GATEWAY CONTROL PROTOCOL
Medya Ağ Geçidi Kontrol Protokolü

ND: NEIGHBOR DISCOVERY
Komşu Saptama

PCM: PULSE CODE MODULATION
Darbe Kodlu Modülasyon

PSTN: PUBLIC SWITCHED TELEPHONY NETWORK
Kamusal Anahtarlamalı Telefon Ağı

QoS: QUALITY OF SERVICE
Servis Kalitesi

RAS: REMOTE ACCESS SERVER
Uzak Erişim Sunucusu

RCF: REQUEST CONFIRM
İstek Kabul Edildi

RRJ: REQUEST REJECT
İstek Red Edildi

RRQ: REQUEST TO REGISTER
Kaydolma İsteği

RTP: REAL TIME TRANSPORT PROTOCOL
Gerçek Zamanlı Taşıma protokolü

RSVP: RESOURCE RESERVATION PROTOCOL
Kaynak Ayırma Protokolü

RTCP: REAL TIME CONTROL PROTOCOL
Gerçek Zamanlı Kontrol Protokolü

SAP: SESSION ANNOUNCEMENT PROTOCOL
Oturum Duyuru Protokolü

SDH: SYNCHRONOUS DIGITAL HIERARCHY
Senkron Sayısal Hiyerarşi

SDP: SESSION DESCRIPTION PROTOCOL

Oturum Açıklama Protokolü

SIP: SESSION INITIATION PROTOCOL

Oturum Başlatma Protokolü

SMTP: SIMPLE MAIL TRANFER PROTOCOL

Basit Posta Transfer Protokolü

SNMP: SIMPLE NETWORK MANAGEMENT PROTOCOL

Basit Ağ Yönetim Protokolü

SSRC: SYNCHRONIZATION SOURCE IDENTIFIER

Senkronize Kaynak Tanımlayıcısı

SS7: SIGNALLING SYSTEM 7

İşaretleşme Sistemi Numara 7

TCP: TRANSMISSION KONTROL PROTOCOL

İletim Kontrol Protokolü

TCS: TERMINAL CAPABILITY SET

Terminal Yeteneği Ayarlama

UA: USER AGENT

Kullanıcı Ajanı

UAC: USER AGENT CLIENT

Kullanıcı Tarafı Kullanıcı Ajanı

UAS: USER AGENT SERVER

Sunucu Tarafı Kullanıcı Ajanı

UDP: USER DATAGRAM PROTOCOL

Kullanıcı Datagram Protokolü

URL: UNIFORM RESOURCE LOCATOR

Düzenli Kaynak Bulucusu

VoIP: VOICE OVER INTERNET PROTOCOL

IP Üzerinden Ses Aktarım Protokolü

WAN: WIDE AREA NETWORK

Geniş Alan Ağı

İÇİNDEKİLER

BÖLÜM I. GİRİŞ VE AMAÇ

I.1. GİRİŞ

Son yıllarda Internet'in büyümesi ve internet kullanımında görülen belirgin artışla birlikte, haberleşmenin çeşitliliği ve kişiselleşmesine ilaveten, sesten veri haberleşmesine ve sabit hattan mobil haberleşmeye kadar gelişen talep yapısı içinde de önemli değişiklikler söz konusu olmuştur. Daha da ötesi, veri iletiminde dar banttan genişbant haberleşmesine geçiş, endüstrinin dönüşümünü hızlandırmıştır. Söz konusu gelişmeler çerçevesinde haberleşmenin kişiler arası, kişiler ve cihazlar arası, hatta cihazlar arası genişlemesi telekomünikasyon pazarının büyümesine tanıklığı beraberinde getirmiştir. Günümüzde mobil telefon haberleşmesinde uluslararası dolaşım (roaming) hemen hemen tamamen sağlanmıştır. Ancak İnternet erişiminde bunu sağlamak, IP adreslerinin ağa bağımlı olması nedeniyle o kadar kolay olmamaktadır.

Günümüzde, IP uygulamalarının artan oranda kullanılması, kullanıcı sayısındaki artış, İnternetteki hızlı büyüme, adres sıkıntısını gündeme getirmekte ve tüm dünyada gelecek yıllarda IP adreslerinin tükeneceği korkusuna yol açmaktadır. Mevcut Internet Protokolünün adres kıtlığı sorununu çözmek için, birçok İnternet kullanıcısı Internete giriş/çıkışta Ağ Adres Değişimine (NAT) veya herkese ait özel adres kumbarası ile yetinmeye zorlanmıştır. Bu yöntemde, özel IP adresleri tanımlanmış ve özel ağlara tahsis edilmeye başlanmıştır. Ancak bu adresler sadece yerel ağda geçerli olup Internette tanınmamaktadır. Ağ Adres Değişimi (NAT) kullanılarak, özel ağa bir veya birkaç Internet adresi atanmakta ve özel ağdaki tüm bilgisayarlar bu adresler ile İnternete ulaşmaktadır.

Örneğin ses ve görüntü dağıtan uygulamalar, düzenli aralıklarla verinin dağıtılmasına gereksinim duymaktadır.

Tez'e yönelik yapılan tüm bu çalışmalarda, şu an için IPv4 altyapısı üzerinden gerçeklenen VoIP uygulamalarının IPv6 alt yapısı oluşturulmuş ağlar üzerinden uygulaması

için mevcut yöntemler araştırılmış ve bunlar test ortamında uygulanabilirliği görülmeye çalışılmıştır.

Yine yapılan bu tez çalışmasında çözüme yönelik bir yaklaşım olarak; İnternet ve Web'in büyümesindeki önemin dikkate alınmasıyla, yine aynı şekilde mevcut geleneneksel ses sistemlerinden IP tabanlı ağlar üzerinden taşınan ses teknolojisine hızla geçişin sağlandığı günümüzde, IPv6 ile VoIP teknolojilerine yapılacak hızlı desteğin İnternetin gelecekteki performansında kesin bir farklılık yaratacağı varsayımına dayanılarak, Mobil IP'yi destekleme gerekliliğine işaret edilmekte ve IPv4'ten IPv6 adresleme sistemlerine geçişin, özellikle gelişmekte olan ülkelerde İnternetin geniş çaplı genişlemesini kolaylaştıracağı öngörüsü yapılmaktadır.

I.2. AMAÇ

Bu tezde amaçlanan temel olarak IPv6 ve VoIP teknolojileri hakkında genel bir bilgi verdikten sonra IPv4'ten IPv6'ya geçişin hızlandığı bu dönemde yine aynı şekilde geleneksel ses şebekesinden (PSTN) yeni nesil şebekeye geçişin aynı platformda buluşturulmaya çalışılması ve IPv6 üzerinden ses uygulaması için bazı ön çalışmalar yapmak. Yine aynı zamanda VoIP'in olumlu ve olumsuz yanları, VoIP sisteminin işleyişi, ses sıkıştırma teknikleri, servis kalitesini etkileyen unsurlar ve sesin gerçek zamanlı olarak taşınabilmesi için geliştirilmiş olan şebeke elemanları tanıtılmak amaçlanmaktadır.

Yine aynı şekilde IP üzerinden ses aktarım'a ilişkin protokol tanımlamaları ve bu protokollerin karşılaştırmaları yapılması amaçlanmıştır.

BÖLÜM II. GENEL BÖLÜM

II.1 GENEL BILGILER

II.1.1 Internet Protokol Sürüm 6 Genel Tanıtımı

Internet Protokol sürüm 6, RFC 791'in IPv4'ü tanımlaması ve 1981 yılında yayınlanmasından sonra geçen bu süre zarfında internet'in büyümesiyle birlikte oluşan eksiklik ve gereklilik için RFC 2460 ile tanımlanmış ve yayınlanmıştır.

IPv6 da paket yapısı IPv4'e göre değiştirilmiştir. IPv4'de başlık paketi yapısında kullanılan bazı bölgeler IPv6'da bulunmamaktadır. IP paketi temel-başlık yapısında sadeleşme göze çarpmakla birlikte, IPv6'nın esas getirileri başlık paketinin arkasına zincir gibi bağlanmak sureti ile eklenebilen ek-başlık yapısı incelendiğinde görülmektedir.[1]

II.1.1.1. Neden IPv6

Internet Protokol Sürüm 4'den, Internet Protokol Sürüm 6'ya geçişi zorunlu kılan nedenlerden bazıları aşağıda verilmiştir.

- Internet'in gitgide büyümesi ve IPv4 adres alanlarının tükenmesi.
- Ağlarda basit yapılandırma ihtiyacı
- IP düzeyinde güvenlik mekanizmalarındaki eksiklik ile daha fazla güvenlik ihtiyacı
- IPv4 adreslerinin azalması ile birlikte yaygınlaşan NAT teknolojisinin oluşturduğunu sıkıntılar.
- IPv4 te bulunan QOS desteğinin tam anlamıyla randıman veremediği bu durumun iyileştirmeye gereksinim duyması.
- Elle , manuel olarak set edilen veya DHCP kullanılarak dağıtılan IPv4 adreslemenin daha basit ve daha otomatik yapılandırılması ihtiyacı
- Bu nedenlere çözüm bulmak üzere tanımlanan Internet Protokol Sürüm 6 (IPv6) özellikle üst ve alt katman iletişim kurallarına en az etki edecek şekilde tasarlanmıştır.

IPv6 iletişim kuralının özellikleri şunlardır[2]:

- **Yeni üstbilgi biçimi**

IPv6 üstbilgisi, üstbilgisi genel giderini en aza indirecek şekilde tasarlanmış yeni bir biçime sahiptir. Bu, zorunlu olmayan alanları ve seçenek alanlarını IPv6 üstbilgisinin sonrasına yerleştirilen uzantı üstbilgilerine taşıyarak elde edilmiştir. Gelişmiş IPv6 üstbilgisi ara yönlendiricilerde daha verimli işlemeye olanak tanır.

- **Büyük adres alanı**

IPv6, 128 bitlik (16 baytlık) kaynak ve hedef adreslere sahiptir.
Kullanılabilir adres sayısının çok daha büyük olması nedeniyle, NAT'ların dağıtımı gibi adres koruma tekniklerine artık gerek yoktur.

- **Etkili, hiyerarşik adresleme ve yönlendirme alt yapısı.**

Internet'in IPv6 bölümünde kullanılan IPv6 genel adresleri, yaygın çok düzeyli Internet hizmet sağlayıcılarına yönelik verimli, hiyerarşik ve özetlenebilir bir yönlendirme alt yapısı oluşturmak üzere tasarlanmıştır. IPv6 Internet'inde omurga yönlendiricileri çok daha küçük yönlendirme tablolarına sahiptir.

- **Durum bilgisi olan ve olmayan adres yapılandırması**

Ana makine yapılandırmasını basitleştirmek için, IPv6 hem bir DHCP sunucusu eşliğinde adres yapılandırması gibi durum bilgisi olan adres yapılandırmasını, hem de durum bilgisi olmayan (DHCP sunucusu bulunmayan) adres yapılandırmasını desteklemektedir. Durum bilgisi olmayan adres yapılandırmasında, bir bağlantıdaki ana makineler kendilerini otomatik olarak, bağlantının IPv6 adresleriyle ve yerel yönlendiriciler tarafından bildirilen öneklerden türetilen adreslerle yapılandırır. Yönlendirici olmadığında da, aynı bağlantı üzerindeki ana makineler, kendilerini otomatik olarak bağlantı yerel adreslerle yapılandırıp el ile yapılandırma olmadan iletişim kurabilirler.

- **Yerleşik güvenlik**

  IPSec desteği bir IPv6 iletişim kuralı takımında bir gerekliliktir. Bu gereklilik, ağ güvenliği gerekleri için standartlara dayalı bir çözüm sunar ve farklı IPv6 uygulamaları arasında ortak çalışabilirliği destekler.

- **Hizmet kalitesi (QoS) için daha iyi destek**

IPv6 üstbilgisindeki yeni alanlar trafiğin nasıl işlendiğini ve ayırt edildiğini tanımlar. IPv6 üstbilgisinde Akış Etiketi alanını kullanarak trafik tanımlaması yönlendiricilere, bir akışa ait paketleri tanıma ve özel olarak işleme olanağı tanır. Akış, hedef ve kaynak arasındaki bir paketler dizisidir. Trafik IPv6 üstbilgisinde tanımlandığından, QoS desteği, paket yükü IPSec ile şifrelenmiş olsa bile kolayca elde edilebilir.

- **Komşu düğüm etkileşimi için yeni iletişim kuralı**

IPv6 için komşu saptama iletişim kuralı, komşu düğümlerin (aynı bağlantı üzerindeki düğümlerin) etkileşimini yöneten bir dizi IPv6 için Internet Denetim İletisi İletişim Kuralı (ICMPv6) iletisidir. Komşu saptama, Adres Çözümleme İletişim Kuralı'nı (ARP), ICMPv4 Yönlendirici Saptamasını ve ICMPv4 yeniden yönlendirme iletisini etkili çok noktaya yayın ve tek noktaya yayın iletileriyle değiştirir ve ek işlevsellik sağlar.

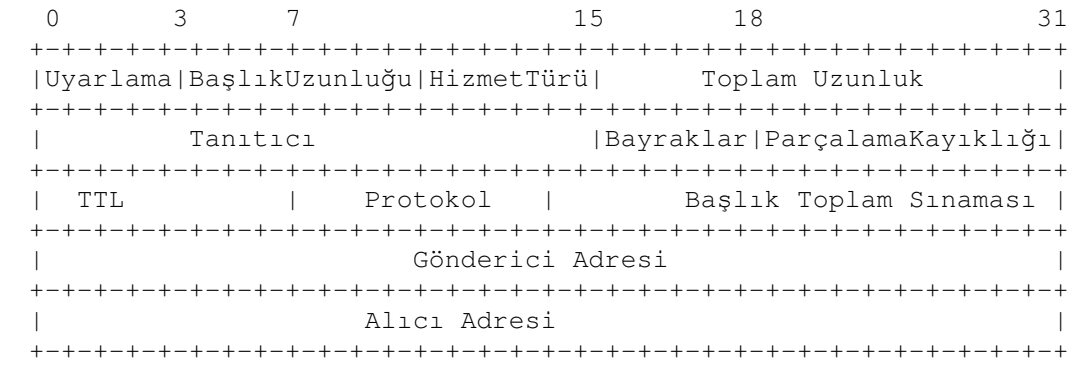
- **Genişletilebilirlik**

IPv6, IPv6 üstbilgisinin sonrasına uzantı üstbilgileri eklenerek yeni özelliklerle genişletilebilir. Yalnızca 40 baytlık seçeneği destekleyebilen IPv4 üstbilgisinden farklı olarak, IPv6 uzantı üstbilgilerinin boyutu yalnızca IPv6 paketiyle sınırlıdır.

II.1.1.2. IPv6 Başlık Yapısı

IPv6 temel/standart başlığı IPv4 başlığına kıyasla daha yalındır. IPv4 başlığında bulunan *başlık uzunluğu* alanı kaldırılmış, yerine sadece başlık dışında kalan paketin boyutunu ifade eden *Yararlı Veri Boyu* alanı bırakılmıştır. Ayrıca IPv4'deki *Bayraklar,Parçalama Kayıklığı, Başlık Toplam Sınaması, Tanıtıcı,* alanları kaldırılmıştır. Geri kalan alanlar ise değişikliğe uğrayarak IPv6 temel başlığında kullanılmıştır. IPv4'de başlık uzunluğu 20 Byte iken

IPv6'da temel başlık uzunluğu 40 Byte'a çıkarılmıştır. Fakat sadeleşmenin tersine başlık uzunluğunun artmasının nedeni IPv6'da adreslerin 128 bit olmasıdır. IPv4 başlığında adres alanlarını çıkardığımızda başlık uzunluğu 12 Byte iken bu değer IPv6 da 8 Byte olmaktadır.[3]



Şekil-0 IPv4 Başlık Yapısı

Şekil-1 IPv6 Başlık Yapısı

IPv6 başlığı içerisindeki alanlar ve fonksiyonları aşağıdaki gibidir.

Uyarlama (4 bit) : Geçerli olan internet protokolünün sürüm bilgisi bu alan ile bildirilir.

Trafik Türü (8 bit) : IPv6 paketi için belirlenecek trafik türü veya öncelik bilgisi bu alanda taşınır. IPv4 de ki Servis Türü alanına benzer bir işleve sahiptir.

Akış Etiketi (20 bit) : Paketlerin kaynak ile hedef arasındaki aktarımı esnasında belirlenen özel bir sıralamada aktarılması ve aradaki yönlendiriciler tarafından belirtilen bu özel sıralamada değerlendirilmesi için kullanılır.

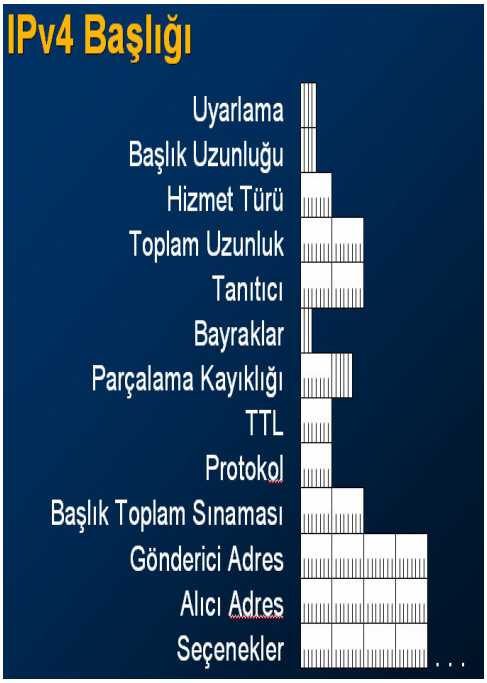
Yararlı Veri Boyu (16 bit) : IPv6 başlığının arkasındaki yararlı veri-yükünün uzunluğunu belirtir. En fazla 65535 Byte'lık veri büyüklüğünü işaret edebilir. Bu değerden büyük verilerin taşınması durumunda bu alan "0" yapılır ve düğümden-düğüme atlama başlığının seçenek alanında "Jumbo veri-yükü" özelliği işaret edilmek suretiyle temel başlığın arkasına eklenir.

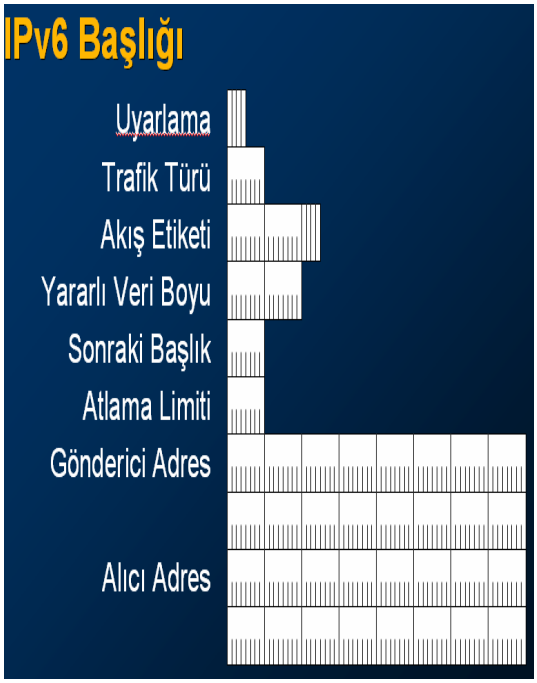
Sonraki Başlık (8 bit) : Temel başlığın arkasına eklenmek suretiyle kullanılacak olan bir sonraki başlığın tür bilgisi bu alanda taşınır.

Atlama Limiti (8 bit) : IPv6 paketinin yok edilmeden önce üzerinden geçebileceği düğüm sayısını işaret eder. IPv4 başlığındaki TTL değeri gibidir.

Gönderici Adresi (128 bit) : Paketin kaynak adresi (gönderici) bilgisi bu alanda taşınır.

Alıcı Adresi (128 bit) : Paketin ulaşması istenen hedefin adres (alıcı) bilgisi bu alanda taşınır.





Şekil-2 IPv4 Başlığı

Şekil-3 IPv6 Başlığı

IPv4 Başlık Alanları	**IPv6 ile değişen alanlar**
Uyarlama	Yeni değer olarak 6
Başlık Uzunluğu	Silindi
Hizmet Türü	Trafik Türü
Toplam Uzunluk	Yararlı Veri Boyu alanı
Tanıtıcı	Silindi
Bayraklar	Silindi
Parçalama Kayıklığı	Silindi
TTL	Atlama Limiti
Protokol	Sonraki Başlık alanı
Başlık Toplam Sınaması	Silindi
Gönderici Adres	Aynı, ama 128-bit uzunluğunda
Alıcı Adres	Aynı, ama 128-bit uzunluğunda
Seçenekler	Silindi

Tablo-1 IPv6-IPv4 Değişiklikleri

II.1.1.3. IPv6 Adresleme Türleri

IPv6 iletişim kuralının en belirgin özelliği çok daha büyük bir adres alanı kullanmasıdır. IPv6'daki adres boyutu 128 bittir; bu IPv4'teki bir adresten dört kat daha büyüktür. 32 bitlik bir adres alanı, 232 veya 4.294.967.296 olası adrese olanak tanır. 128 bitlik bir adres alanı, 2^128 veya 340.282.366.920.938.463.463.374.607.431.768.211.456 (3,4 × 1038) olası adrese olanak tanır.[2]

IPv4 adresleri noktalı ondalık biçiminde gösterilir. Bu 32 bitlik adres 8 bitlik bölümlere ayrılmıştır. Her 8 bitlik küme, ondalık eşdeğerine dönüştürülür ve noktalarla ayrılır. IPv6'da, 128 bitlik adres 16 bitlik bölümlere ayrılır ve her 16 bitlik blok 4 basamaklı onaltılık bir sayıya dönüştürülüp iki nokta üst üste işaretiyle ayrılır. Ortaya çıkan gösterim, onaltılı iki nokta üst üste işareti olarak adlandırılır.

