YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

İNTERNET ÜZERİNDEN YAPILAN TELEFON GÖRÜŞMELERİNİ KAYIT EDEBİLEN, ARŞİVLEYEBİLEN SİSTEM TASARIMI

Emrah GÜVEN

FBE Elektronik ve Haberleşme Müh. Anabilim dalı
Haberleşme Programında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Yrd. Doç. Dr. Ünal KÜÇÜK

İSTANBUL, 2008

İÇİNDEKİLER

KISALTMA LİSTESİ

ACF	Admission Confirm
ADPCM	Adaptive Differential PulseCode Modulation
ADSL	Asymmetric Digital Subscriber Line
ARJ	Admission Reject
ARPANET	Advanced Research Projects Agency Net
ARQ	Admission request
BB&N	Bolt Beranek and Newman
BCF	Bandwidth Confirm
BGP	Border Gateway Protocol
BRJ	Bandwidth Reject
BRQ	Bandwidth Request
CCS7	Common Channel Signalling Sistem 7
CELP	Code-excited linear prediction
DARPA	Department of Defense Advanced Research Projects Agency
DCF	Disengage Confirmation
DECS	In Direct Endpoint Call Signaling
DHCP	Dynamic Host Configuration Protocol
DM	Delta Modulation-
DNS	Domain Name System
DoD	Department of Defense
DRJ	Disengage Reject
DRQ	Disengage Request
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
FDM	Frequency division multiplexing
FFT	Fast Fourier Transform-
GCF	Gatekeeper Confirm
GKRCS	Gatekeeper Routed Call Signaling
GOSIP	Government Open System Interconnection Profile
GPL	Gateway Location Protocol
GRJ	Gatekeeper Reject
GRQ	Gatekeeper Request
HDLC	High-Level Data Link Control protocol

HTTP	Hyper Text Transfer Protocol
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Net -
IS-IS	Intermediary System to Intermediary System
ISO	The International Organization for Standardization
ITU-T	International Telecommunication Union
L2PT	Layer 2 Protocol Tunneling
LAN	Local Area Net
LAPB	Link Access Procedure Balanced
LCF	Location Confirm
LPC	Linear Predictive Coding-
LRJ	Location Reject
LRQ	Location Request
MCU	Multiple Control Units
MEGACO	Media Gateway Control Protocol (CISCO)
MGCP	Media Gateway Control Protocol
MP-MLQ	Multi-Pulse Maximum Likelihood Quantization
MSN	Microsoft Messenger Service
NAT	Network Address translation Protocol
NIC	Net Information Center
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PCM	Pulse Code Modulation
PLP	Perceptual Linear Predictive-
POTS	Plain old telephone service
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
RAS	Registration, Admission, and Status
RCF	Registration Confirm
RFC	Request For Comments

RIP	Routing Information Protocol
RRJ	Registration Reject
RRQ	Registration Request
RSVP	Resource Reservation Protocol
RTCP	Real-time Transfer Control Protocol
RTP	Real-time Transfer Protocol
SCP	Service Control Point
SGCP	Simple Gateway Control Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SS7	Signaling System 7
SSL	Secure Socket Layer
SSP	Service Switching Point
STP	Signal Transfer Point
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol
UAS	User Agent Server
UCF	Unregister Confirm
UDP	User Datagram Protocol
URJ	Unregister Reject
URQ	Unregister Request
VAD	Voice Activity Detection
VOIP	Voice Over Internet Protocol
WAN	Wide Area Network
WFQ	Weighted Fair Queuing

ŞEKİL LİSTESİ

ÇİZELGE LİSTESİ

ÖNSÖZ

Ses ve kayıt arşivleme sistemleri, pek çok alanda kullanılmaktadır. Başta güvenlik amacıyla zorunlu olarak kullanılan sistemlerin yanı sıra hizmet kalitesini arttırmak amacıyla da ses kayıt ve arşivleme işlemleri gerçekleştirilmektedir. Günümüzde pek çok işletme tarafından karma santraller üzerinden voip görüşmesi yapılmaktadır. Özellikle çağrı merkezleri, ya da bağlantı merkezleri voip kullanmaktadır. Bu nedenle büyük kapasitedeki merkezlerde bu uygulama başlamış olup, gelen aramaları kayıt edebilen yeteneğine sahip sistemlere ihtiyaç duyulmaktadır. Bu çalışma bu ihtiyaçları karşılamaya yönelik bir fikir ortaya sunmaktadır. Çalışmam sırasında bana yol gösteren ve güler yüzünü hiçbir zaman esirgemeyen sevgili hocam Yrd.Doç. Dr Ünal Küçük'e yardımlarından dolayı çok teşekkür ederim.