Aşağıdaki IPv6 adresi ikili biçimindedir:

00100001110110100000000011010011000000000000000000010111100111011
00000010101010100000000011111111111111000101000100111000101101O

Bu 128 bitlik adres, aşağıda gösterildiği gibi 16 bitlik bölümlere ayrılır:

0010000111011010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010

Her 16 bitlik blok onaltılıya dönüştürülür ve iki nokta üst üste işaretleriyle ayrılır.

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

IPv6 gösterimi her bir 16 bitlik bloğun başındaki sıfırlar kaldırılarak daha da basitleştirilebilir. Bununla birlikte, her bloğun en az bir basmağı olmalıdır. Baştaki sıfırları atıldığında, adres gösterimi şu şekilde olur:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

Adresleme Yapısı:

IPv6 da üç adet adresleme yapısı mevcuttur.

Unicast : Tek bir arabirim için tanımlanmıştır. Bir veri paketi unicast adres'e gönderildiğinde adresin tanımlı olduğu arabirim bu paketi alır.

Anycast : Birkaç arabirim tanımlanması için belirlenmiştir. Genellikle uygun olan farklı bir düğüm içindir. Bir veri paketi anycast adres'e gönderildiğinde adresin tanımlı olduğu arabirim bu paketi alır.

Multicast : Birkaç arabirim için tanımlanmıştır. Bir veri paketi multicast adres'e yönlendirildiğinde bu adres'e tanımlı tüm düğümler bu paketi alır. Ipv6 da broadcast adres yoktur, bunun yerine Multicast adres tanımlaması geçmiştir. [4]

Sıfırları Sıkıştırma:

Bazı adres türleri uzun sıfır dizileri içerir. IPv6 adreslerinin gösterimini daha da basitleştirmek üzere, onaltılı iki nokta üst üste işaretleri biçimde 0 olarak belirlenen kesintisiz 16 bitlik bloklar **::** şeklinde sıkıştırılabilir. Bu çift iki nokta üst üste işareti olarak bilinir.

Örneğin FE80:0:0:0:2AA:FF:FE9A:4CA2 şeklindeki bir bağlantı yerel adresi FE80::2AA:FF:FE9A:4CA2 olarak sıkıştırılabilir. FF02:0:0:0:0:0:0:2 çok noktaya yayın adresi FF02::2 olarak sıkıştırılabilir. Sıfırları sıkıştırma, yalnızca onaltılı iki nokta üst üste işaretleri biçimde gösterilen kesintisiz bir 16 bitlik blok dizisini sıkıştırmak için kullanılabilir. Sıfırları sıkıştırma işlemi 16 bitlik bloğun bir bölümünü içerecek şekilde yapılamaz. Örneğin FF02:30:0:0:0:0:0:5 adresi FF02:3::5 şeklinde gösterilemez.

Kullanılan **::** sıkıştırma işaretinin kaç 0 biti gösterdiğini belirlemek için sıkıştırılan adresteki blok sayısını sayıp bu sayıyı 8 sayısından çıkartıp sonucu 16 ile çarpmanız gerekir. Örneğin FF02::2 adresinde iki blok bulunur (FF02 bloğu ve 2 bloğu). (::) işareti ile ifade edilen bit sayısı 96'dır (96 = (8 - 2) × 16).

Sıfırları sıkıştırma verili bir adreste yalnızca bir kez uygulanabilir. Aksi durumda, çift iki nokta üst üste işaretinin **(::)** her kullanımında gösterilen 0 bit sayısını belirlemeniz mümkün değildir.

IPv6 önekleri

Önek, adresin sabit değerleri olan bitleri veya ağ tanımlayıcısının bitlerini gösteren bölümüdür. IPv6 yollarının ve alt ağ tanımlayıcılarının önekleri IPv4'ün Sınıfsız Etki Alanları Arası Yönlendirme (CIDR) gösterimiyle aynı şekilde gösterilir. Bir IPv6 öneki adres/önek-uzunluk gösterimiyle yazılır. Örneğin, 21DA:D3::/48 bir yol önekidir ve 21DA:D3:0:2F3B::/64 bir alt ağ önekidir.

• IPv4 uygulamaları genellikle, alt ağ maskesi olarak bilinen ağ önekinin noktalı ondalık bir gösterimini kullanır. IPv6'da alt ağ maskesi kullanılmaz. Yalnızca önek uzunluğu gösterimi desteklenmektedir.

Yerel olarak kullanılan tek noktaya yayın adresleri

IPv6'da lokalde kullanılan tek noktaya yayın yapan adresler tanımlanabilmektedir.

Bağlantı yerel adresi

Bağlantı yerel adresleri 1111 1110 10 önekiyle gösterilirler, düğümler tarafından, aynı bağlantı üzerindeki komşu düğümlerle iletişim kurmak için kullanılır. Örneğin, yönlendiricisiz tek bağlantılı IPv6 ağında, bağlantı yerel adresleri bağlantı üzerindeki ana makineler arasında iletişim kurmak için kullanılır. Bağlantı yerel adresleri Otomatik Özel IP Adresleme (APIPA) IPv4 adreslerine eşdeğerdir (169.254.0.0/16 önekini kullanarak). Bir bağlantı yerel adresi, Komşu Saptama işlemleri için gereklidir ve tüm diğer tek noktaya yayın adresleri yokken bile daima otomatik olarak yapılandırılır.

Bağlantı yerel adresleri daima FE8X ile başlar. 64 bitlik arabirim tanımlayıcısı ile, bağlantı yerel adreslerinin öneki daima FE80::/64 şeklindedir. Bir IPv6 yönlendiricisi, bağlantı yerel trafiğini asla bağlantının ötesine iletmez.

Site yerel adresi (Link Local Address) :

Site yerel adresleri 1111 1110 11 önekiyle gösterilirler,
IPv4'de kullandığımız,

```
10.0.0.0        -   10.255.255.255  (10/8 prefix)
172.16.0.0      -   172.31.255.255  (172.16/12 prefix)
192.168.0.0     -   192.168.255.255 (192.168/16 prefix)
```

ağlarına karşılık gelir. Özel adresler olduklarından bu tür adreslere ,site yerel adreslerine başka ağlardan erişilemez. [5]

Bağlantı yerel adreslerinden farklı olarak site yerel adresleri otomatik olarak yapılandırılmaz ve durum bilgisi olmayan veya durum bilgisi olan adres yapılandırma işlemleri tarafından atanmaları gerekir.

Diğer IPv6 adres türleri:

• Belirtilmemiş-Belirsiz adres

Belirtilmemiş-Belirsiz adres 0:0:0:0:0:0:0:0 veya :: , IPv4'de "any" veya "0.0.0.0" şeklinde gösterilen adrese denk gelir..

Belirtilmemiş-Belirsiz(::) adres hiçbir zaman arabirime atanmaz veya hedef adresi olarak kullanılmaz.

Geridöngü-Geridönüş (Loopback) adresi

0:0:0:0:0:0:0:1 veya 0000:0000:0000:0000:0000:0000:0000:0001 veya ::1 şeklinde gösterilmektedir. IPv4'de 127.0.0.1 şeklinde gösterilmektedir.
Geridöngü-geridönüş(loopback) arabirimini tanımlamak ve bir düğümün kendi kendine paket göndermesini sağlamak için kullanılır.

IPv4 Uyumlu Adresler:

Bu tür adresler IPv4'den IPv6'ya geçişe yardımcı olmak ve her iki türdeki ana makinenin bir arada var olmasını kolaylaştırmak için tanımlanmıştır. Aşağıda bu adresler gösterilmiştir.

IPv4 uyumlu adres

IPv4 uyumlu adresler 0:0:0:0:0:0:w.x.y.z veya ::w.x.y.z şeklinde gösterilir. Örnek olarak ::1.2.3.4 verilebilir.
Burada 1.2.3.4 kullanılan IPv4 adresini göstermektedir.

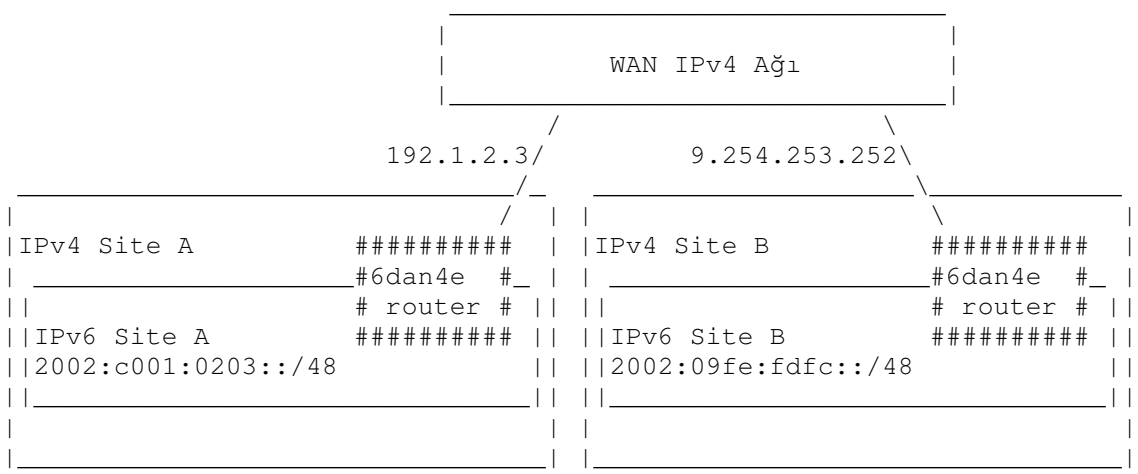
IPv4 uyumlu adres IPv6 hedefi olarak kullanıldığında, IPv6 trafiği otomatik olarak bir IPv4 üstbilgisi ile kapsüllenir ve IPv4 alt yapısı kullanılarak hedefe gönderilir.

IPv4 eşlemli adres

IPv4 eşlemli adres (0:0:0:0:0:FFFF:w.x.y.z veya ::FFFF:w.x.y.z) IPv4 adresini IPv6 adresinde göstermek için kullanılır.

6to4 adresi

6to4 adresi, hem IPv4 hem de IPv6 kullanan iki düğüm arasında Internet üzerinden iletişim kurmak için kullanılır. 6to4 adresi, 2002::/16 önekini düğümün genel IPv4 adresinin 32 bitiyle birleştirip bir 48 bitlik bir önek oluşturularak üretilir. Örneğin, 137.107.0.1 IPv4 adresi için 6to4 öneki 2002:836B:1::/48 şeklindedir.



Şekil-4 IPv6 dan IPv4 e Tünelleme [6]

Yukarıdaki topolojide 6'dan 4'e tünelleme yapıldığı görülmektedir.

Multicast Adresleri:

İlgili servisler için kullanılan multicast adresleri aşağıdaki gibi başlarlar.

3ffe:ffff:100:f101::/64 [7]

II.1.2. Internet Protokol Üzerinden Ses Aktarımı Genel Tanıtımı

Sesin paket anahtarlamalı ağlardan, internet protokolü üzerinden iletimi sesin sayısallaştırılması ve kodlanması ile başlamaktadır. Sesin sayısallaştırılması ve düşük hızlarda iletilmesi için birçok teknikler ve algoritmalar kullanılmaktadır. Yeni nesil teknolojiler ve buna paralel olarak DSP'lerdeki (Sayısal İşaret İşlemcilerindeki - Digital Signal Processor) hızlı gelişme bu tekniklerin ve algoritmaların uygulanmasında çığır açmıştır. [8]

Kodlanan sesin paket anahtarlamalı ağlardan iletilmesi için ses küçük parçalara bölünerek paketlenmektedir. Bu paketlerin başlıklarında kaynak adresi, hedef adresi ve benzeri bilgiler yer almaktadır.[9] Paketlerin iletiminde devre anahtarlamalı ağlardaki gibi bir yol kurulumu bulunmamaktadır. Paketler her bir ağ noktasında bu başlık bilgilerine göre

yönlendirilmektedir. Bu nedenle her bir ağ noktasında istatistiksel çoklama yapılmaktadır. Paket anahtarlamalı ağlardaki bu ağ noktalarındaki yoğunluk veya tıkanıklık istatistiksel çoklama nedeniyle bazı paketlerin gecikmesine veya geç ulaşmasına neden olmaktadır. Gerçek zamanlı konuşma gecikmeye duyarlı olduğundan sesin paket anahtarlamalı ağlardan istenilen sürede ve kalitede ulaşması için servis kalitesi teknikleri geliştirilmektedir.

Internet üzerinden ses aktarımının sağladığı avantajlarlar arasında; VoIP de, Sabit bağlantı bir bağlantı gerektirmez ve değişken bant genişlikleri kullanabilir. VoIP sisteminde bir kullanıcı eş zamanlı birden fazla oturum açabilir, aynı anda bir dosyayı indirirken ya da web'de sörf yaparken bir yandan da telefon konuşması yapabilir, ve yine buna benzer bir şekilde aynı telefon üzerinden birden fazla ses görüşmesi-konferans yapabilir durumda olabilecektir.

Günümüzde Internet üzerinden ses aktarımının temel sorunu; güvenilirlik, aktarılan sesin kalitesi ve paket anahtarlamalı ağlar ile devre anahtarlamalı ağlar arasında kullanılan farklı standartların birbirleriyle uyumlu çalışabilmesi gibi görünmektedir. Bu problemleri çözmek için birçok protokol standartı geliştirilmiştir. Bu protokollerden bir kısmı H.323, SIP (Oturum Başlatma Protokolü - Session Initiation Protocol) gibi kontrol ve işaretleşme ile ilgili standartları tanımlarlarken bir kısmı da RTP (Gerçek Zamanlı Taşıma Protokolü - Realtime Transport Protokol), RSVP gibi sesin kaliteli iletimini sağlamaktadır. İlerleyen bölümlerde bu protokoller incelenmeye çalışılacaktır.

II.1.2.1. Internet Protokol Üzerinden Ses Aktarımı Sisteminin İşleyişi

- Sinyal yollanmadan önce dijital formata ADC (analog to digital converter – analog'dan dijital'e dönüştürücü) ile çevrilmektedir.
- Ve bu dijital bit'lerin iletişim için iyi bir formatla sıkıştırılmış olması olması gerekmektedir.
- Bu ses paketlerini gerçek zamanlı protokol ile veri paketlerine iliştirmemiz gerekmektedir. (genellikle IP üzerinde UDP, onunda üzerinde RTP)
- DSP (Digital Signal Processing – Dijital sinyal prosesi) segmentleri ile ses sinyali frame'lere çevrilir ve belli bir gurup oluşturduklarında ses paketlerine çevrilir. Bu paketler ITU-T'nin tanımladığı H.323 protokolü ile IP üzerinden transfer edilir.

II.1.2.2. Internet Protokol Üzerinden Ses Aktarımı Protokolleri

Bu bölümde temel olarak kullanılan VoIP protokollerinden en yaygın olarak kullanılanlarından H.323 ve SIP protokollerini ayrıntılı bir biçimde incelenmeye çalışılacaktır.

II.1.2.2.1 H.323 Protokolü

H.323 ITU tarafından iki veya ikiden daha fazla uç birim arasında IP benzeri kalite servis garantisi vermeyen bir ağ üzerinde ses ya da görüntü trafiği taşımak için geliştirilmiş bir standarttır. Daha önceleri sadece yerel ağlar içerisinde konferanslar için geliştirilmiş olan H.320 standardına ses iletişimi için gerekli eklentilerin yapılması ile ortaya çıkmıştır. İlk uyarlaması 1996'da çıkan H.323 ün DRAFT halinde çıkan son uyarlaması 2006 yılında ortaya çıkmıştır. Bu süre aralığında çıkan uyarlamalar ve farklarını ilerleyen bölümlerde inceleyeceğiz.

II.1.2.2.1.1 H.323 Mimarisi Ve Temel Bileşenleri

H.323 Protokolü temel olarak aşağıdaki bileşenlerden oluşur.

II.1.2.2.1.1.1 Terminal

H.323 protokolünde , herhangi bir IP ağına bağlı uç birim ekipmanıdır. Bu bir PC olabileceği gibi, bir Video aygıtı, bir sesli yanıt sistemi, bir SoftPhone, bir Netmeeting istemcisi veya bir IP Telefonu da olabilir.

H.323 te tüm terminaller, ses ve kontrol haberleşmesi desteğini verebiliyor olması gerekir. Bunun yanında opsiyonel olarak Video ve Veri trafiği için desteğinin olması beklenir.

Kontrol haberleşmesi aşağıdaki unsurları içermektedir:

- Kanal kullanımı, düzenlenmesi ve yetenekler için, H.245
- Çağrı işaretleşmesi ve çağrı kurulumu için, Q.931
- GateKeeper ile haberleşmek ve Kayıt, İzin ve durum için, RAS
- Ses ve Video paketlerinin sıraya konması, iletilmesi için, RTP/RTCP

II.1.2.2.1.1.2 Geçityolu (Gateway)

Genel olarak PSTN ağları(Devre Anahtarlamalı) ile IP ağları arasında geçişleri sağlamak üzere çalışan modüllerdir. Gatewayler aynı zamanda, veri-ses-video formatları arasında dönüşümleri gerçekleştirerek çağrı başlatma ve kontrol işaretleşmeleri arasındaki dönüşümleri sağlar.

II.1.2.2.1.1.3 Kapı Muhafızı (Gatekeeper)

Terminaller ve gatewaylerin kayıt,kabul ve statü (RAS) takiplerinden sorumlu modüllerdir. Genel olarak bir gatekeeper'dan aşağıdaki unsurları yerine getirmesi beklenir.

- Bant Genişliği Yönetimi
- Giriş Kontrolü
- Adres Dönüşümü
- Kayıtlı kullanıcılar var ise bunlara servisler verme
- Çağrı Kontrolü
- Çağrı Yetkilendirme

II.1.2.2.1.1.4 Çoklu Nokta Kontrol Birimi (MCU)

Mevcut H.323 ağ üzerinde ikiden fazla terminal, gateway var ise böyle bir ortamda çoklu konferans yapılabilmesini sağlayan modüllerdir. MCU lar da kendi içerisinde, çoklu görüşmeler için işlevler sağlayan kontrol kanalı ve alınan verileri işleyen kontrol işlemcisinden oluşur. Bir MCU , kontrol işlemci olmadan da çalışabilir.

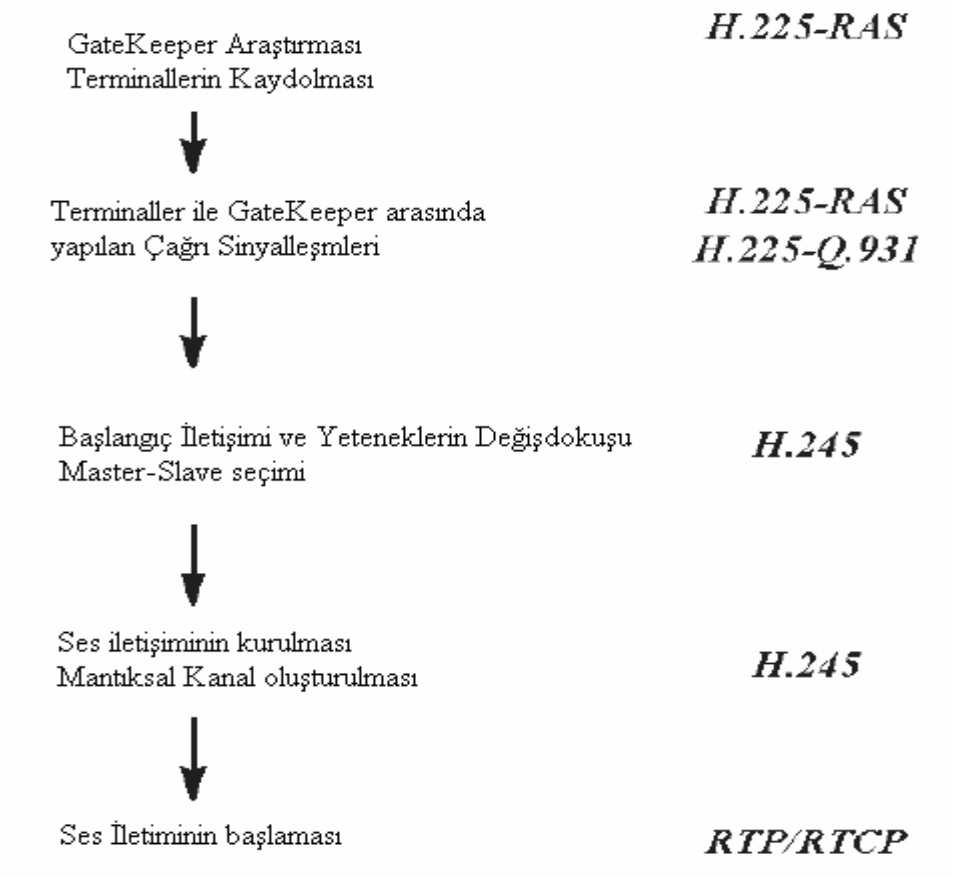
II.1.2.2.1.2 H.323 Protokolü Kümesi

H.323 protokolü aslında bir çok protokolü altında barındıran bir şemsiye görevi gören bir standarttır.

H.323 Protokol kümesi genel olarak aşağıdaki bileşenlerden oluşur.

<table>
<tr><td colspan="2">Ses / Görüntü</td><td colspan="2">Terminal Kontrol ve Yönetimi</td><td colspan="3">Veri</td></tr>
<tr><td>G.7XX</td><td>H.26X</td><td rowspan="2">RTCP</td><td rowspan="2">Terminallerden Gatekeeper 'a İşaretleşme RAS</td><td>H.225.0 Çağrı İşaretleşmesi</td><td rowspan="2">H.245</td><td>T.125</td></tr>
<tr><td colspan="2">RTP</td><td rowspan="2">Güvenilir Taşıma (TCP)</td><td>T.124</td></tr>
<tr><td colspan="3">Güvenilmeyen Taşıma (UDP)</td><td>T.123</td></tr>
<tr><td colspan="6">Ağ Katmanı (IP)</td></tr>
<tr><td colspan="6">Veri Bağı Katmanı</td></tr>
<tr><td colspan="6">Fiziksel Katman</td></tr>
</table>

Şekil-5 H.323 Protokol Kümesi



Şekil-6 H.323 Çalışması & Protokol İlişkisi

II.1.2.2.1.3 Kodekler

Ses işleme uygulamalarında bu iş için özelleşmiş DSP (Sayısal İşaret İşleyiciler) kullanılır. DSP'lerin yerine getirdikleri en önemli görev ise; analog telefon işaretlerini IP şebekesinin algılayabileceği sayısal forma dönüştürmek ve bunları telefon hatlarına vermektir. [10]

Kodekler ise, analog formda gelen sesin, sayısal forma, gönderildiği noktada ise gelen sayısal formdan analog sesin üretilmesini sağlamaktadır. Kodekler aldıkları analog ses verisini belirli aralıklarla örnekleyerek bu değerleri sayısal forma dönüştürürler. VoIP sisteminde kodek seçimi yapılacağı zaman kullanılacak ortam önem kazanmaktadır. Şöyle ki; Seçilen ortam bir LAN (Yerel Alan Ağı) ise bu ağ üzerinde kullanılacak kodek'in G.711 olması ses kalitesini artırıcı unsur olarak gözükecektir. Bant genişliğinin önemli olduğu

ortamlarda ise WAN (Geniş Alan Ağı) kullanılacak kodek'lerin seçiminde daha az bant genişliğine ihtiyaç duyacak olan kodek'ler seçilmelidir. G.729 sıkıştırma tekniği bu seçim için bir örnek oluşturabilir; Seçilen bu kodek sistemi G.723 ile kıyaslandığında çok daha iyi bir ses kalitesi sağlamakta iken G.711 ile kıyaslandığında yetersiz kalmaktadır. Bu noktada dikkat edilmesi gereken bir diğer husus ise; G.729 kodek sisteminin G.723'e göre 1/4 daha fazla bant genişliğine gereksinim duyduğudur.

Sesi sıkıştırılması ve sıkıştırılan sesin tekrar çözülmesi işlemine Kodek (codec) (*Co*ding*Dec*oding) denir.

VoIP sistemlerinde kullanılan her kodek sisteminin belirli bir ses kalitesi vardır. Bunu ölçümlemek için bir grup dinleyici bir araya getirilip, dinletilen ses görüşmelerinin kalitesi puanlanıp bu sonuçlar MOS (Mean Opinion Score- Ortalama Fikir Değeri) adı altında belirlenmiştir. Burada dinleyiciler 1-5 arasında puanlama şeklinde görüşlerini belirtmişlerdir. Aşağıda kullanılan kodek sistemi ortamlarında alınan MOS değerleri birlikte tablo halinde verilmiştir.

Video Kodekler

- H.261 - video kodek >= 64kbps
- H.263 - video kodek < 64kbps

Audio Kodekler

G.711 Kodeki: Örnekme frekansı 8 kHz'dir. Örnek başına 8 bit kullanılır. Toplam bit hızı gereksinimi 64kbit/sn olur. Standart PCM sıkıştırmasıdır. MOS (Mean Opinion Score) değeri 4,1'tür.

G.723 Kodeki: Genel olarak düşük bit hızlarında iletim için kullanılır kalite olarak G.711'den kötüdür. Ama band genişliği gereksinimi de G711'in yaklaşık onda biri kadardır. Cebirsel CELP (ACELP) (6,3 kbit/sn) ya da MP-PLQ (5,3 kbit/sn) algoritmaları kullanılır. MOS değeri 2 - 3,8 değerleri arasındadır.

G.726 Kodeki: 16, 24, 32, 40 kbit/sn bit hızlarında adaptif diferansiyel PCM kodlaması

kullanır. MOS değeri 3,85'dir.

G.728 Kodeki: Bit hızı 16kbit/sn ve MOS değeri 3,61'dir.

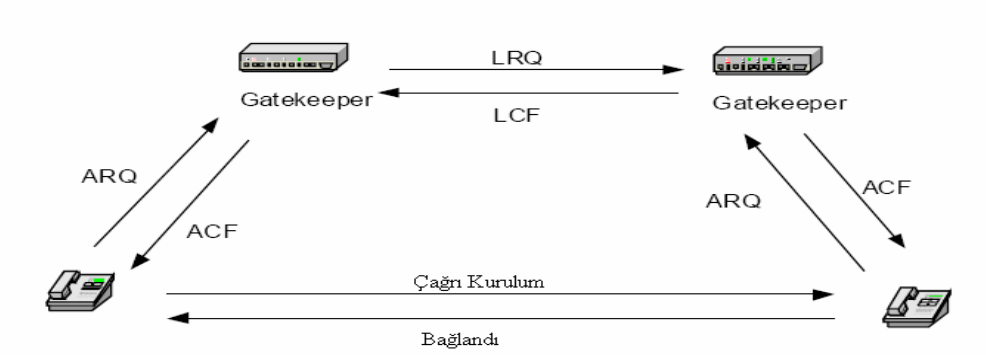
G.729 Kodeki: Bit hızı 8 kbit/sn'dir. MOS değeri 3,92'dir.

II.1.2.2.1.3 H.323' de Kontrol ve Haberleşme

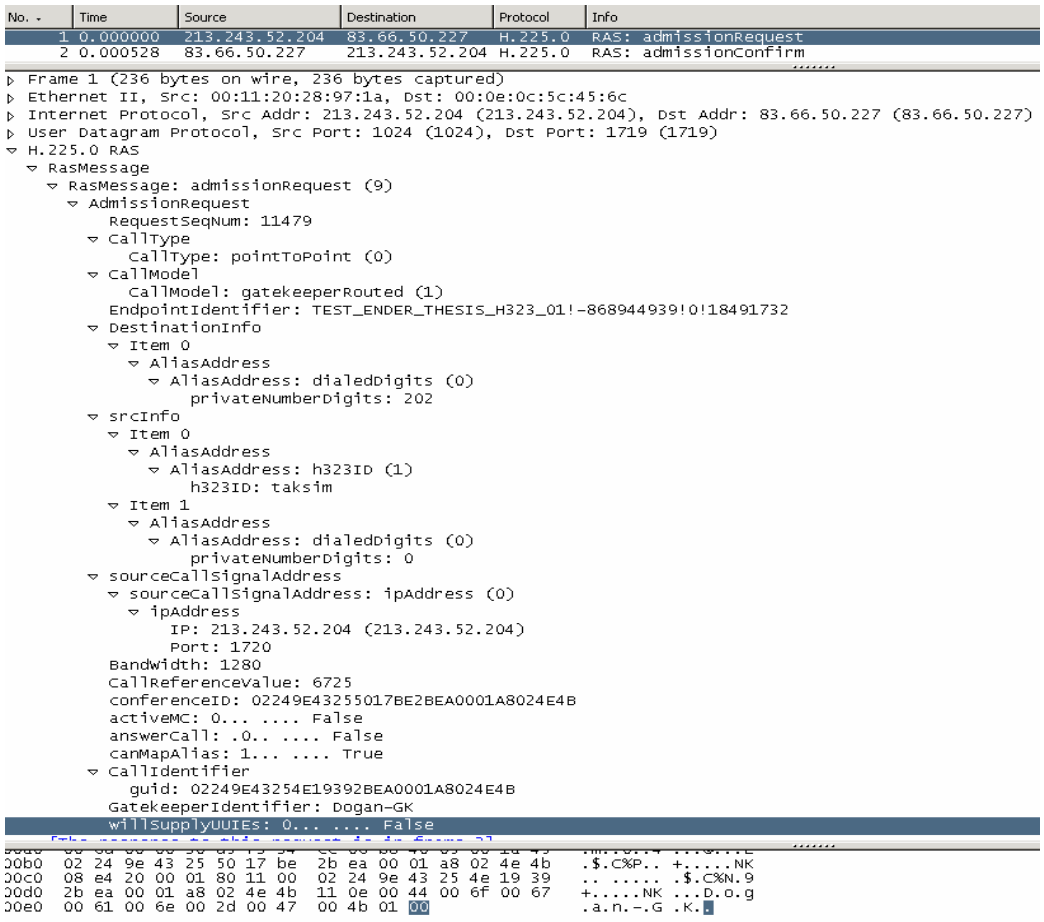
H.323 Çağrı Kontrolü ve Çağrı işaretleşmesi için H.245 ve H.225 protokollerini kullanır.

H.245 ile; Her akış için oluşturulan mantıksal kanal işaretleşmesini, ortamda video trafiği varsa bant genişliği artırımını, master-slave ayırımını, zamanlayıcı ve sayıcı değerlerini sağlar.

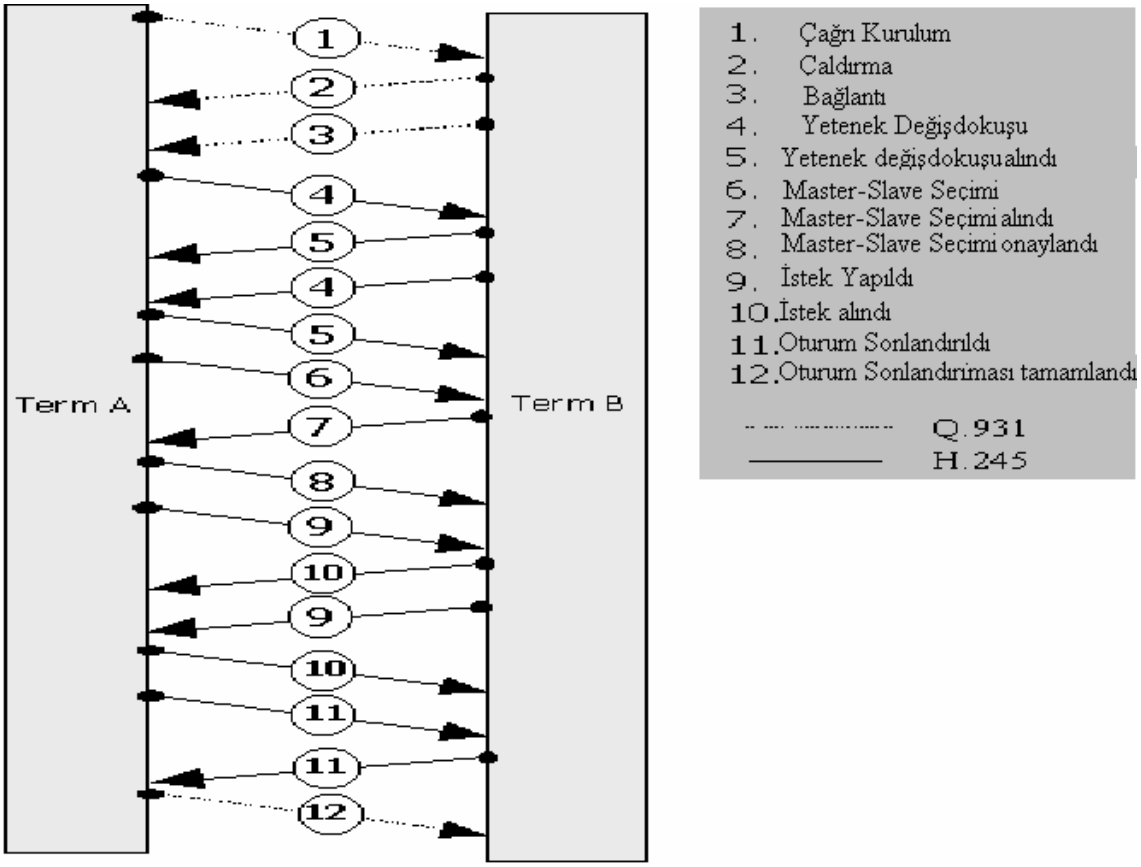
H.225 ile ise; Çağrı işaretleşmesini sağlar. H.225 çağrı işaretleşmesinde; Çağrı kurulum ve Bağlantı Q.931 ve TCP kullanılırken, RAS mesajları için UDP kullanılır.



Şekil-7 H.225 Çağrı İşaretleşmesi



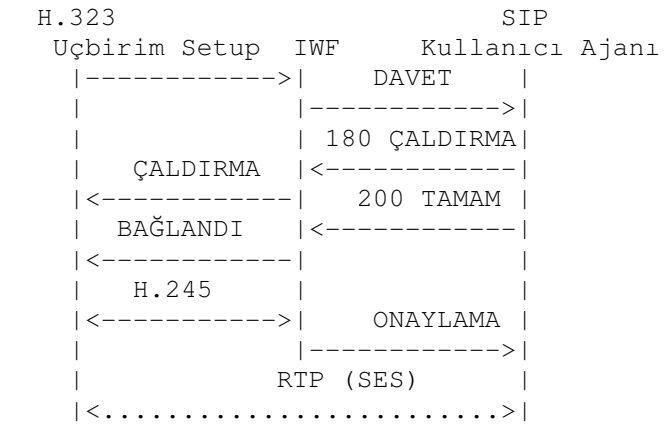
Şekil-8 H.225 Çağrı İşaretleşmesi (ARQ Mesaj) Çıktısı



Şekil-9 H.323 Çağrı Kurulum Aşamaları

- TCP 1720 port üzerinden H.225.0 oturumu başlatılır.
- ISDN kuralları ile işaretleşme ve kontrol kanalları oluşturulur. Kullanılacak video, veri ve ses gibi servisler konusunda anlaşma sağlanır
- RTP oturumu ile mantıksal kanal oluşturulur
- Router'lar RTP oturumu üzerinden multimedya verisini karşılıklı olarak gönderirler.
- Oturum çağrıyı başlatan noktanın Realese Complete mesajı ile sonlandırılır.

H.323 Terminal den SIP Kullanıcı Ajanına yapılan bir çağrı diagramı aşağıdaki gibi olmaktadır.



IWF: Interworking Function [11]

II.1.2.2.1.5 H.323 de Tamamlayıcı Hizmetler

H.323 Protokolünde aşağıdaki hizmetler tanımlıdır.

H.450.1 Series defines Supplementary Services for H.323

ITU-T H.450.1'de tanımlı olan bu servis, Tamamlayıcı Hizmetler için kontrol ve işaretleşme görevlerini üstlenir. [12]

H.450.2 Call Transfer supplementary service for H.323

ITU-T H.450.2'de tanımlı olan bu servis H.323 için çağrı transferi desteğini verir. [13]

H.450.3 Call diversion supplementary service for H.323

ITU-T H.450.3'de tanımlı olan bu servis, H.323 protokol'ü için çağrı yönlendirme servisini sağlar. [14] Bu servis içerisinde;

- Koşulsuz Çağrı Yönlendirme (Call Forwarding Unconditional) (SS-CFU)
- Çağrı Yönlendirme Meşgul (Call Forwarding Busy) (SS-CFB)
- Yanıtsız Çağrı Yönlendirme (Call Forwarding No Reply) (SS-CFNR)
- Çağrı Saptırma (Call Deflection) (SS-CD) servislerini barındırır.

H.450.4 Call Hold supplementary service

ITU-T H.450.4'de tanımlı olan bu servis, Gelen bir çağrıyı bekletip (Call Hold) (SS-HOLD), varsa başka çağrıyı yanıtlamaya olanak yaratır. [15]

H.450.5 Call Park supplementary service

ITU-T H.450.5'de tanımlı olan bu servis, gelen çağrının beklemeye alınıp, daha önce oluşturulmuş pick-up grup üyeleri tarafından karşılanabilemesine olanak yaratır. Call Pickup (SS-PICKUP).Gelen çağrı pick-up grubu üyeleri tarafından çekilebilmesine de olanak verir. [16]

H.450.6 Call Waiting supplementary service

ITU-T H.450.6'de tanımlı olan bu servis, aranan tarafın meşgul ise gelen çağrının bekletilmesine olanak yaratır. (call waiting) (SS-CW). [17]

H.450.7 Message Waiting Indication supplementary service

ITU-T H.450.7'de tanımlı olan bu servis, kullanıcıya mesaj bırakıldığı durumlarda, okunmayan mesajlarını olduğunu bildiren servistir.[18]

H.450.8 Calling Party Name Presentation supplementary service

ITU-T H.450.8'de tanımlı olan bu servis, Kullanıcı bilgilerinin karşı taraftaki uç birim noktasına gönderilmesini sağlar. [19]

H.450.9 Completion of Calls to Busy Subscribers supplementary service

ITU-T H.450.9'de tanımlı olan bu servis, Aranan taraf meşgul olduğunda veya cevap yoksa çağrının otomatik olarak kesilmesini sağlar. [20]

H.450.10 Call Offer supplementary service

ITU-T H.450.10'de tanımlı olan bu servis, Arayan tarafın isteğine bağlı olarak aranan taraf meşgulse, arayanın hatta tutulması ve meşgul durumun sona ermesiyle birlikte çağrının kurulmasını sağlar. Bu özellik, ülkemizde aranan tarafın devamlı meşgul olduğu, yarışma programları gibi yerlerde, kullanılmak için oldukça elverişlidir. [21]

H.450.11 Call Intrusion supplementary service

ITU-T H.450.11'de tanımlı olan bu servis, Arayan A kullanıcısının, aranan B kullanıcısı C kullanıcısıyla görüşme halindeyse araya girmesini sağlar. Bu hizmet, A kullanıcısının isteğine göre verilebilir. Özellikle önceliği yüksek olan kullanıcılar (komutanlar, büyük patronlar) bu hizmetten yararlanmak isteyeceklerdir. [22]

II.1.2.2.1.6 H.323 Protokol Sürümlerine Bakış

II.1.2.2.1.6.1 H.323 Sürüm 3

H.323'ün bu sürümü ile birlikte;

Hızlı bağlantı (Fast Connect) kurulması için protokol olarak TCP yerine UDP üzerinden işaretleşmenin yapılmasını sağlanmıştır.

H.323 Sürüm 3, SS7 işaretleşmesinin olduğu PSTN şebekeleri ile de uyumlu çalışabilmektedir.

Ayrıca H.323 v.3, H.246C desteğidir. Bu destek ise ISUP ile H.226 konuşabilmesini sağlar.

Bu Sürüm ile birlikte tamamlayıcı hizmet olarak H.450.4 – 5 – 6 – 7 servisleri eklenmiştir.

II.1.2.2.1.6.2 H.323 Sürüm 4

H.323'ün bu sürümü ile birlikte;

Ses ile görüntü verilerinin birleştirilmiş bir şekilde aynı anda açılan kanal üzerinden akması sağlanmıştır.

H.323 protokolü, daha geniş şebekelere cevap verebiliyor duruma gelmiştir.

İlk sürümlerde işaretleşme dönüşümleri, çağrı kontrolleri, kodekler arası dönüşümler gibi görevler,n ağ geçitleri üzerinden yapılması işlemi bu sürüm ile birlikte ağ geçityolu görev anlamında üç ayrı bölüme ayrılarak çözümlenmiştir.

İşaretleşmeler için Ağ Geçidi : Yapıdaki tüm işaretleşme sistemlerinden sorumludur.

Akılsız Medya Ağ Geçidi (MG) : PSTN ağı ile, IP ağı arasındaki dönüşümlerden sorumludur.

Medya Ağ Geçidi Kontrolörü (MGC) : Medya Ağ Geçidlerinin çağrıları nasıl işlemesi gerektiğini bilen ve gerekli direktifleri Media Ağ Geçidlerine vermekten sorumludur.

Bu sürüm ile birlikte tamamlayıcı hizmetler olarak; H.450.8 – 9 - 10 -11 servisleri tanımlanmıştır.

H.323 Sürüm 4, yukarıdaki özelliklerinin yanında H.323 ekipmanlarının WEB tabanlı kontrolüne izin veren Annex K özelliğine ve bir H.323 bileşeninin öznitelik sunucusuna (feature server) bağlanıp ek özellikler sağlayan Annex L desteğine sahiptir. Ayrıca, ek kayıt (additive registration) özelliği bu sürüm ile birlikte tanımlanmıştır.

Bu sürümler ile birlikte Sürüm 5 ve draft aşamasında olan Sürüm 6 tanımlamaları yapılmıştır.

II.1.2.2.1.7 H.323'de QoS (Hizmet Kalitesi)

Servis kalitesi bir performans kriteridir. Servis kalitesini etkileyen her etken, sistem performansını doğrudan etkileyecek ve hatta belirli bir QoS değerinin tutturulabilmesi için de sisteme ek maliyet getirecek yatırımlar yapmak gerekecektir. Bu yüzden servis kalitesini etkileyen unsurları iyi analiz edebilmek bir mühendis için çok önemlidir. Servis kalitesini etkileyen unsurlar aşağıda verilmiştir.

Gecikme (Delay): Ses paketinin kaynaktan yollanması ile alıcı tarafından alınması arasında geçen süre olarak tanımlanır. Başlıca gecikmeler beş adettir.

Örnekleme Gecikmesi: Darbe kodlama modulasyonu yapılmadan önce ses işareti örneklenir. İşte bu örnekleme esnasında belirli bir süre geçer. Bu geçen süreye örnekleme ecikmesi denir. Bu değer işaretin örnekleme aralığı ile doğru orantılıdır. Çoğu zaman 125-150 ms kadardır.
Sıkıştırma Gecikmesi: Sesin belirli bir kodek ile kodlanması sırasında geçen süredir. Bu süre kodlama algoritmasının karışıklığına ve kodlama yapan işlemcinin işlem yapma hızına bağlıdır.