ÖZET

Bu çalışmada her geçen gün hayatımızda daha fazla yer alan internet üzerinden yapılan telefon görüşmelerinin kaydedilmesini ve istendiğinde açılmasını (sıkıştırılmış yapıdan PCM'e geçirme) sağlamak için bir sistemin nasıl gerçekleştirilebileceği incelenmiştir.

İnternet üzerindeki telefon konuşmaları iki ana sinyalleşme ile oluşmaktadır. Bu sinyalleşme grubundan birincisi aranan kullanıcının ağdaki yerini ve aramayı kabul edip etmeyeceğini bildiren, ses bağlantısının hangi portlar ve hangi kodlayıcılar ile yapılacağını belirleyen SIP, H323, MGCP gibi arama başlatma protokolleri, ikincisi ise seçilen kodlayıcıya göre kodlanan ses işaretlerini konuşma yapanlar arasında taşıyan RTP/RTCP gibi ses taşıma protokolleridir. Konuşma içeriği sadece RTP protokolü ile taşındığı için, ağ üzerinde gidip gelen RTP paketlerinin birer kopyası alınıp, dinleme yapmak istenilen kullanıcılara göre filtrelenip, daha sonra uygun sıraya getirilip kod çözme işlemine tabi tutulursa konuşma dinlenebilir bir formata çevirebilir. Bu çalışmada geliştirilen örnek bir ağ üzerinden telefon görüşmelerini dinlemeye yarayan sistem bu prensipten yola çıkılarak oluşturulmaya çalışılmıştır.

Anahtar Kelimeler: SIP, H323, MGCP, RTP, VOIP kodlayıcı kod çözücü , yasal dinleme

ABSTRACT

In this study, the development of a voice system, which is intended to record voice calls over Internet, has been investigated.

The voice call on Internet initializes via two different protocol groups. The first one, which is referred Signaling group can be classified as group of call initialization protocols which are responsible from defining the network address of called party, the status of called party and the port number and codec type of the call session. SIPS, H323, MGCP are the protocols, which are supposed to be in this group. The second groups of protocols like RTP/RTCP take place at the voice transmission between calling parties. Since the speech data only carried with RTP packets on the network, speech data can be captured and converted in an audible format via coding and decoding filtered packets of a particular user. The system developed in this work arises this principle.

Keywords: SIP, H323, MGCP, RTP,VOIP and codec

1. GİRİŞ

Telefon haberleşmesi dünyasında en yaygın tercih edilen haberleşme türüdür. Klasik telefon haberleşmesi yaygın olarak kullanılmaya devam ederken her geçen gün internet üzerinden yapılan telefon haberleşmesi klasik telefon haberleşmesinin yerini almaktadır.

1.1 Klasik Telefon Haberleşmesi

Sabit telefon ağları dünyadaki en eski iletim ağlarından biri olarak kurulmuş ve bugün dünya üzerinde yaklaşık 560 Milyon abonenin bağlı olduğu ağlardır. Geleneksel olarak bu ağlar, ses iletimi, faks veri iletimi ve düşük hızlardaki veri iletimini gerçekleştirmek amaçlı kurulmuşlardır.

1.1.1 Analog ve Sayısal İşaretleşme

Ses analogdur ve işlenebilmesi için öncelikle analog formdan sayısal forma dönüştürülmesi gerekir. Bir elektriksel iletim hattı sadece iki kişi arasındaki konuşmayı iletmek üzere ayrıldığı zaman önemli bir israf yapılmış olur. Çoğullama teknikleri kullanılarak bir hat üzerinden birden fazla bilgi aynı zaman içerisinde ya da sırayla iletilebilir. Analog işarette çoğullama yöntemi Frekans Bölmeli Çoğullama (Frequency Division Multiplexing – FDM); dijital işarette ise Zaman Bölmeli Çoğullama (Time Division Multiplexing – TDM)'dir. FDM çoğullama tekniğinde ses kanalının bant genişliği üzerindeki parçaların her bir ses işaretine bölüştürülür. İnsan sesinin frekans aralığı yaklaşık 4 KHz olarak kabul edilir. İletim hattı 60-108 KHz aralığındaki sinyali taşıyabildiğine göre (108-60)/4 = 12 adet ses işareti taşınabilir demektir. Mesela, 60-64KHz aralığında birinci ses işareti, 64-68 KHz ikinci v.s. şeklinde belirlenir (Harte, 2003).