Kod Çözme Gecikmesi: Belirli bir codec ile sıkıştırılmış sesin açılması (decode) sırasında geçen süredir. Bu süre de kod çözücü işlemcinin hızına ve sıkıştırma algoritmasının karmaşıklığına bağlı olarak değişir.

Transmisyon Gecikmesi: Paketin iletimi esnasında iletim yollarında geçen süredir. Bu süreyi azaltmanın en iyi yolu, iletim hattının enformasyon hızını arttırmaktır. Örneğin, 16kb'lik bir veri paketi 4kb/s hızındaki bir hattan iletildiğinde iletim 4 saniye alırken, 48kb/s'lik bir hattan (ISDN-D kanalı)yollandığında iletim 0,33 saniye alır.

Bellekleme Gecikmesi: Tüm paket gecikmelerinin aynı yapılması amacıyla verilerin belirli bir süre belleklerde (buffer) tutulmasından kaynaklanan gecikmedir. Ayrıca bu gecikme sadece

karasal transmisyonda görülmez. Bunun yanı sıra uydu haberleşmesinde de uydunun Dünya ile olan konumunun devamlı değiştiği orta (MEO) ve kısa yörünge (LEO) uydularının veri aktarımı esnasında da görülür.

Jitter: Bir kaynaktan çıkan paketlerin her birinin farklı gecikme değerleriyle alıcıya ulaşması sonucu oluşur. Buna gecikme varyasyonu da denir.

II.1.2.2.2 SIP Protokolü

SIP *(Session Initiation Protocol),* Internet üzerinden çoklu ortam hizmetlerinin işletilebilmesi için geliştirilen ve IETF tarafından (RFC 2543) te tanımlanmış bir protokoldür. Söz konusu çoklu ortam servislerinden en çok bilineni ve kullanılanı Internet üzerinden sunulan telefon hizmetleridir. Internet üzerinden sunulan telefon hizmetleri *(Internet Telephony)* ucuz ancak daha düşük kalitede, uluslararası sesli görüşme yapma olanağı sağlamaktadır. Internet bu telefon çağrıları için taşıma ortamı olarak kullanıldığından ve uluslararası pahalı özel hatlar kullanılmadığında, görece daha ucuz hizmet sunulabilmektedir.

SIP'de, SMTP ve HTTP benzeri diğer Internet hizmetleri gibi metin bazlı bir arayüz kullanılması SIP protokolünün esnekliğini artırmaktadır. SIP, bir IP ağı üzerindeki iki ya da daha fazla kullanıcı arasında çağrı kurulumu, çağrı sırasında oturumlu ilgili parametrelerin değiştirilmesi ve nihayi olarak çağrının çözülmesi, sona erdirilmesi, için kullanılmaktadır. Telefon hizmetlerinin IP ağları üzerinden sunulmasında SIP ile birlikte mevcut başka protokollerde kullanılmaktadır; ses ve görüntünün akışkan bir şekilde iletimi için RTP, ses ve görüntü kalitesinin ağ boyunca istenen kalitede sağlanabilmesi için ağ cihazları arasında işaretleşmeyi sağlayan RSVP, kullanıcı dizin hizmetleri için LDAP ve kullanıcıların doğrulanması için RADIUS gibi. [23]

II.1.2.2.2.1 SIP Mimarisi Ve Temel Bileşenleri

SIP iki temel bileşene sahiptir; [10]

SIP Kullanıcı Ajanı (SIP User Agent):

Kullanıcı Ajanı, çağrı başlatan ve cevaplayan birimdir. Kullanıcı ajanı iki alt birime sahiptir:

Kullanıcı Ajanı İstemcisi (User Agent Client, UAC)
Kullanıcı Ajanı Sunucusu (User Agent Server, UAS)

İstemci birimi çağrıyı başlatır ve Sunucu birimi ise çağrıyı cevaplar. SIP kullanıcı ajanı herhangi bir PC ye kurulu olan yazılımsal bir Soft IP Phone, bir Netmeeting kullanıcısı, bir Windows Messenger kullanıcısı veya hardphone olarak IP telefonu ya da otomatik cevap sistemi olarak bir sesli yanıt sistemi olarak (IVR) uyarlanabilir. Böyle bir yapıda yönetici konumunda olan SIP Ağ Sunucusu na gerek olmamaktadır.

SIP Ağ Sunucusu (SIP Network Server) :

Kullanıcı Ajanı İstemcisi *(User Agent Client, UAC)* ve SIP Ağ Sunucusu temel olarak isimden IP adresine çözümleme işlevini sağlar. Tipik olarak SIP kullanıcıları kendilerini tanımlayan benzersiz alfanümerik adresler kullanırlar. Ayrıca E. 164 formunda telefon numaralarının da kullanılması mümkündür. Alfanümerik adreslerde e-mail adreslerine benzer şekilde kullanici_adi@etki_alani yapısı kullanılır. Kullanım kolaylığı açısından mevcut e-mail adresleri de kullanılmaktadır. [23]

Bir SIP uygulamasında üç tür sunucu bulunabilir:

Vekil Sunucu (Proxy Server), diğer kullanıcılar adına talepte bulunabilen ve hem sunucu ve hem de kullanıcı rolünü üstlenebilen bir sunucu türüdür. Talepler dahili olarak karşılanabildiği gibi, isim çevriminden sonra başka sunuculara aktarılabilir. Bir Vekil Sunucu, talebi yorumladıktan sonra gerekiyorsa talep mesajını yeniden yapılandırarak iletebilir. Bu tür sunucular SIP olmayan uçlarla çoklu ortam oturumlarının kurulabilmesine de olanak sağlayabilirler; örneğin SIP'den H.323'e çevrim gibi.

Yönlendirme Sunucusu (Redirect Server) SIP talebini kabul eder, aranan tarafın adresini yada aranan tarafın adresini bilmiyorsa adres olarak sıfırı geri döndürür. Vekil Sunucunun aksine Yönlendirme Sunucusu talepleri diğer sunuculara aktarmaz.

Kayıt Sunucusu (Registrar) Bir kayıt sunucusu, kullanıcıların kayıt taleplerini kabul ederek, kullanıcıların konum bilgilerinin bulunduğu veri tabanını günceller.

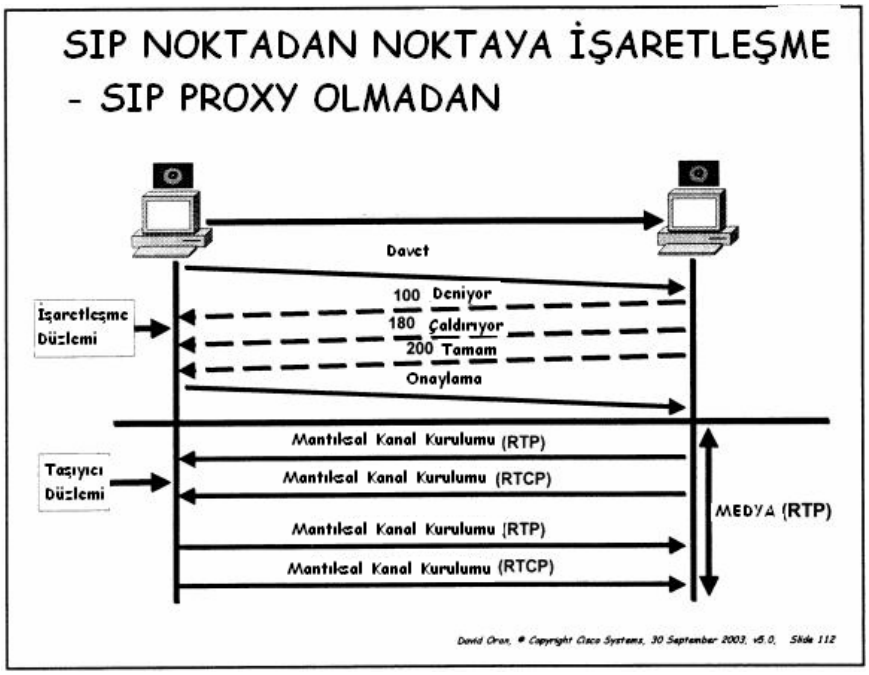
SIP, a**ğ** katmanından bağımsız olarak, kendi hata denetim ve düzeltme mekanizmalarına sahip olduğundan bu işlevleri sağlamayan Datagram ortamında da SIP hizmetleri işletilebilir. SIP hem TCP ve hem de UDP üzerinde işletilebilmektedir. SIP aşağıdaki hizmetlerin sunulabilmesi için protokol mekanizmalarına sahiptir:

Bir kullanıcı, diğer bir kullanıcıyı aramak istediğinde, kullanıcı bir davet talebi ile çağrıyı başlatır. Talep mesajı aranan tarafın oturuma dahil olabilmesi için yeterli bilgileri içermektedir. Eğer aranan tarafın konum bilgisi, IP adresi, biliniyorsa talep mesajı doğrudan karşı tarafa gönderilebilir. Eğer bu bilgi elde yoksa talep mesajı yerel SIP sunucusuna gönderilir. Eğer yerel sunucu bir vekil sunucu ise aranan tarafın adresini çözümler ve talebi aranan uca iletir. Çözümleme birçok şekilde gerçekleştirilebilir; DNS sorgulaması, LDAP taraması gibi. Eğer yerel sunucu bir yönlendirme sunucusu ise, arayan uca, aranan ucun adres bilgisini iletir ve arayan taraf doğrudan çağrıyı kurar.
Hedef kullanıcının bulunması sırasında, aranılan asıl kullanıcının kayıtlı bulunduğu sunucu bulunana kadar yerel sunucu, diğer sunuculara çağrıyı aktarabilir.

Kullanıcı bulunduğunda talep, aranan kullanıcıya iletilir. Davet talebine, cevaplayan kullanıcının uçbirim yetenekleri ile cevap verilir ve bağlantı gerçekleştirilir. Uçbirim yetenekleri kullanıcı tarafından da yapılandırılabilmektedir. Örneğin kullanıcı uçbirimi görüntülü çağrıları desteklese de kullanıcı yalnızsa sesli çağrıları kabul etmeği tercih edebilir. Bu özellikler daha sonra da eklenebilir. Eğer çağrı aranan kullanıcı tarafından reddedilirse çağrı bir telesekreter *(Voice Mail)* ya da başka bir kullanıcıya yönlendirilebilir.

SIP ayrıca iki önemli özelliğe sahiptir. Bir vekil sunucu gelen bir çağrıyı paralel olarak aynı anda birden fazla uca iletebilir. Örneğin kullanıcı iki ofiste birden çalışıyorsa, hangisinde olursa olsun çağrıyı cevaplama imkanına sahip olmaktadır. İkinci önemli ve benzersiz özellik

ise, SIP sunucusunun bir arama talebine değişik ortam bağlantı seçenekleri ile cevap verebilmesidir. Örneğin bir arama yapıldığında eğer aranan kişi erişilemiyorsa, SIP sunucusu telesekreter servisi ile birlikte, alternatif olarak aranabilecek SIP uçlarının bir listesini geri döndürebilir; arayan kullanıcı bu seçeneklerden birini seçip aramayı gerçekleştirebilir.



Şekil-10 SIP'ten SIP'e Çağrı İşaretleşmesi [24]

Yukarıda SIP Proxy olmadan gerçekleşen bir SIP çağrı diagramı gösterilmektedir.

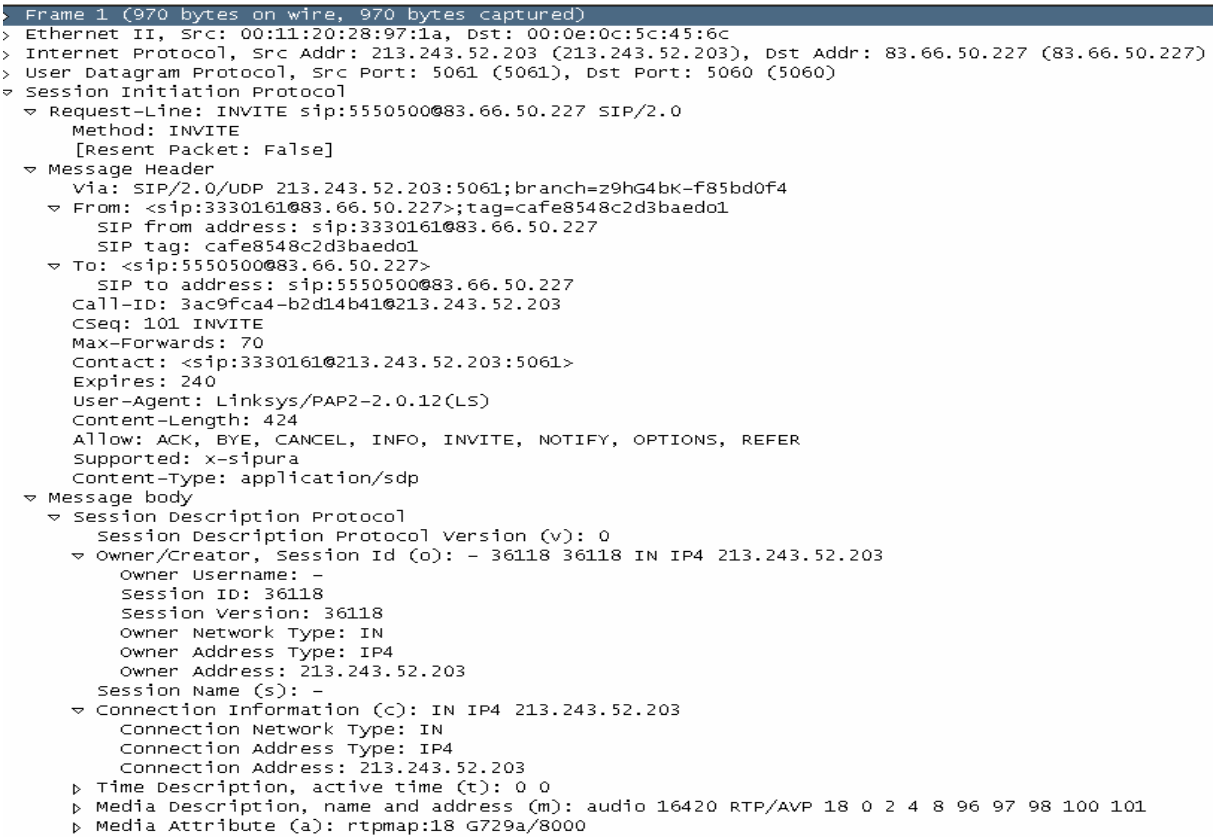
II.1.2.2.2.2 SIP Mesajları

Temel olarak iki gruba ayrılan SIP mesajları, kullanıcıdan gelen istek(Request) mesajları ile bu istek mesajlarına Sunucu tarafından verilen yanıt(Response) mesajlarından oluşur. SIP oturumlarında kullanılan bu mesajlar bir başlık alanı ve opsiyonel olarak gövde alanından oluşur. Aşağıda genel istek(request) mesaj türleri ve açıklamaları gösterilmiştir.

II.1.2.2.2.2.1 SIP İstek Mesajları

SIP istek mesajları aşağıdaki gibidir.

Davet (İnvite) : Kullanıcının oturuma davet edilmesini sağlayan mesajdır. Davet – İnvite mesajının gövde kısmında davet edilen, çağrıya çağırılan taraf ile ilgili bilgilerde mevcuttur. Aşağıda Davet-İnvite mesajının parametreleri ile örnek bir Davet-İnvite mesaj görüntüsü verilmiştir.



Şekil-11 SIP İnvite (Davet) Mesajı

Request-Line: INVITE sip:5550500@83.66.50.227 SIP/2.0
"İstek-Satırı: Burada yapılan isteğin türü ve SIP protocol sürümü belirtilmektedir."

Message Header
Via: SIP/2.0/UDP 213.243.52.203:5061;branch=z9hG4bK-f85bd0f4
"Bu satırda bir önceki atlama noktası belirtilmekte."

From: <sip:3330161@83.66.50.227>;tag=cafe8548c2d3baedo1
"Bu satır istekte bulunan kişinin bilgisini belirtmekte."

To: <sip:5550500@83.66.50.227>
„Bu satırda istekte bulunulan kişi bilgisi belirtilmekte."

Call-ID: 3ac9fca4-b2d14b41@213.243.52.203
"Bu satırda yapilan isteğin belirteci belirtilmekte."

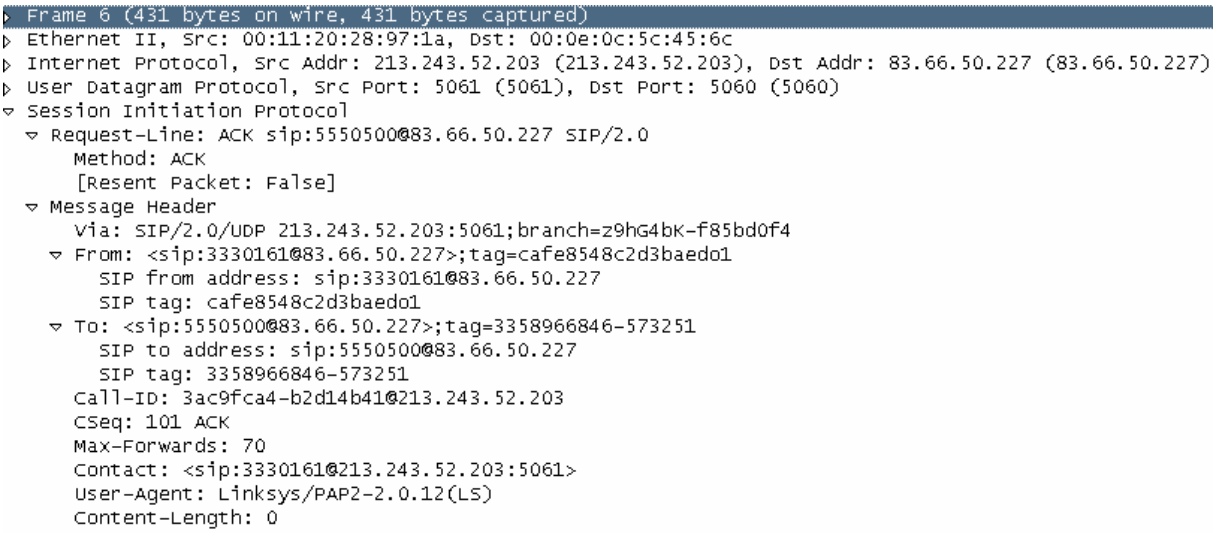
CSeq: 101 INVITE
" Bu satırda yapılan iletim belirtilmekte."

Max-Forwards: 70
Contact: <sip:3330161@213.243.52.203:5061>
"Bu satırda kontak bilgisi ve UDP portu belirtilmekte."

Expires: 240
User-Agent: Linksys/PAP2-2.0.12(LS)

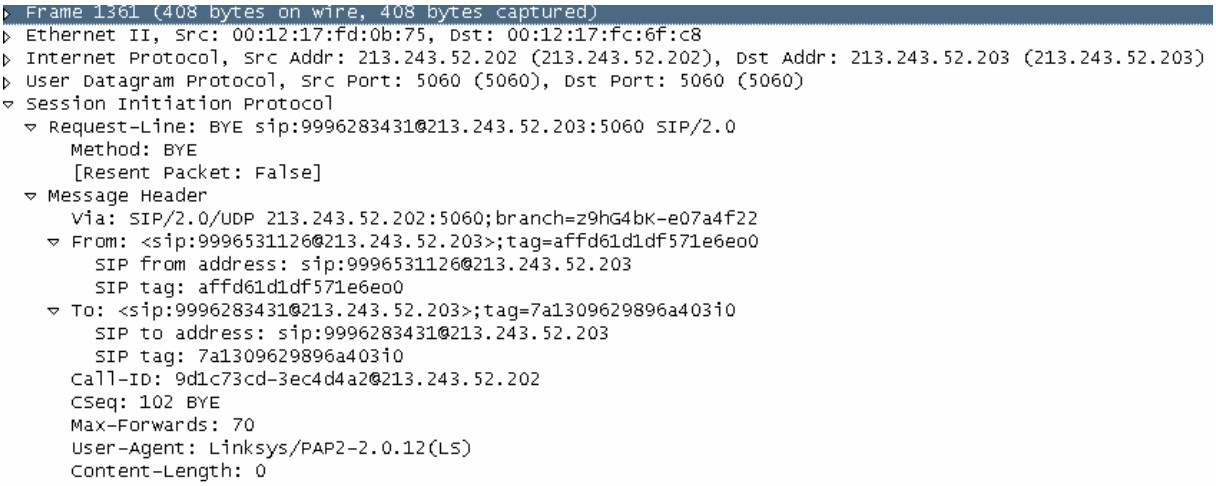
```
       " Bu satırda kullanıcı ajanda kullanılan SIP uç birim bilgisi
verilmekte."
        Content-Length: 424
        Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
        Supported: x-sipura
        Content-Type: application/sdp
        "Bu satırda içerik tipi belirtilmekte. Burada SDP gösterilmekte."

  Message body
        Session Description Protocol
            Session Description Protocol Version (v): 0
            Bu satırda kullanılan SDP sürümü belirtilmekte.
            Owner/Creator, Session Id (o): - 36118 36118 IN IP4
213.243.52.203
            Burada SIP oturumunu başlatan kullanıcı bilgisi verilmekte.

            Session Name (s): -
            "Oturumun adı belitilmekte bu satırda."

            Connection Information (c): IN IP4 213.243.52.203
            "Bu satırda yapılan bağlantının bilgileri verilmekte."

            Time Description, active time (t): 0 0
            Media Description, name and address (m): audio 16420 RTP/AVP 18
0 2 4 8 96 97 98 100 101
            "Burada oluşturulan SIP ortamının bilgileri verilmekte."
```

Onaylama (ACK) : Mesaj alışverişinin yapılabileceğini belirten onaydır.



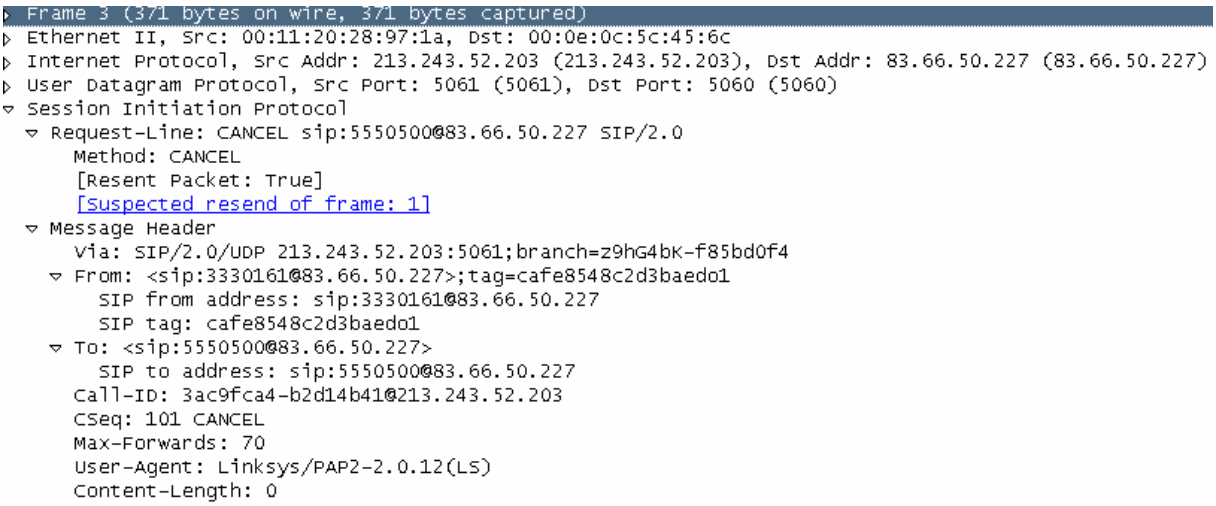
Şekil-12 SIP ACK (Onaylama) Mesajı

Çözülme (BYE) : UA tarafından Sunucuya iletilen çağrıyı sonlandırma isteği mesajıdır. Bu mesajı arayan taraf gönderebildiği gibi, aranan tarafta gönderebilir.



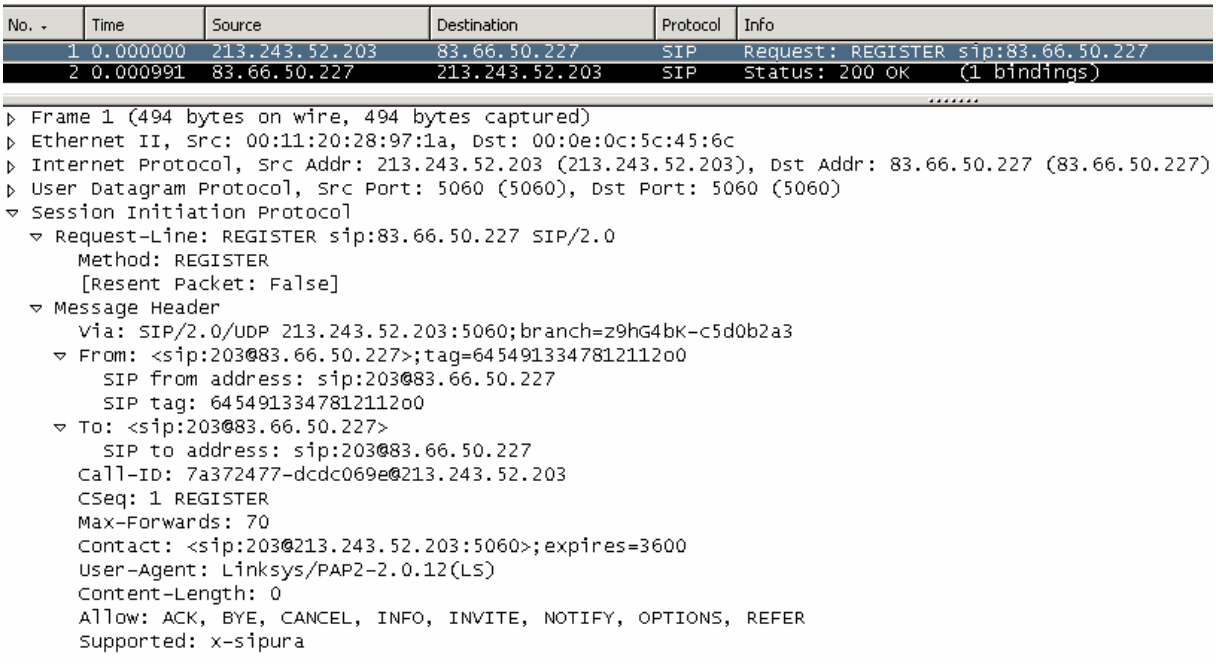
Şekil-13 SIP BYE (Çözülme) Mesajı

İptal (CANCEL) : Çağrının kurulmasının iptalini isteyen istek mesajıdır.



Şekil-14 SIP CANCEL (İptal) Mesajı

Kaydolma (REGISTER) : Başlık alanında listelenen adrese kayıt olunmasını sağlayan istek mesajıdır.



Şekil-15 SIP REGISTER (Kaydolma) Mesajı

Seçenekler (OPTIONS) : Karşı uç birimden yeteneklerini ve kapasite sınırları bilgisini isteyen istek mesajıdır.

Bilgi (INFO) : Oturumun kapatılmadan , bu oturuma ait bilgilerin gönderilmesini sağlayan istek mesajıdır.

II.1.2.2.2.2.1 SIP Yanıt Mesajları

Alınan bir SIP istek(request) mesajının ardından bu istek mesajına bir yanıt verilir. İstek mesajlarına verilen yanıt mesajları başlıca altı sınıfa ayrılır. [25]

== 1xx— Bilgilendirme Mesajları ==

Bu yanıt mesajları, kullanıcı tarafından gelen istek mesajlarının alındığını ve çağrı aşamalarının başlama süreçlerini belirtir. Aşağıda SIP bilgilendirme mesaj türleri gösterilmiştir.

* 100 = Deniyor

* 180 = Zil Çaldırılıyor
* 181 = Çağrı Yönlendiriliyor
* 182 = Çağrı Sıraya Konuldu
* 183 = Oturum işlemde

== 2xx—Başarılı Yanıt Mesajları ==

Bu yanıt mesajları anılan istek mesajlarının başarılı bir şekilde alındığını ve kabul edildiğini gösterir.

* 200 = Tamam

== 3xx—Yönlendirme Yanıt Mesajları ==

Bu yanıt mesajları yapılan isteğin yerine getirilmesi için yeni işlemlere gereksinim olduğunu belirtir.

* 300 = Çoklu Seçim
* 301 = Kalıcı olarak yer değiştirilmiş
* 302 = Geçici olarak yer değiştirilmiş
* 305 = Proxy sunucusu kullanılmalı
* 380 = Alternatif Servisler

== 4xx—Kullanıcı Tarafı Hata Mesajları ==

Bu yanıt mesajları yapılan isteğin sunucu tarafında çözülemediğini-anlaşılamadığını veya servis dışı olduğunu belirtir.

* 400 = Hatalı istek, sözdizimi hatası
* 401 = Gerekli izin bulunmuyor.
* 402 = Ödeme gerekli,
* 403 = Giriş yasağı bulunuyor.

* 404 = Kullanıcı bulunamadı.
* 405 = Metoda izin verilmiyor
* 406 = Kabul edilebilir değil.
* 407 = Proxy doğrulaması gerekli
* 408 = İstek zaman aşımı: Kullanıya zamanında ulaşılamadı.
* 410 = Artık yok
* 412 = Koşullu istek hatası (Bu mesaj RFC [3903] te tanımlanmıştır.)
* 413 = Kimlik isteği çok geniş
* 414 = URI isteği çok uzun
* 415 = Desteklenmeyen Medya Tipi
* 416 = Desteklenmeyen URI düzeni
*420 = Bozuk Uzantı: Bozuk SIP Protokol eklentisi kullanılıyor,server tarafından anlaşılmadı.
* 421 = Uzantı gerekli
* 423 = Aralık çok kısa
* 480 = Geçici kullanılamaz
* 481 = Çağrı/Hareket-İşlem yok
* 482 = Dögü saptandı
* 483 = Çok atlama noktası var
* 484 = Tamamlanmamış adres
* 485 = Belirsiz
* 486 = Meşgul
* 487 = Sonlandırılmış istek
* 488 = Kabul edilebilir değil
* 489 = Kötü olay (Bu mesaj RFC [3265] de tanımlanmıştır.)
* 491 = Bekleyen İstekler
* 493 = S/MIME gövde bölümü şifresi çözülemedi
* 494 = Güvenlik anlaşması gerekli (Bu mesaj RFC [3329] da tanımlanmıştır.)

== 5xx—Sunucu Tarafı Hata Mesajları ==

* 500 = Sunucu iç hatası
* 501 = SIP istek metodu buraya uyarlanamaz

* 502 = Bozuk geçityolu
* 503 = Servis bulunamadı
* 504 = Sunucu zaman aşımı
* 505 = Sürüm desteklenmiyor
* 513 = Mesaj çok uzun

== 6xx—Global Hata Mesajları ==

* 600 = Meşgul
* 603 = Rededildi
* 604 = Hiçbiryerde yok
* 606 = Onanamaz- kabul edilemez

II.1.2.2.2.3 SIP Destekleyen Protokoller

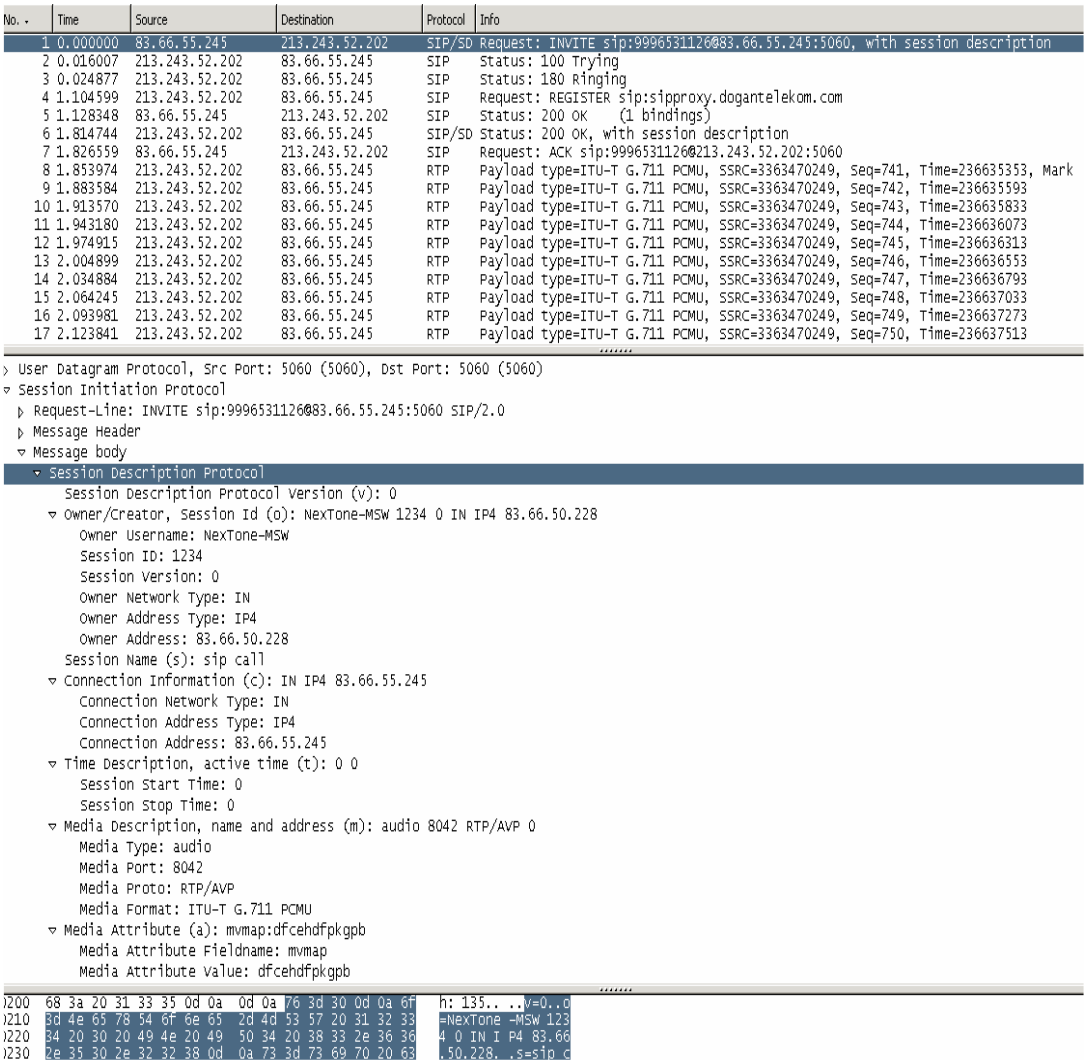
II.1.2.2.2.3.1 SDP Protokolü

RFC 2327 de tanımlanan bu protokolün görevi; Bunlar varolan bir oturum ile haberleşmeyi sağlamak ve oturuma katılmak isteyen taraflara gerekli bilgiyi sağlamaktır. Unicast bir ortamda ise görevi ; Oturuma katılmak isteyen kullanıcıya gerekli bilgiyi sağlamaktır. SDP nin sağlamakla yükümlü olduğu bilgiler aşağıdaki gibidir.

- Oturumun adı, amacı
- Oturumun ne kadar süre ile aktif kalacağı
- Oturumu oluşturan medya türü
- Bu medyayı (adres, port numarası , format vb.) almak için gerekli olan bilgi
- Konferansta kullanılacak band genişliği bilgisi
- Oturumu yöneten kişi bilgisi

SDP Medya içeriği ise aşağıdaki bilgileri içerir;

- Medyanın türü
- Taşıma protokolü
- Medyanın formatı
- Taşınacak medya için multicast adresi (Multicast ortamda)
- Taşınacak medya için taşıma portu (Multicast ortamda)
- Karşı tarafın adresi (Unicast ortamda)
- Karşı tarafta iletişimde kullanılacak port numarası bilgisi (Unicast ortamda)



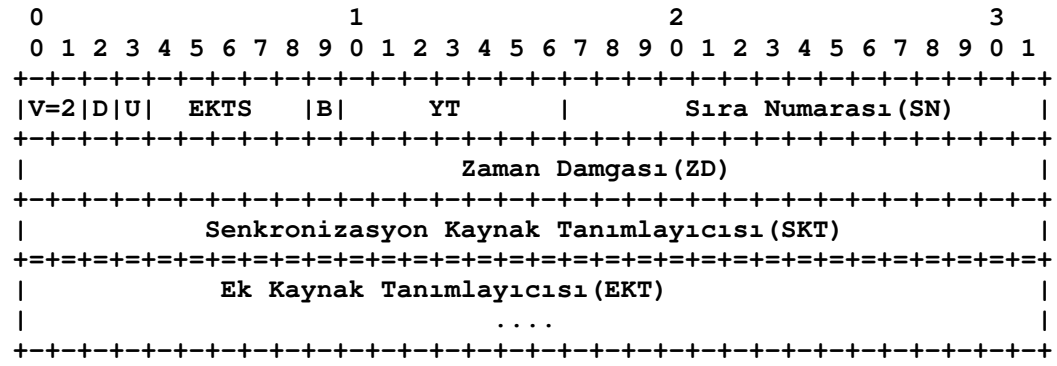
Şekil-16 SDP Mesajı

II.1.2.2.2.3.2 RTP Protokolü

RFC 3350'de tanımlanan RTP, bir ses paketinin önüne yerleşerek, UDP ve IP paketlerinin içine konularak çalışır. Ve temel anlamda gerçek zamanlı iletişim için kullanılan UDP ye sıra numarası ve zaman damgası gibi özellikleri ile UDP nin güvenirlik sorununu ortadan kaldırmaya çalışır. [26]

Bir kodek ile kodlanan gerçek zaman sesi RTP başlığı ile paketlenir. RTP, eş zamanlama gibi yöntemler kullanarak ağ gecikme değişkenliğinin etkilerini azaltmaktadır. Geç iletilen paketler alıcı tarafından düşürüleceği için eşzamanlama ile ağdaki gecikme değişkenliği büyüdükçe ses parçalarının alıcı tarafında işlenmesi için gereken bekleme süresi (playout time) artırılır.

RTP (Real-time Transport Protocol), gerçek zamanlı ses, görüntü ya da simülasyon verilerinin uçtan ucu taşınmasını sağlayan protokoldur. RTP, kaynak ayırtımı (resource reservation) yapmaz ve hizmet kalitesini (QoS) garanti etmez.



Şekil-17 RTP Mesaj Yapısı [17]

Sürüm (V) (2 bit): RTP sürüm numarası

Dolgu (D) (1 bit) : Bu alan 1 olarak işaretlendiğinde bazı bit ekleme oktetlerinin olduğunu gösterir.

Uzantı (U) (1 bit) : Ek bir başlığın olduğunu belirtir.

Ek Kaynak Tanımlayıcı Sayısı (EKST) (4 bit) : Ek kaynak tanımlayıcı sayısını belirtir.

Belirteç (B) (1 bit) : Veri akışını sınırlarını belirtir.

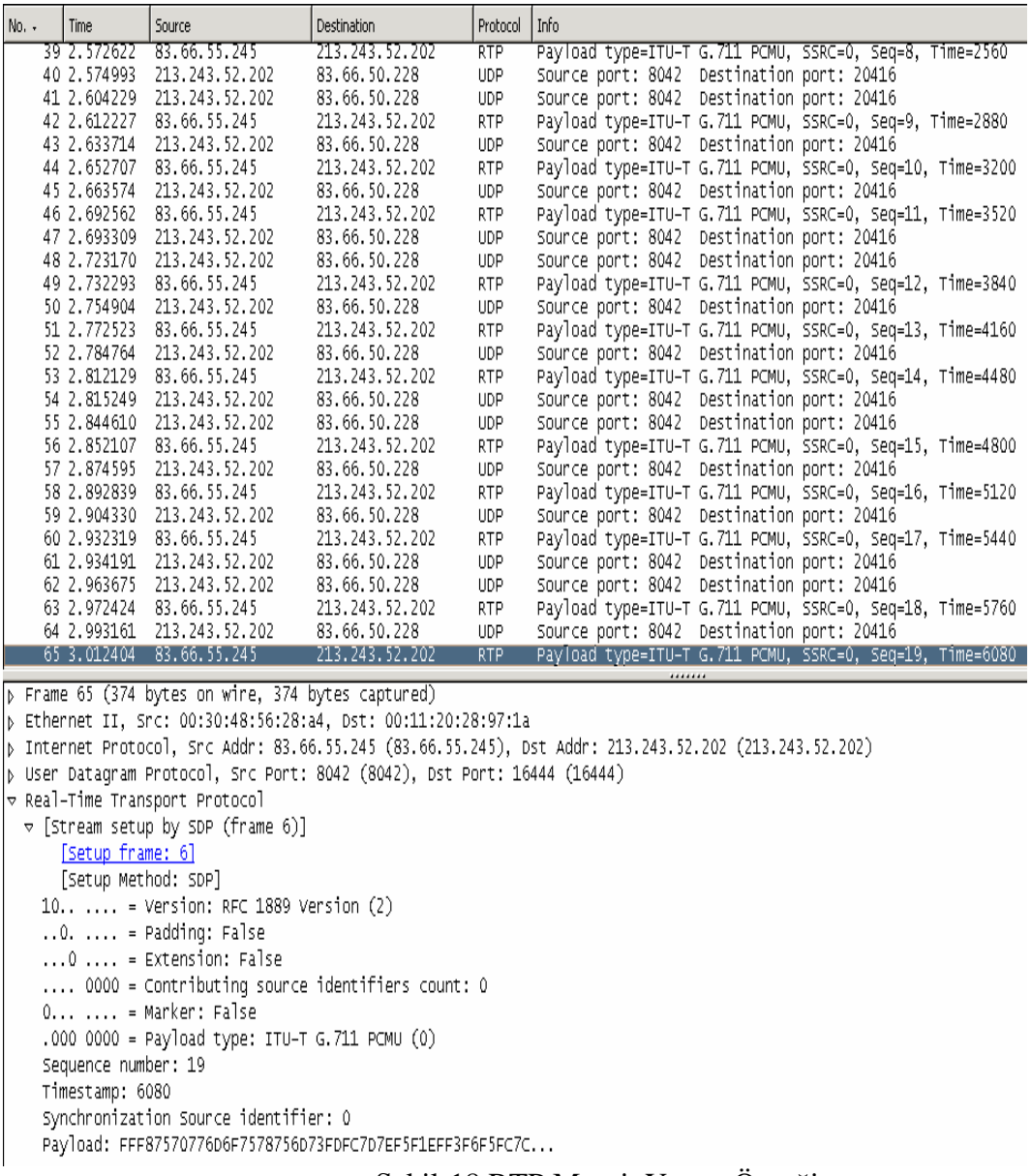
Yük Tipi (YT) (8 bit) : Ne tür yük taşındığını belirtir.(Ses mi , video mu vb.)

Sıra Numarası (SN)(16 bit) : Bu değer her RTP paketinde artış gösterir.