1.1.2 Sayısal İşaretleşme

Sayısal işaret süreklilik ifade eden bir fonksiyonla tanımlanamaz. Kesikli ya da ayrık adıyla ifade ettiğimiz bir fonksiyonla temsil edilir. Belirli bir zaman aralığında değişmeyen değerler alır. Değişim durumu ise ani ve keskindir. Analog işaretleri sayısala dönüştürmek için geliştirilmiş olan farklı kodlama metotları vardır. Kodlama metotları üç genel sınıfa bölünebilir (Monson H. Hayes 1998):

Basit dalga formu kodlayıcıları, veri oranı 16 kbit/s üzerinde işlem yapar:

- Darbe Kodu Modülasyonu (Pulse Code Modulation-PCM)
- Uyarlanabilir Farksal darbe kod modülasyonu (Adaptive Differential PulseCode Modulation-ADPCM)
- Delta Modülasyonu (Delta Modulation-DM)

Analiz/Sentez sistemleri şunlardır:

- Ses Kodlayıcılar (Vocoders based on
- Kanal Ses Kodlayıcılar (Channel Vocoders)
- Sinüsoid Kodlayıcılar (Sinusoidal Coders)
- LPC Ses Kodlayıcılar (LPC Vocoders)
- Biçimlendirici Ses Kodlayıcılar (Formant Vocoders)
- Etkin Parametre Kodlama (Efficient Parameter Coding)
- Parçasal/Fonetik Yapıdaki (segmental/phonetic structure)

Aşağıda listelenen orta düzey sitemler, yukarıdaki iki kategorinin bazı özelliklerine sahiptir ve 4-32 kbit/s bölgesindeki geniş bir alanı kapsar.

- Alt-Bant Kodlama (Sub-band Coding)
- Kalanı basit kodlama ile doğrusal tahmin (Linear prediction with simple coding of the residual)
- Uyarlanabilir Kestirimci Kodlama (Adaptive predictive coding)
- Çoklu-sinyal LPC (Multipulse LPC)
- Kod-uyarımlı Lineer Tahmin (Code-excited linear prediction-CELP)

1.1.2.1 Basit Dalga Formu Kodlayıcıları

Dalga formu kodlayıcıları, mikrofon ve ilgili olduğu analog devrelerin ürettiği gerçek dalga şeklini kopyalamaya çalışmaktadırlar.

a. Darbe Kodu Modülasyonu (Pulse Code Modulation-PCM)

PCM işlemi dört aşamada gerçekleşir. Filtreleme ile frekans aralığı dışına düşen sinyalleri süzülür, Örnekleme metodu işaretin anlık değeri tespit edilir. Bu aşamada elde edilen sinyale PAM denir. Basamaklama ile alınan örnek 256 alternatif değerden biri ile temsil edilir, Kodlama ile de elde edilen değer, bit serisine dönüştürülür.

Analog sesi sayısal forma dönüştürmenin yolu örneklemedir. Sinyal bir saniye içerisinde birçok kere örneklenir, işaretin genliği kaydedilir. Sayısal ses, analog ses sinyallerinin bit olarak adlandırılan ikilik sistemdeki "1" ve "0" olarak işaretlenmiş halidir. PCM, 64Kbps data olarak sayısallaştırılmış ses sinyalidir. Analog ses sinyali saniyede 8000 defa örneklenir. Her bir örnek 8 bit'tir. Bu da toplamda 8bit x 8000/s=64.000 bit/s eder. Bu oran Harry Nyquist tarafından geliştirilen Nyquist teoreminden türetilmiştir (Nyquist, 1928).