Zaman Damgası (ZD) (32 bit) : Burada ilk oktetin örnekleme anı, RTP paketine yansıtılır. Örnekleme anı standart artan bir saatten alınabilir. Böylece senkronizasyon ve jitter hesaplamaları yapılabilir.

Senkronizasyon Kaynak Tanımlayıcısı (SKT) (32 bit) : Senkronizasyon kaynağını belirtir.Bu belirtec rastgele olarak seçilir. Aynı oturumdaki senkronize olacak her kaynağın SKT numarası farklı olur.

Ek Kaynak Tanımlayıcısı (EKT) (32 bit) : Paket yüküne katkıda bulunan kaynakları tanımlar. Bu kaynakları sayısı EKTS de belirtilir.



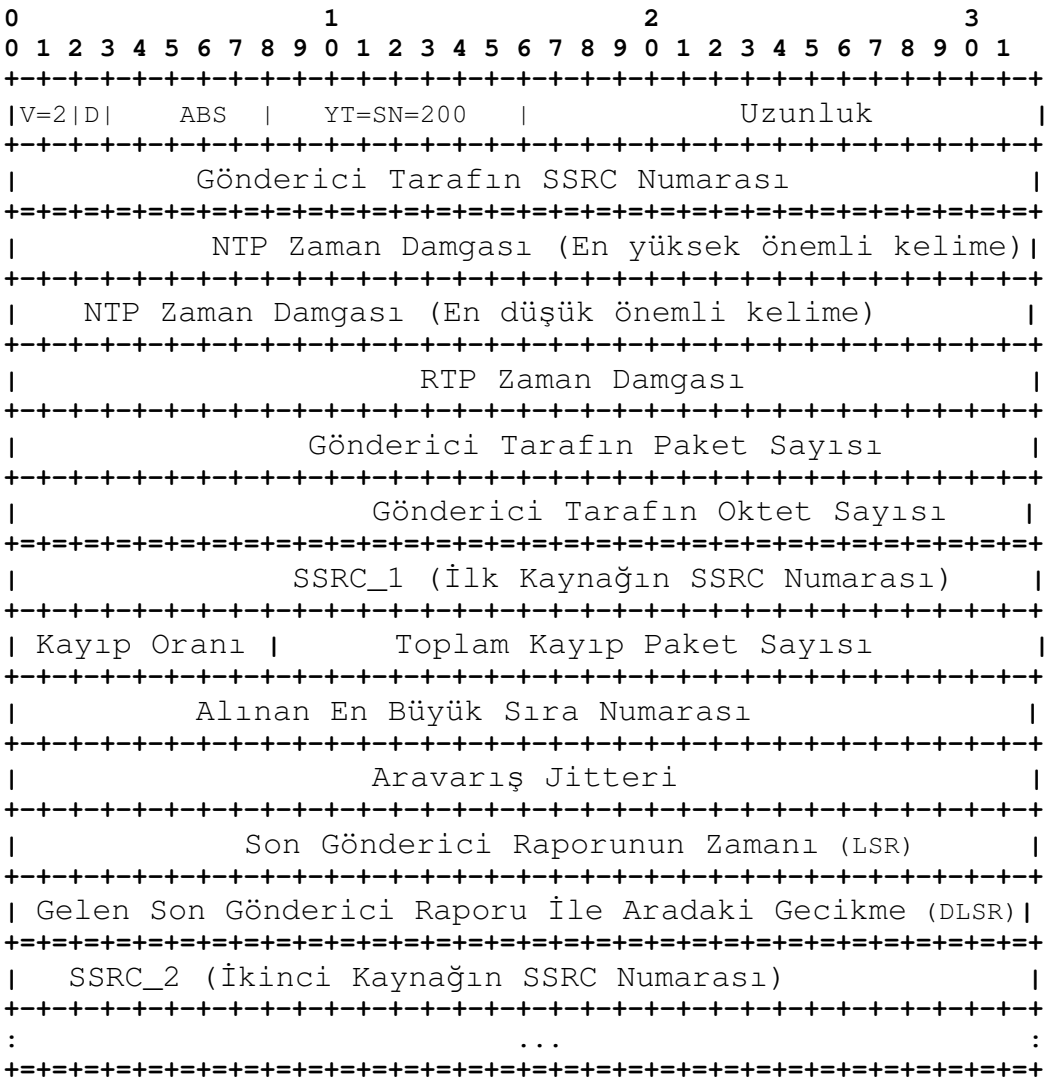
No.	Time	Source	Destination	Protocol	Info
39	2.572622	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=8, Time=2560
40	2.574993	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
41	2.604229	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
42	2.612227	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=9, Time=2880
43	2.633714	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
44	2.652707	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=10, Time=3200
45	2.663574	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
46	2.692562	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=11, Time=3520
47	2.693309	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
48	2.723170	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
49	2.732293	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=12, Time=3840
50	2.754904	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
51	2.772523	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=13, Time=4160
52	2.784764	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
53	2.812129	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=14, Time=4480
54	2.815249	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
55	2.844610	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
56	2.852107	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=15, Time=4800
57	2.874595	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
58	2.892839	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=16, Time=5120
59	2.904330	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
60	2.932319	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=17, Time=5440
61	2.934191	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
62	2.963675	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
63	2.972424	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=18, Time=5760
64	2.993161	213.243.52.202	83.66.50.228	UDP	Source port: 8042 Destination port: 20416
65	3.012404	83.66.55.245	213.243.52.202	RTP	Payload type=ITU-T G.711 PCMU, SSRC=0, Seq=19, Time=6080

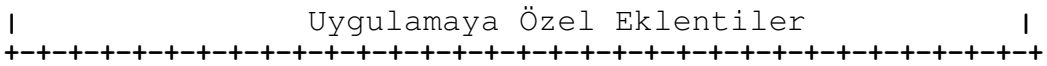
Şekil-18 RTP Mesajı Yapısı Örneği

II.1.2.2.2.3.3 RTCP Protokolü

RTCP (RTP Control Protocol), RTP protokolu ile birlikte çalışır ve oturumda yer alan tüm kullanıcılara periyodik olarak kontrol paketleri göndererek alma kalitesi (reception quality) ile ilgili bilgi sağlar. Eğer sıkışıklık oluşmaya başlamışsa, uygulama veri hızını azaltabilir.

Her RTCP paketi, uygulamaya yönelik, alıcı ve/veya verici istatistik raporlarını içerir. Bu istatistikler, gönderilen paket sayısı, kayıp paket sayısı, gecikme değişkenliği süreleri, son SR (Gönderici Raporu - Sender Report) 'dan bu yana olan gecikme, son SR zamanı gibi değerleri içerir.





Şekil-19 RTCP Mesaj Yapısı (Gönderici Raporu) [3] [23]

Sürüm (V) (2 bit): RTP sürüm numarası

Dolgu (D) (1 bit) : Bu alan 1 olarak işaretlendiğinde bazı bit ekleme oktetlerinin olduğunu gösterir.

Alıcı Blok Sayısı(RC) (5 bit): Kaç tane alıcı bloğunun mesaj içinde yer aldığını gösterir.

Paket Tipi (PT) (8 bit): Gönderici rapor mesajı için 200'e ayarlıdır.

NTP Zaman Damgası (64 bit): Sistem saatine ilişkin ifadedir. Lokal saatten bağımsız olarak NTP (Network Time Protocol) kullanır. Senkronizasyon amacıyla kullanılır.

Gönderici Paket Sayısı ve Oktet Büyüklüğü (32 bit): Alıcı tarafı kaç PDU'nun (paketin) ve kaç oktetlik enformasyonun yollandığı hakkında bilgilendirir.

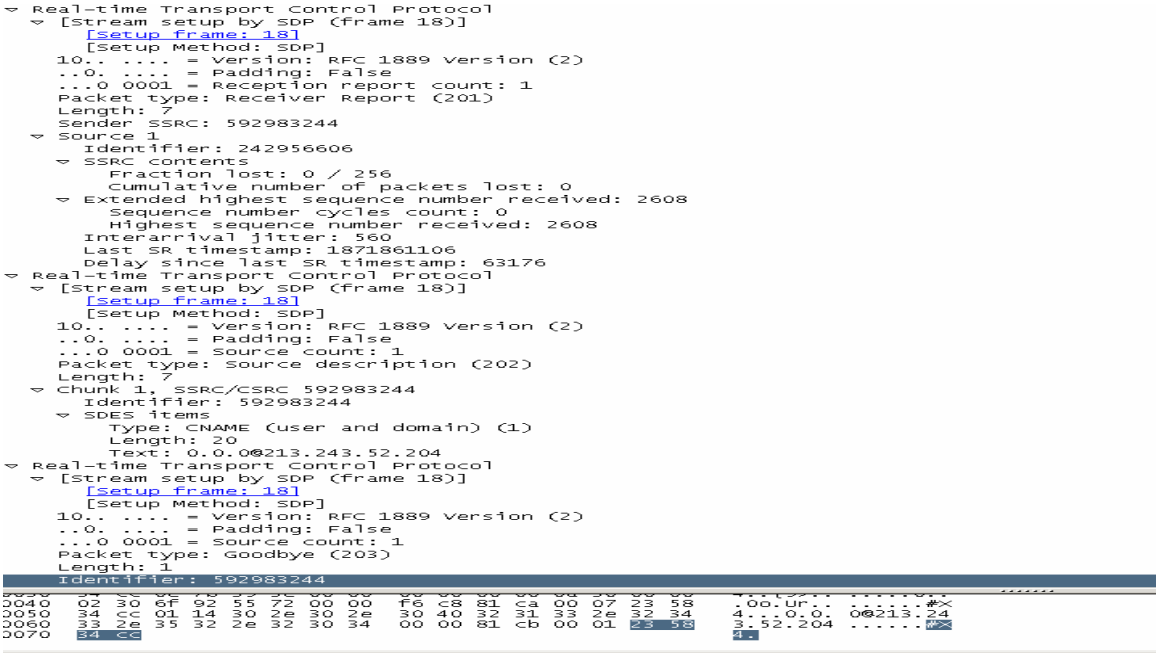
Kayıp Oranı (8 bit): Kayıp paketlerin gelmesi düşünülen paketlere oranıdır.

Toplam Kayıp Paket Sayısı (24 bit): Algılamanın SSRC_n adlı kaynaktan çıkan toplam kayıp paket sayısı veren ifadedir.

Alınan En Büyük Dizi Numarası (32 bit): SSRC_n nolu kaynaktan alınan RTP paketlerin en büyük dizi numarasıdır.

Arageliş Jitteri (32 bit): Paketlerin gelişleri arasındaki zaman varyasyonlarının zaman damgası birimleri cinsinden ifadesidir.

Aşağıda, yukarıda mesaj formatı verilen RTCP gönderici raporunun paket çıktısı yer almaktadır.



Şekil-20 RTCP Mesajı

RTCP protkolünün temel işlevi veri dağıtımının kalitesi hakkında geri besleme yapmaktır. Bu geri besleme adaptif kodlama kontrolü için kullanılabilir. Burada geri besleme işlevi alıcı ve verici raporlarıyla elde edilir. Yine aynı şekilde RTCP bir oturumdaki bütün katılımcıların kaydını tutar. Herbir kaynağa ait, CNAME (Takma Ad - Canonical Name) denilen taşıma katmanı tanımlayıcılarını ve de eş zamanlayıcı kaynak tanımlayıcısını taşıyarak bu işlevi yerine getirir Bir katılımcı oturumu terkettiğinde, RTCP çıkış mesajı gönderilir.

II.1.2.2.2.4 IPv6 üzerinden SIP Mesaj Örnekleri

Aşağıda IPv6 üzerinden yapılacak olan bir SIP çağrısının INVITE (Davet) mesajı örneği ve açıklaması yer almaktadır. [24]

INVITE sip:user@[2001:db8::10] SIP/2.0

"Bu satırda, yapılan davet ile birlikte, yöntem türü ve SIP sürümü belirtilmektedir."

To: sip:user@[2001:db8::10]

"Davet edilen kullanıcı adres bilgisi yer almaktadır bu satırda"

From: sip:user@example.com;tag=81x2

"Daveti başlatan kullanıcı bilgisi bu satırda yer almaktadır"

Via:SIP/2.0/UDP [2001:db8::9:1];branch=z9hG4bKas3-111

"Bir önceki adres atlama noktası belirtilmektedir."

Call-ID: SSG95599055239970770@hlau_4100

"Yapılan çağrının belirteci belirtilmektedir."

Contact: "Caller" <sip:caller@[2001:db8::1]>

“Kontak bilgisi verilmekte bu satırda”

CSeq: 8612 INVITE

« İletimi tanımlayan komut dizisi, mesajın tipi belirtilmekte, yapılan mesaj bir davet mesaj »

Content-Type: application/sdp

« Bu davet mesajındaki gövde türü belitilmektedir. Bu mesaj örneğinde SDP gözükmektedir. »

Content-Length: 268

« Mesajın içeriğinde yer alan gövde deki byte sayısı belirtilmektedir bu satırda »

« Aşağıdaki satırlar tamamen SIP gövde mesajlarının içeriğini göstermektedir. »

v=0

«Burada SDP sürümü gösterilmektedir. »

o=assistant 971731711378798081 0 IN IP6 2001:db8::20

“Bu satırda , oturumun sahibi,oturum belirteci, oturum sürümü, ve adres belirtilmektedir.”

s=Live video feed for today's meeting

“yapılan çağrının, oluşturulan oturumun konusu belirtilmektedir.”

c=IN IP6 2001:db8::1

“Yapılan çağrının bağlantı bilgisi verilmektedir bu satırda”

“Aşağıda ise ortam ile ilgili olarak; tür, port, çağrıyı başlatan tarafın kullanmak istediği-isteyeceği olsaı format biçimleri tanımlanmaktadır.”

t=3338481189 3370017201
m=audio 6000 RTP/AVP 2
a=rtpmap:2 G726-32/8000
m=video 6024 RTP/AVP 107
a=rtpmap:107 H263-1998/90000

BÖLÜM III. TEZ ÇALIŞMALARI

III.1. Araştırma Araçları

Bu tez çalışmasında VoIP protokollerini uygulama , RFC lerdeki bazı teorideki özelliklerini uygulamada görmek ve sonuçlarını değerlendirmek için örnek senaryolar ile oluşturulan test ortamında uygulamaya konuldu.

Öncelikli olarak Internet Protokol Sürüm 6 altyapısı kurularak bu ağ üzerinde bazı protokoller çalıştırılarak paket çıktıları gözlemlendi. Bu uygulama için üzerinde Internet Protokol Sürüm 6 etkinleştirilmiş Windows tabanlı serverlar ile yine IPv6 üzerinde çalışan Linux tabanlı bir server ve bunun üzerinde IPv6 destekli BIND DNS Server hazırlanarak ilgili örnek test senaryolarında kullanılmıştır.

VoIP uygulamaları için günümüzde yoğunlukla kullanılan iki protocol olan H.323 ve SIP protocol uygulamaları test ortamları oluşturulmuş ve bunların sonuçları değerlendirilmiştir. Bu örnek senaryolar için oluşturulan test ortamında;

SIP&H.323 Server :

Nextone SBC (Session Border Controller): Tüm çağrıların kontrol altında tutulduğu, arama kayıtlarının oluşturulmasına olanak veren yönlendirme cihazı-programı.

Voice Gateway (Ses Yönlendiricileri):

1-) Linksys Phone Adapter with 2 Ports for Voice-over-IP
Cisco firmasının üretmiş olduğu 2 portlu Ses yönlendirici cihazı bazı testlerde kullanıldı. Bu cihazdan VoIP protokollerinden sadece SIP protokolünü desteklediği için SIP protokol testlerinde yararlanıldı.
2-) WellGate 3504A modeli, 4 port SIP&H.323 destekli.

3-) Cisco IPPhone 7912 modeli, 1 port SIP destekli.

IPv6 platformu için kullanılan araçlar :

1-) Windows Vista, 2000 Server ve XP ile Linux Cent-OS İşletim Sistemleri.

2-) Cisco 2811 Serisi Yönlendirici.

3-) Cisco Catalyst 2948 Serisi Switch araçları kullanılmıştır.

III.2. Yapılan Çalışmalar

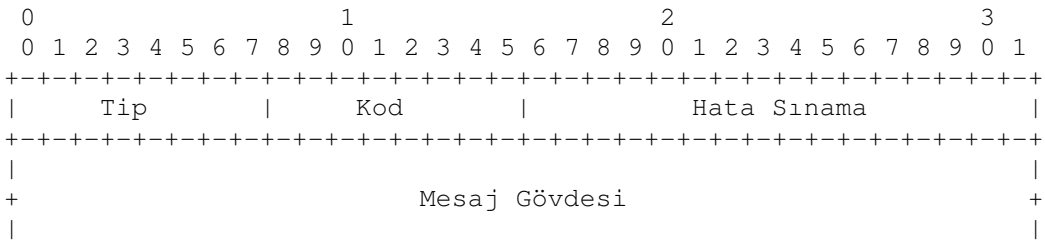
Tez çalışmasının uygulamaları bu bölümde gösterilmektedir.

III.2.1. IPv6 Uygulamaları

Bu bölümde IPv6 ağı üzerinde bazı örnek uygulamalar protokol bazında yapılmış ve bunlar ile ilgili paket yapıları gösterilmeye çalışılmıştır.

III.2.1.1. IPv6 Üzerinden ICMP Uygulaması

IP' nin işlerini kontrol etmesine ve yönetmesine yardımcı olan aynı zamanda TCP/IP de ki ağ katmanının bir parçası konumunda olan Internet Kontrol Mesajı Protokolü(ICMP) nin ismindeki 'kontrol mesajı' kısmı protokolün kullanım amacını bize açıklamaktadır. ICMP, daha üst bir protokolmüşcesine IP'nin temel desteğini kulanır ancak, ICMP aslında IP'nin tümleşik bir parçasıdır. [27]



Şekil-21 ICMPv6 Paket Yapısı [RFC 2463]

ICMP, görevlerini gerçekleştirmek için mesajları kullanır. Bu mesajların birçoğu en küçük IP ağında bile kullanılır. Aşağıdaki tabloda RFC 2463'teki ICMP mesajları listelenmiştir.

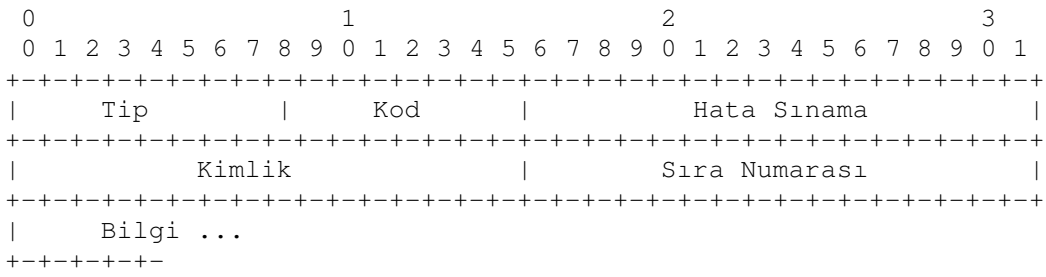
ICMPv6 Hata Mesajları:

TİP	MESAJ
1	Hedefe Erişilemiyor
2	Paket Fazla Büyük
3	Zaman Aşıldı
4	Parametre Sorunu

ICMPv6 bilgilendirme mesajları:

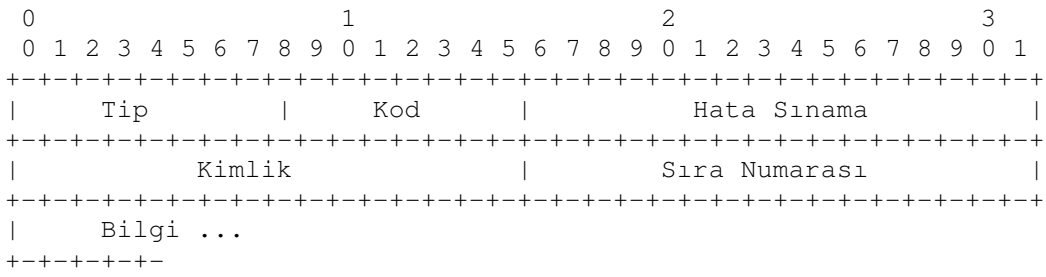
TİP	MESAJ
128	Yankı İsteği
129	Yankı Yanıtı

ICMPv6 Yankı İstek Mesajı:

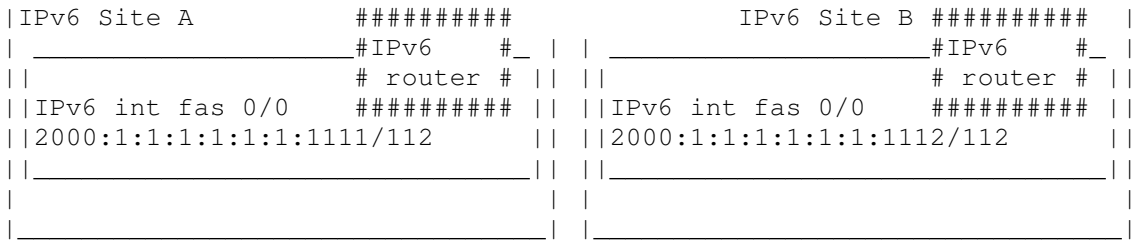


Şekil-22 ICMPv6 Yankı İstek Mesajı Yapısı [28]

ICMPv6 Yankı Yanıt Mesajı:



Şekil-23 ICMPv6 Yankı Yanıt Mesajı Yapısı [28]



Şekil-24 ICMPv6 Ping Testi

IPv6'ya üzerinden hazırlanan ağın katman üç seviyesinde çalışırlığından emin olmak için IPv6 sorgulaması yapılabilir. Bu sorgulama,hata ayıklama/sorun çözme konularında da faydalı olmaktadır.

IPv6 Site A da bulunan yönlendirici üzerinde kullanılan komut ve gönderilen yankı istek mesajı ile buna gelen yankı yanıt mesajı çıktısı aşagıda gösterilmiştir.

IPv6_Test_Router_1#ping ipv6 2000:1:1:1:1:1:1:1111

```
Source                 Destination           Protocol Info
2000:1:1:1:1:1:1:1112 2000:1:1:1:1:1:1:1111 ICMPv6   Echo request

Ethernet II, Src: 00:10:b5:3e:c1:e6, Dst: 00:10:b5:86:dd:c8
    Destination: 00:10:b5:86:dd:c8 (AcctonTe_86:dd:c8)
    Source: 00:10:b5:3e:c1:e6 (AcctonTe_3e:c1:e6)
    Type: IPv6 (0x86dd)
„Katman 2 , Veri Bağı Katmanı bilgileri yukarıdaki gibidir. Burada alıcı ve
gönderici MAC adresleri bilgisi ve tür , bu örnek için“Ipv6“ belirtilmiştir.

Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 40
    Next header: ICMPv6 (0x3a)
    Hop limit: 128
    Source address: 2000:1:1:1:1:1:1:1112
    Destination address: 2000:1:1:1:1:1:1:1111
Internet Control Message Protocol v6
    Type: 128 (Echo request)

“IPv4 te ICMP Echo Reguest (Yankı İstek) mesajı türü 8 iken IPv6 da bu
değer 128 olarak tanımlanmıştır.”

    Code: 0
```

Checksum: 0x72c8 (correct)
ID: 0x0000
Sequence: 0x0002
Data (32 bytes)

```
Source                Destination           Protocol Info
2000:1:1:1:1:1:1:1111 2000:1:1:1:1:1:1:1112 ICMPv6   Echo reply

Ethernet II, Src: 00:10:b5:86:dd:c8, Dst: 00:10:b5:3e:c1:e6
    Destination: 00:10:b5:3e:c1:e6 (AcctonTe_3e:c1:e6)
    Source: 00:10:b5:86:dd:c8 (AcctonTe_86:dd:c8)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 40
    Next header: ICMPv6 (0x3a)
    Hop limit: 128
    Source address: 2000:1:1:1:1:1:1:1111
    Destination address: 2000:1:1:1:1:1:1:1112
```

Internet Control Message Protocol v6
Type: 129 (Echo reply)

"IPv4 te ICMP Echo Reply (Yankı Yanıt) mesajı türü 0 iken IPv6 da bu değer 129 olarak tanımlanmıştır."

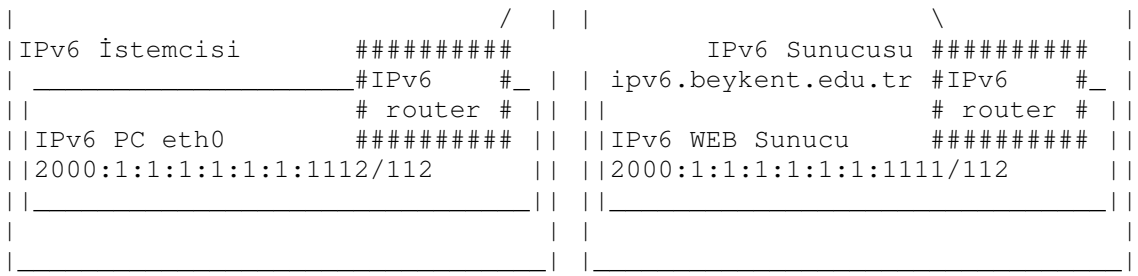
Code: 0
Checksum: 0x71c8 (correct)
ID: 0x0000
Sequence: 0x0002
Data (32 bytes)

ICMPv4 ve ICMPv6 Mesaj Karşılaştırması

ICMPv4 Mesajları	ICMPv6 Eşdeğeri
Alıcı Ulaşılamaz - Ağ ulaşılamaz……	Alıcı Ulaşılamaz- Alıcıya doğru yönlendirme yok
Alıcı Ulaşılamaz - Protokol ulaşılamaz…….	Parametre Problemi- Tanınmayan Sonraki Başlık Alanı
Alıcı Ulaşılamaz - Port Ulaşılamaz…….	Alıcı ulaşılamaz-Port ulaşılamaz
Alıcı Ulaşılamaz - Parçalamaya ihtiyaç var..	Paket çok büyük
Zaman Aşıldı - TTL Zaman Aşımı	Zaman Aşıldı - Atlama Limiti Aşıldı
Parametre Problemi	Parametre Problemİ
Yeniden yönlendirme	Komşu Saptama Yeniden Yönlendirme Mesajı

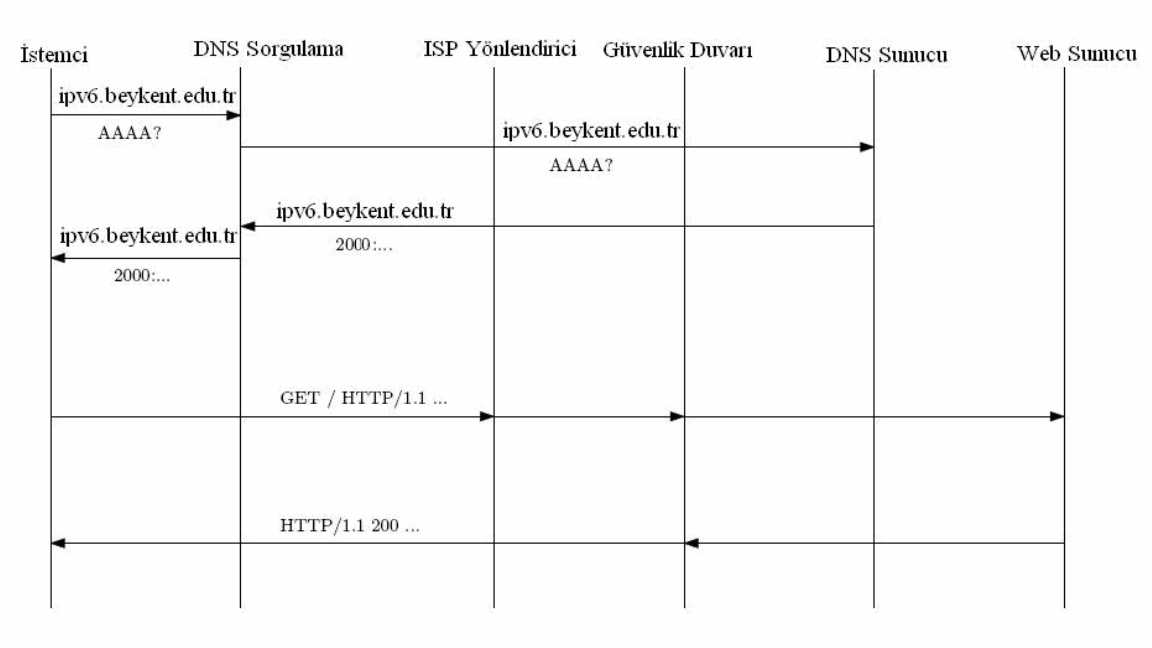
Şekil-25 IPv4-IPv6 Mesaj Karşılaştırılması

III.2.1.2. IPv6 Üzerinden HTTP Uygulaması



Şekil-26 HTTPv6

IPv6 istemcisi bir http (TCP Port 80) isteğinde bulunur. IPv6 Sunucusu bu isteğe yanıt döner.



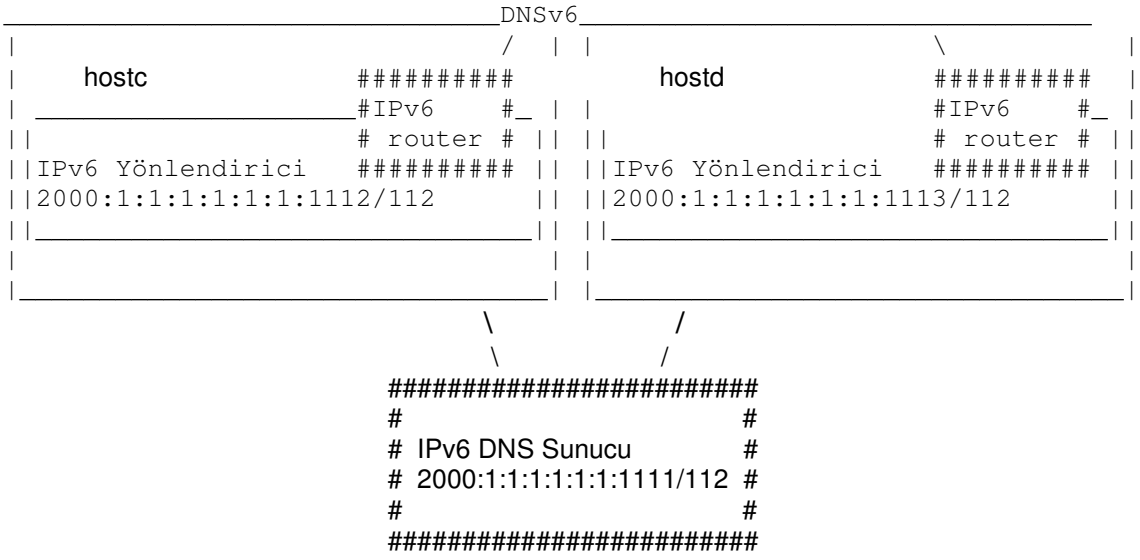
Şekil-27 HTTPv6 Akış Diagramı

```
Source                Destination           Protocol Info
2000:1:1:1:1:1:1:1112 2000:1:1:1:1:1:1:1111 TCP      49179 > http [SYN]
Seq=0 Ack=0 Win=8192 Len=0 MSS=1440 WS=8

Ethernet II, Src: 00:10:b5:3e:c1:e6, Dst: 00:10:b5:86:dd:c8
    Destination: 00:10:b5:86:dd:c8 (AcctonTe_86:dd:c8)
    Source: 00:10:b5:3e:c1:e6 (AcctonTe_3e:c1:e6)
    Tip: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: TCP (0x06)
```

```
    Hop limit: 128
    Source address: 2000:1:1:1:1:1:1:1112
    Destination address: 2000:1:1:1:1:1:1:1111
Transmission Control Protocol, Src Port: 49179 (49179), Dst Port: http (80),
Seq: 0, Ack: 0, Len: 0
    Source port: 49179 (49179)
    Destination port: http (80)
    Sequence number: 0    (relative sequence number)
    Header length: 32 bytes
    Flags: 0x0002 (SYN)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...0 .... = Acknowledgment: Not set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..1. = Syn: Set
        .... ...0 = Fin: Not set
    Window size: 8192
    Checksum: 0x5055 (correct)
    Options: (12 bytes)
        Maximum segment size: 1440 bytes
        Window scale: 8 (multiply by 256)
        NOP
        NOP
        NOP
        SACK permitted


Kaynak                Hedef                 Protokol Bilgi
2000:1:1:1:1:1:1:1111 2000:1:1:1:1:1:1:1112 TCP      http > 49179 [SYN,
ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=8

Ethernet II, Src: 00:10:b5:86:dd:c8, Dst: 00:10:b5:3e:c1:e6
    Hedef: 00:10:b5:3e:c1:e6 (AcctonTe_3e:c1:e6)
    Kaynak: 00:10:b5:86:dd:c8 (AcctonTe_86:dd:c8)
    Tip: IPv6 (0x86dd)
Internet Protokol Sürüm 6
    Sürüm: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: TCP (0x06)
    Hop limit: 128
    Source address: 2000:1:1:1:1:1:1:1111
    Destination address: 2000:1:1:1:1:1:1:1112
Transmission Control Protocol, Src Port: http (80), Dst Port: 49179 (49179),
Seq: 0, Ack: 1, Len: 0
    Kaynak port: http (80)
    Hedef port: 49179 (49179)
    Sıra numarası: 0    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0012 (SYN, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..1. = Syn: Set
        .... ...0 = Fin: Not set
    Window size: 8192
    Checksum: 0xcbe4 (correct)
    Options: (12 bytes)
        Maximum segment size: 1440 bytes
        Window scale: 8 (multiply by 256)
        NOP
        NOP
        NOP
        SACK permitted
    SEQ/ACK analysis
        This is an ACK to the segment in frame: 1
        The RTT to ACK the segment was: 0.000171000 seconds
```

III.2.1.3. IPv6 Üzerinden DNS Uygulaması



Şekil-28 DNSv6

Yukarıda senaryo da ana makine adlarını IPv6 adresleri olarak çözümlemek için Etki Alanı Ad Sistemi (DNS) sunucusu kullanılmıştır. IPv6 adresiyle yapılandırılan yönlendirici, DNS sunucusunun adresiyle yapılandırıldığından, DNS ad sorgularını çözümlenmek üzere DNS Sunucuya gönderir. DNS sunucusunda saklanan AAAA (quad-A) kaynakları, ana makine adından IPv6 adresine eşleme sağlar.

Etki Alanı Ad Sistemi (DNS) IPv6 ana makine kayıtlarının (AAAA veya dört A kaynak kayıtları olarak bilinir ve RFC 1886 "DNS Extensions to support IP version 6" [IP sürüm 6'yı destekleyecek DNS Uzantıları] Internet taslağında tanımlanmıştır)

IPv6 kaynak ve hedef ana makinelerin 128 bitlik IPv6 adresiyle çalışmak üzere tasarlanmıştır ancak bilgisayar kullanıcılarının iletişim kurmak istedikleri bilgisayarların IPv6 adreslerini kullanmak ve hatırlamakta zorluk çekmeleri olasıdır. Bunun yerine hatırlanması daha kolay benzersiz adlar kullanılabilir.

Ana makine adı çözümleme, ana makinenin adını başarıyla bir IPv6 adresi ile eşlemek anlamına gelir. Ana makine adı, bir IPv6 düğümünü IPv6 ana makinesi olarak tanımlamak için IPv6 düğümüne atanmış bir diğer addır. Ana makine adı en çok 255 karakter uzunluğunda olabilir ve alfabetik karakterlerden başka, sayısal karakterler, tireler ve noktalar içerebilir. Aynı ana makineye birden çok ana makine adı atanabilir.

Windows Sockets (Winsock) programları bağlanmak istediğiniz hedef için iki değerden birini kullanabilir: IPv6 adresini veya ana makine adını. IPv6 adresi belirtilmişse ad çözümlemesine gerek yoktur. Ana makine adı belirtilmişse, bir kaynakla IPv6 tabanlı iletişime geçilmeden önce ana bilgisayar adı bir IPv6 adresine dönüştürülmelidir.

Etki alanı adları, yapılandırılmış bir DNS sunucusuna DNS ad sorguları gönderilerek çözümlenir. DNS sunucusu etki alanı adından IPv6 adresine eşleme kayıtları saklar veya başka DNS sunucularının kayıtlarına sahiptir. DNS sunucusu sorgulanan etki alanı adını bir IPv6 adresine dönüştürür ve sonuçları döndürür.

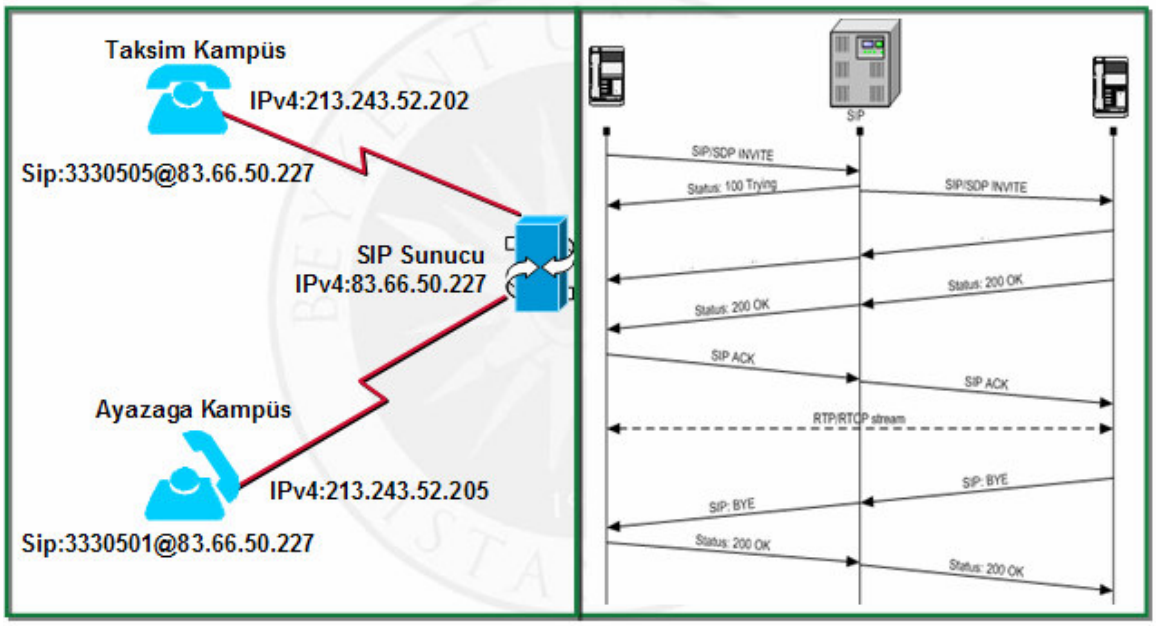
Aşağıda IPv6 çalışan bir DNS Sunucusuna girilen kayıtlar gösterilmektedir.

```
$TTL 86400

@       IN      SOA     localhost.      ecan.dol.com.tr. (
                        2006080201      ; serial number YYMMDDNN
                        28800           ; Refresh
                        7200            ; Retry
                        864000          ; Expire
                        86400           ; Min TTL
                        )
```

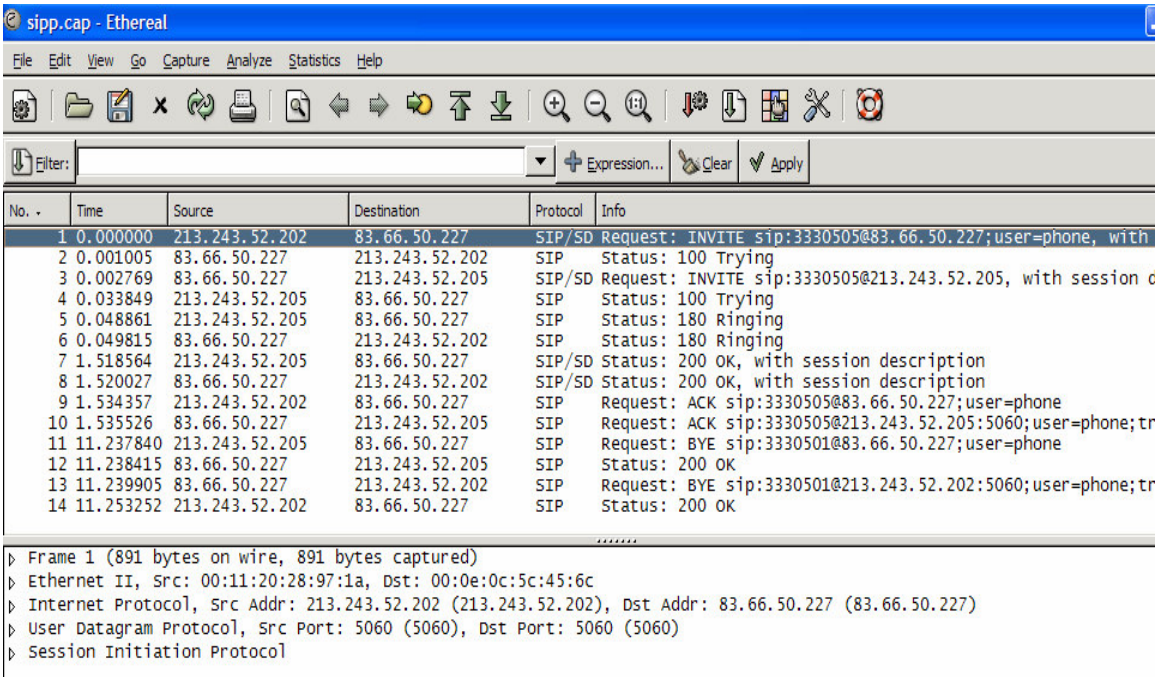
```
            NS      localhost.
            NS      localhost.
www         A       213.243.1.1
hosta       A       213.243.52.204
hostb       A       213.243.57.62
hostc       AAAA    2000:1:1:1:1:1:1:1112
hostd       AAAA    2000:1:1:1:1:1:1:1113
_sip._udp.hostc.ender.com       43200 IN SRV 0 0 5060   hostc.ender.com
_sip._udp.hostd.ender.com       43200 IN SRV 0 0 5060   hostd.ender.com
_sips._tcp.hostc.ender.com      43200 IN SRV 0 0 5060   hostc.ender.com
_sips._tcp.hostd.ender.com      43200 IN SRV 0 0 5060   hostd.ender.com
_sip._tcp.hostc.ender.com       43200 IN SRV 0 0 5060   hostc.ender.com
_sip._tcp.hostd.ender.com       43200 IN SRV 0 0 5060   hostd.ender.com
$ORIGIN ender.com.
```

III.2.2. VoIP Uygulamaları

III.2.2.1. SIP'den SIP'e Çağrı Uygulaması



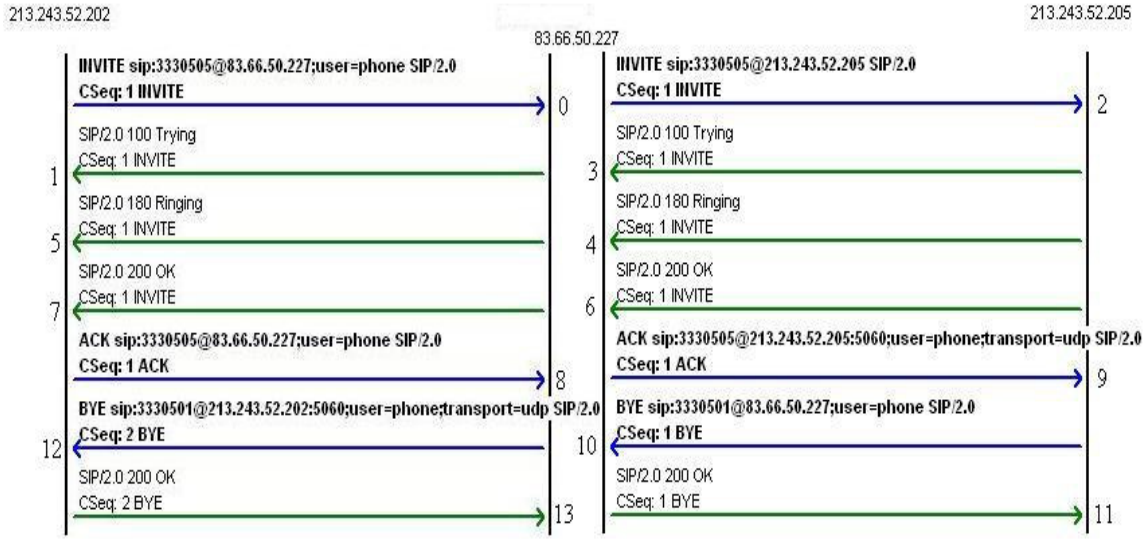
Şekil-29 SIP Çağrı Senaryosu Örneği



Şekil-30 SIP Çağrı Akışı Çıktısı

- SIP'in çağrı kontrol mesajlarının geçirilebileceği güvenilir bir kanal açmak için INVITE ve ACK mesajları bulunmaktadır.