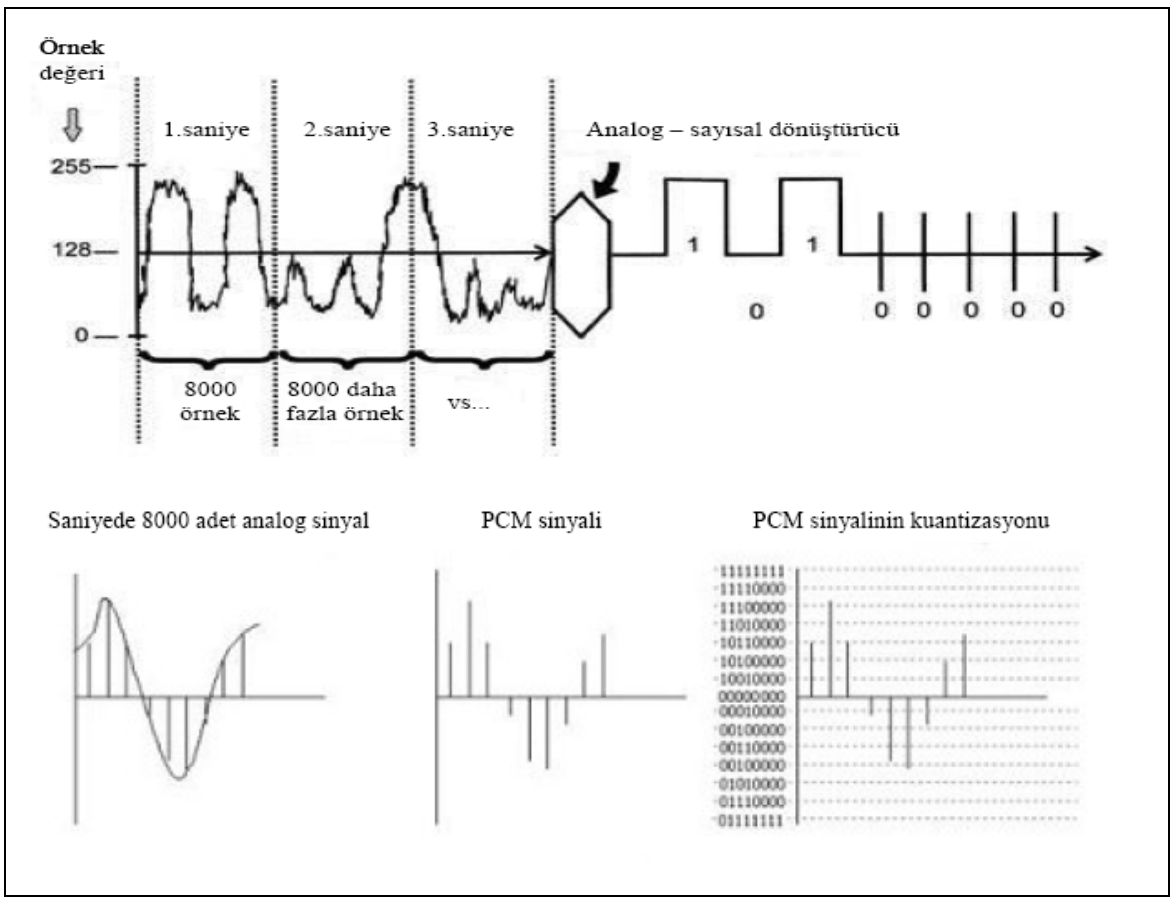
Bu teoriye göre bir sinyali yeniden ve bozulmasız olarak elde edebilmek için N tane örnek

almak gerekir. N ise aşağıdaki formülden bulunabilir:

N = 2 x sinyal bant genişliği = 2 x 4000 = 8000

Saniyede 8000 örnek yeterli bir değer olmaktadır. Bu 125 mikro saniyede bir örnek alınması anlamına gelir. Sesin analog seviyeleri 255 adet sayısal seviyeye dönüştürülür . 255 ayrık sayısal seviye 8 bitlik veri blokları ile sağlanabilir (Monson H. Hayes 1998).

Dolayısıyla bir saniyelik ses iletimi için, 8000 x 8 = 64.000 bps bir bant-genişliğine ihtiyaç duyulmaktadır. PCM aşamaları Şekil 1-1 Analog ses sinyalinin PCM'le sayısallaşmasında gösterilmiştir (Monson H. Hayes 1998).