- SIP kullanılacak codec uzlaşması (negotiation) için yani o oturumda hangi codec'in kullanılacağına karar vermek için Session Description Protocol (SDP)'yi kullanmaktadır.

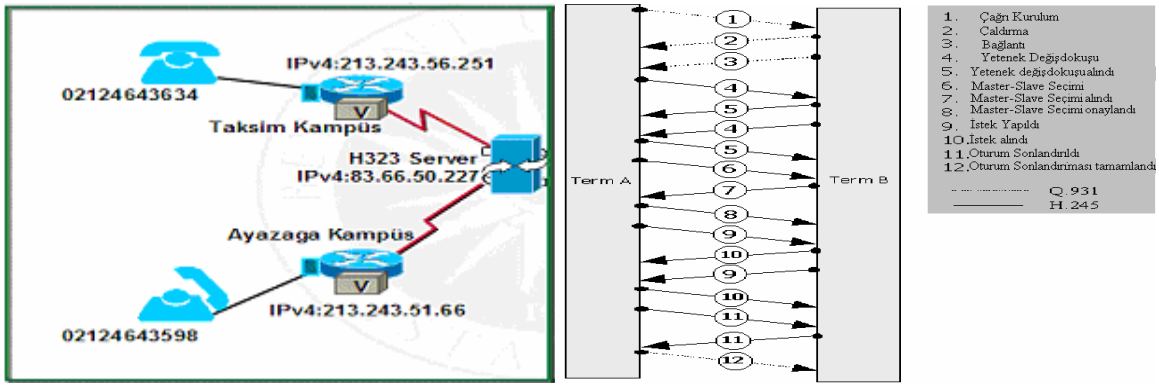


Şekil-31 SIP Çağrı Akışı Örneği

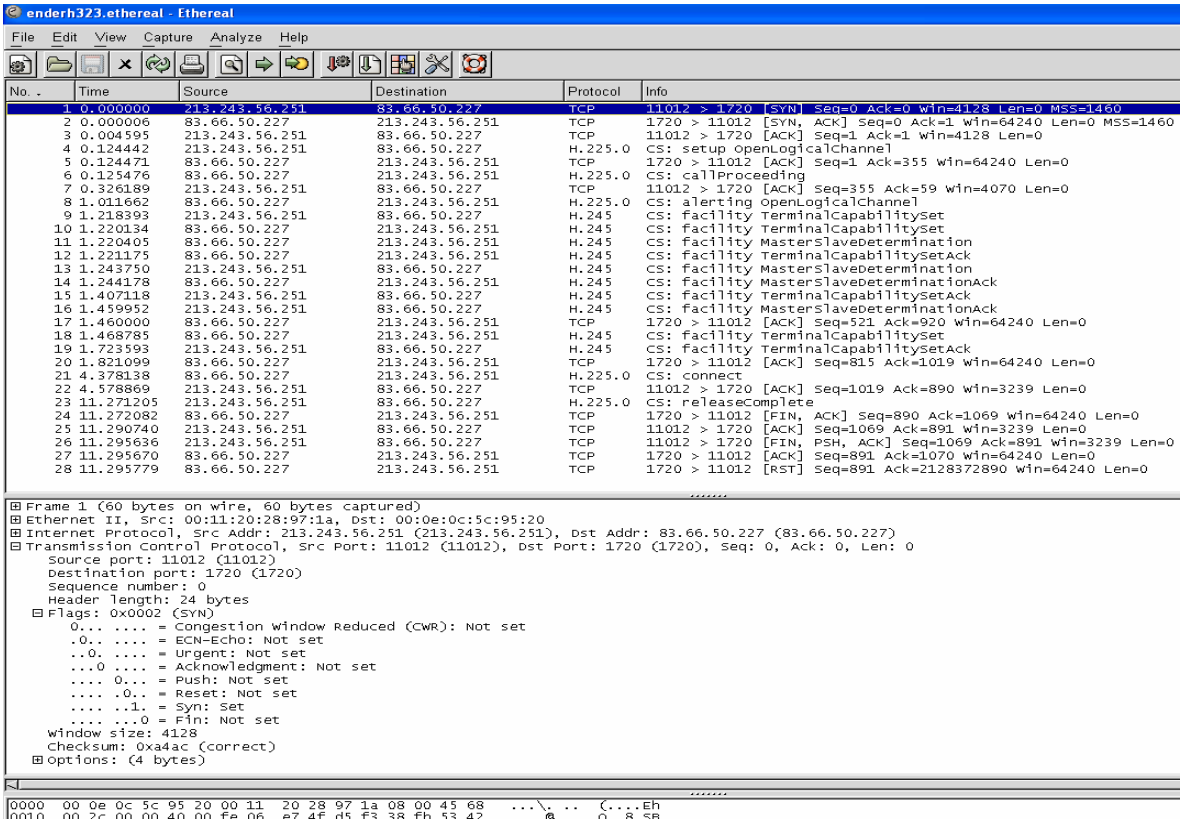
Adım	İşlem	Açıklama
Adım 0	INVITE	Aranan numara bilgisi sip sunucuya iletilir.
Adım 1	100 Trying	Sip sunucu isteği işleme koyduğuna dair arayana mesaj gönderir.
Adım 2	INVITE	Sip sunucu aranan numara bilgisini aranan noktaya iletir.
Adım 3	100 Trying	IP Telefon isteiği işleme koyduğuna dair mesaj gönderir
Adım 4	180 Ringing	IP Telefon zil sesini bilgisini sunucuya iletir.
Adım 5	180 Ringing	Sunucu zil sesi bilgisini arayan noktaya iletir.
Adım 6	200 OK	Aranan taraf telefonu açtı bilgisini sunucuya iletir.
Adım 7	200 OK	Sunucu telefon açıldı bilgisini arayan tarafa iletir.
Adım 8	ACK	Arayan sunucuya telefon açıldı bilgisinin kendisine ulaştığını onaylama bilgisini iletir.
Adım 9	ACK	Sunucu aranana telefon açıldı bilgisinin kendisine ulaştığını onaylama bilgisini iletir.
Adım 10	BYE	Aranan telefon kapandı bilgisini sunucuya iletir
Adım 11	200 OK	Sunuc kapandı bilgisinin kendine ulaştığı bilgisini aranana iletir.
Adım 12	BYE	Sunucu arayana telefon kapandı bilgisini iletir.
Adım 13	200 OK	Arayan sunucuya telefon kapandı bilgisinin kendine ulaştığını iletir.

Tablo -2 SIP'den SIP'e Çağrı Adımları

III.2.2.2. H.323'den H.323'e Çağrı Uygulaması



Şekil-32 H.323 Senaryosu ve Çağrı Akışı



Şekil-33 H.323 Çağrı Akışı Çıktısı

Adım	İşlem	Açıklama
Adım 0	SETUP	02124643634 çağrı kurulumu için istekte bulunur 02124643598 e
Adım 1	ALERTING	02124643598 aldığı istekten sonra zil tonu gönderir.
Adım 2	CONNECT	02124643598 gönderdiği zil tonundan sonra bağlantı kurulur.
Adım 3	TERMCAPSET	Bu adımda ses geçitleri arasında yetenek değişdokuşları yapılır.
Adım 4	TERMCAPACK	Ses geçitleri arasındaki yetenek değişdokuşu onaylaması yapılır.
Adım 5	MSDET	Bu adımda ses geçitleri arasında master-slave ayarlanması işlemi yapılır.
Adım 6	MSDETACK	Master-Slave seçimi onaylanması gerçekleştirilir bu adımda.
Adım 7	MSDETCONFIRM	Master ses geçiti doğrulanması yapılır.
Adım 8	OPENREQ	Ses kanalı açılır.
Adım 9	OPENACK	Açılan ses kanalından ses iletişimi başlar.
Adım 10	ENDSESSION	Açılan oturum kapatılması isteği döner burada.
Adım 11	RELASECOMPLETE	Oturum sonlandırılır bu son adımda.

Tablo -3 H.323'den H.323'e Çağrı Adımları

BÖLÜM IV. SONUÇLAR VE ÖNERİLER

IPv6 henüz tam anlamıyla kullanıcı dostu arabirimi ile karşımıza çıkmamaktadır. Şu an için güncel olarak kullanılan tüm işletim sistemleri için ek paketler halinde desteklenmektedir. Ancak yeni yeni tümleşik olarak gelen IPv6 desteği gün geçtikçe uygulamalarda kullanılabilecektir. Microsoft Vista işletim sisteminde ilk kez grafik arabirim üzerinden IPv6 adresleri set edilebilmekte buna olanak sağlanabilmektedir. Bunun yanında , henüz sınama aşamasında olan bu işletim sistemi dışında diğer işletim sistemlerinde bazı Linux işletim sistemleri uyarlamaları hariç bu destek fazlaca sunulmamaktadır. Bu durum VoIP hizmeti için kullanılan Ses Yönlendirici cihazlarında da aynı durumdadır. Yani hali hazirda kullanılan ses yönlendiricilerinin hemen hemen tümünde IPv6 desteği henüz sunulmamaktadır. Bu durum IPv6 ya geçişin hızlanacağı önümüzdeki dönemde VoIP servislerininde günden güne arttığı bu ortamda düzenlenmesi gereken, güncelleşme ihtiyacı doğuran bir durum olarak görünmektedir.

Devre Anahtarlama mantığıyla çalışan PSTN ağından , Paket anahtarlama mantığı ile çalışan VoIP servislerine geçişin çok hızlı yaşandığı günümüzde, VoIP ile gelen çoklu ortam hizmetlerinin ve kişiselleştirilmiş hizmetlerin sunulması, ilerleyen teknoloji ile birlikte devre anahtarlamalı şebekelerde kullanılan ses'in yanında, paket anahtarlamalı yapıya geçişten sonra ses'in yanında görüntü ve bilgi'nin de taşınması ile beraber uç birim cihazları –cep telefonu vb- üzerinden televizyon yayını vb. servisler kullanılabilir hale gelmiştir.

Devre anahtarlamalı şebekeler ses temelli olduklarından açılan bir iletişim kanalından sadece ses taşındığından servis kalitesi paket anahtarlama mantığı ile çalışan VoIP'e göre daha üst seviyelerdedir. Ve bu tutarlı bir servis kalitesi güvencesi verebilmektedir. IP tabanlı ağlarda oluşturulan ses ağları üzerinden taşınan ses için böyle bir güvence ve kalite söz konusu değildir henüz. Ancak kısa vadede gerçeklenebilir de gözükmemektedir. Zira IP ağlarında , uçtan uca ses taşımak üzere kurulmuş olan ses iletim kanallarında olmayan bazı dezavantajlar –paket kayıpları, sıkışıklık, gecikme vb- IPv6'da bazı iyileştirmeler yapılmasına rağmen IP' nin doğası gereği her zaman olacak gibi gözükmektedir.

IPv6 ile güvenlik mekanizmalarının iyileştirilmesi, VoIP güvenliğini de olumlu yönde etkileyecektir. Bunun yanında protokol bazında güvenlik açıklarının bulunuyor olması paket anahtarlamalı çalışan ağlarda hala bir tehdit oluşturabilmektedir. Devre anahtarlamalı yani geleneksel ses hizmeti (PSTN) kullanılan ağlarda ilgili iletişim kanalına sızıp mevcut ses görüşmesini dinlemek teknik anlamda çok basit iken bu paket anahtarlamalı ağlarda, kişisel bazlı güvenlik önlemleri ile daha zorlaştırılmış olacaktır. Ancak ses verilerinin IP ağlarında, IP paketleri içerisinde kapsüllenerek gönderiliyor olması ve bu paketlerinde internet ortamında farklı yollar ve birden fazla noktadan geçişler kullanması güvenlik anlamında iyi bir dizayn ve ön çalışma yapılması gerekliliğini ortaya koymaktadır. Zira ses verilerinin içinde bulunduğu ses paketlerinin ağ'dan alınıp, içeriğinin değiştirilip farklı bir ses verisi olarak tekrar yollanması durumu olabilecek bir senaryodur. Bu ve benzeri durumlar yeni nesil IP teknolojisi olan IPv6'nın kendisi ile beraber getirdiği güvenlik mekanizmaları ile daha aza indirgenebilecektir.

Ses hizmetleri ile IP nin aynı yapı üzerinde taşınıyor olması tek bir güvenlik açığının tüm sistem üzerinde yani hem ses hemde veri üzerinde kayıplara yol açabilecek durumlar oluşturabilecektir. Veri hattına gelebilecek bir saldırı ses hizmetini de aksatabilecektir.

Şu an'a kadar olan gelişmeler ile birlikte, IPv6 ve VoIP servislerinin hızla ilerlemesi her ne kadar her iki teknolojinin birbirinden bağımsız yol kat etmelerine rağmen birlikte çalışabilirlik konusunda hala eksiklikler bulunmaktadır. Tez çalışması süresince hem yazılımsal hem de donanımsal olarak Softphone ve hardphone olarak çeşitli üretici firmaların cihazları ve programları incelenmiş ancak IPv4 üzerinde çalışmaları ile birlikte IPv6 desteği henüz tam olarak yerleşmediği görülmüştür. Yönlendiriciler üzerinde ise bazı yazılım değişiklikleri ile IPv6 desteği oluşturulabilinip data servisleri için bu hizmet rahatça alınabilirken, IPv6 ile VoIP servisleri aynı platform üzerinde –donanımsal yönlendiriciler üzerinde- birbirlerini desteklemeleri henüz –incelenen ürünler içerisinde- sağlanmamıştır. İncelenen ürünlerin şu an için dünya Bilgi Teknolojileri pazarında kullanılan ağ cihazları pazarının yaklaşık %85 ine sahip olduğu düşünülecek olursa bu birlikte çalışabilirliğin şu an için mümkün olmaması bir olumsuz durum olarak dikkat çekmektedir. Bunun ile ilgili olarak bu desteğin yakın zamanda tam anlamıyla, yapılacak yazılımsal güncellemelerden sonra ve testler sonrasında sağlanabileceği bilgisi üretici firma yöneticilerinden alınmıştır.

Donanımsal olarak üretilen ses geçitleri, IP Telefonların yeterince ve kullanıcı kolaylığı açısından sağlayamadığı rahatlık, yazılımsal olarak kullanılan IP SoftPhone programları üzerinde de başarılı sonuçlar vermediği görülmüştür. Ancak değişik işletim sistemleri üzerinde, yazılan çeşitli yazılımlar sayesinde SIP protokolü kullanılarak IPv6-VoIP servisleri tüm tamamlayıcı hizmetlerini sağlayamamakla birlikte yapılan test çalışmaları sonucunda başarı ile çalıştırıldığı yapılan literatür taramalarında görülmüştür. [29]

Yeni nesil ses şebekelerinin hızla yenilendiği günümüzde IPv6 ile bu servislerin birlikte çalışırlığı için üretici firmaların başta olmak üzere bu uyarlanma üzerinde hızla çalışmaları ve bu IPv6'ya geçiş sürecinin sonucunda herhangi bir sıkışıklık ve hazırlıklık yakalanmama açısından sorun yaşamamak için ses geçitleri üzerinde yapılması gereken IPv6 desteği güncellemeleri yapılması gereği görülmüştür.

Kaynaklar:

[1] Çölkesen, R. , Efe, A. Soket Programlamada IPv4'den IPv6'ya Geçiş ve Yeni Nesil Uygulama Önerileri, Akademik Bilişim 2005/Gaziantep Üniversitesi, **(2005)**

[2] www.microsoft.com/ipv6 (Erişim tarihi: Ocak 2006)

[3] Çölkesen, R. , Efe, A. IPv6 Paketi Ek-Başlık Yapıları, Türkiye Bilişim Ansiklopedisi, İstanbul, Türkiye, **(2006)** 504-505.

[4] Sümer, O. ; Kipman, E. IPv6 Adresleme ve Başlık Yapısı, Beykent Üniversitesi, İstanbul, Türkiye **(2005)**

[5] RFC [1918]; Y. Rekhter Cisco Systems; B. Moskowitz Chrysler Corp;. D. Karrenberg RIPE NCC; G. J. de Groot RIPE NCC; E. Lear Silicon Graphics, Inc. Address Allocation for Private Internets February 1996

[6] RFC[3056]; K. Moore Connection of IPv6 Domains via IPv4 Clouds **02/2001**

[7] RFC [2373]; R. Hinden; Nokia; S. Deering,Cisco Systems IP Version 6 Addressing Architecture **07/1998**

[8] Dryburgh,L. – Hewett, J. Signalling System No.7 (SS7/C7) IP Telephony Protocol Architecture and Services, Cisco Press IndianaPolis, **2005**, USA 90-91.

[9] Çölkesen, R. - Örencik, B. Bilgisayar Haberleşmesi ve Ağ Teknolojileri, Papatya Yayıncılık, 3.Basım **2002**,Türkiye 265-266.

[10] Deva, M. Internet Üzerinden Ses Aktarımı **Mayıs,2004**

[11] RFC[4123] H. Schulzrinne; C. Agboh,SIP-H.323 Interworking Requirements **07/2005**

[12] http://www.protocols.com/pbook/h323.htm#H4501 (Erişim tarihi: Ocak 2006)

[13] http://www.protocols.com/pbook/h323.htm#H4502 (Erişim tarihi: Ocak 2006)

[14] http://www.protocols.com/pbook/h323.htm#H4503 (Erişim tarihi: Ocak 2006)

[15] http://www.protocols.com/pbook/h323.htm#H4504 (Erişim tarihi: Ocak 2006)

[16] http://www.protocols.com/pbook/h323.htm#H4505 (Erişim tarihi: Ocak 2006)

[17] http://www.protocols.com/pbook/h323.htm#H4506 (Erişim tarihi: Ocak 2006)

[18] http://www.protocols.com/pbook/h323.htm#H4507 (Erişim tarihi: Ocak 2006)

[19] http://www.protocols.com/pbook/h323.htm#H4508 (Erişim tarihi: Ocak 2006)

[20] http://www.protocols.com/pbook/h323.htm#H4509 (Erişim tarihi: Ocak 2006)

[21] http://www.protocols.com/pbook/h323.htm#H4510 (Erişim tarihi: Ocak 2006)

[22] http://www.protocols.com/pbook/h323.htm#H4511 (Erişim tarihi: Ocak 2006)

[23] Kaplan, Y. SIP www.yasinkaplan.com/docs/sip.pdf (Erişim tarihi: Şubat 2006)

[24] Next Generation Networks, Focus on the Future of Networking 17th Annual Conference, November 3, **2003** Boston, USA 227.

[25] Douskalis, B. IP Telephony The Integration of Robust VoIP Services, Prentice Hall, USA **2000,** 79-83.

[26] RFC[1889] H. Schulzrinne; GMD Fokus; S. Casner;Precept Software, Inc. ; R.Frederick; Xerox Palo Alto Research Center; V. Jacobson; Lawrence Berkeley National Laboratory, RTP: A Transport Protocol for Real-Time Applications **01/1996**

[27] Stevens,W.R. TCP/IP Illustrated Volume 1 The Protocols, Addison Wesley Longman, **1994**, USA 69.

[28] RFC [2463] A. Conta; Lucent obsoletes; S. Deering; Cisco Systems; Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification **December 1998**

[29] http://cert.v6pc.jp/sip-ipv6/px6/doc-1.1/sip-ipv6-px/index.html

(Erişim Tarihi: **Nisan 2006**)

ÖZGEÇMİŞ

28 Kasım 1977 tarihi, Adıyaman İli Kahta ilçesi doğumluyum. İlk, Orta ve Liseyi yine aynı ilçede tamamladıktan sonra, Marmara Üniversitesi, Teknik Eğitim Fakültesi, Elektronik-Bilgisayar Öğretmenliği Bölümüne kaydoldum. Bu bölümden 2003 yılında mezun olduktan sonra, Beykent Üniversitesi, Matematik-Bilgisayar Anabilim Dalında yüksek lisans eğitimine başladım. 1999 yılından beri Bilgi Teknolojileri sektöründe Ağ Mühendisi olarak çalışmaktayım.

Ender CAN