Şekil 1-1 Analog ses sinyalinin PCM'le sayısallaşması (Monson H. Hayes 1998)

Örnekleme sonrasında dönüştürücü ortalama değere sahip sinyalleri ortamdan ayırarak kalanları örnekleme değerine uygun biçimde yuvarlar. Sinyalin karşılığı olan değer bir tam sayıya denk gelmiyorsa, dönüştürücü bu değeri en yakın üst veya alt değere yuvarlar. Bu işleme basamaklama (quantization) işlemi adı verilir.

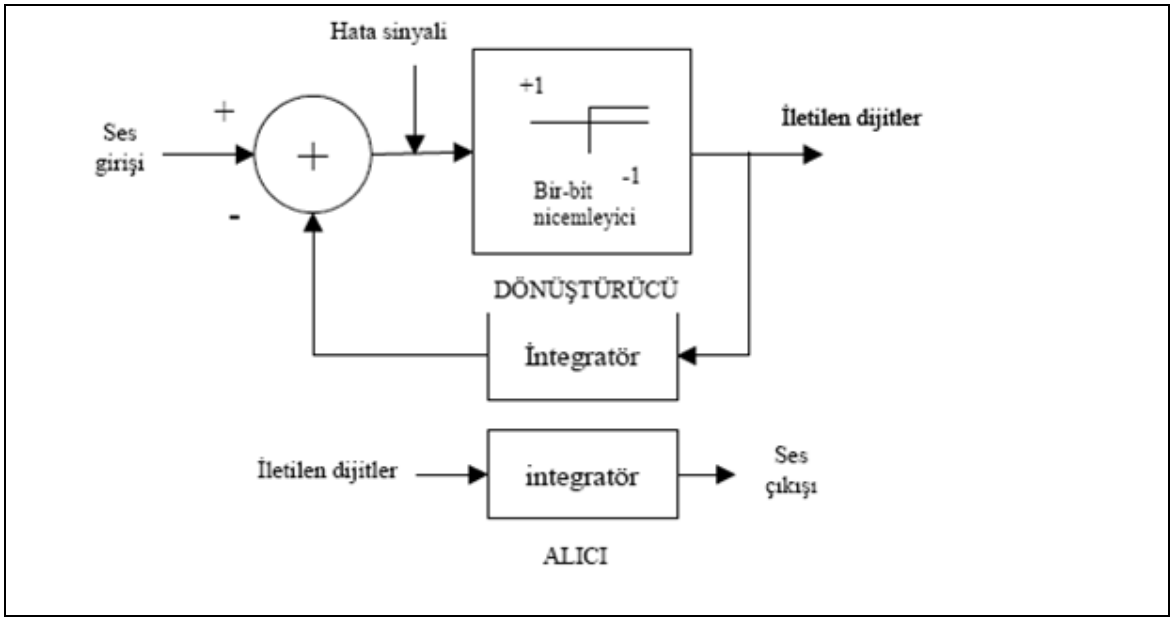
b. Uyarlanabilir Farksal darbe kod modülasyonu (Adaptive Differential Pulse Code Modulation-ADPCM)

Bu teknik 16-40 Kbps arasında sıkıştırma yapar. 32 Kbps ADPCM sıkıştırması ile 64 Kbps PCM arasında pratikte konuşma kalitesinde fark yoktur. ADPCM algoritma olarak PCM'den farklıdır; çünkü örneklenmiş ses sinyalinin basamaklanması yerine, ön kestirilen ve basamaklanan sinyal arasındaki farkı basamaklar olarak kabul eder. İyi bir ön kestirimde gerçek sinyal ile tahmini sinyal arasındaki fark çok küçük olacaktır ve bu da daha düşük bit akış hızı anlamına gelecektir (Monson H. Hayes 1998).

Sinyalin yeniden üretilmesi basamaklanan edilmiş farkın tahmini sinyale eklenmesiyle bulunur. Bu sayede orijinal sese çok yakın bir sinyal elde edilmiş olur. ADPCM metodu sadece 2:1 oranı gibi çok düşük bir sıkıştırma sunsa da veri sıkıştırma metotlarıyla beraber kullanılarak 4:1 oranına ulaşılabilmektedir.

c. Delta Modülasyonu

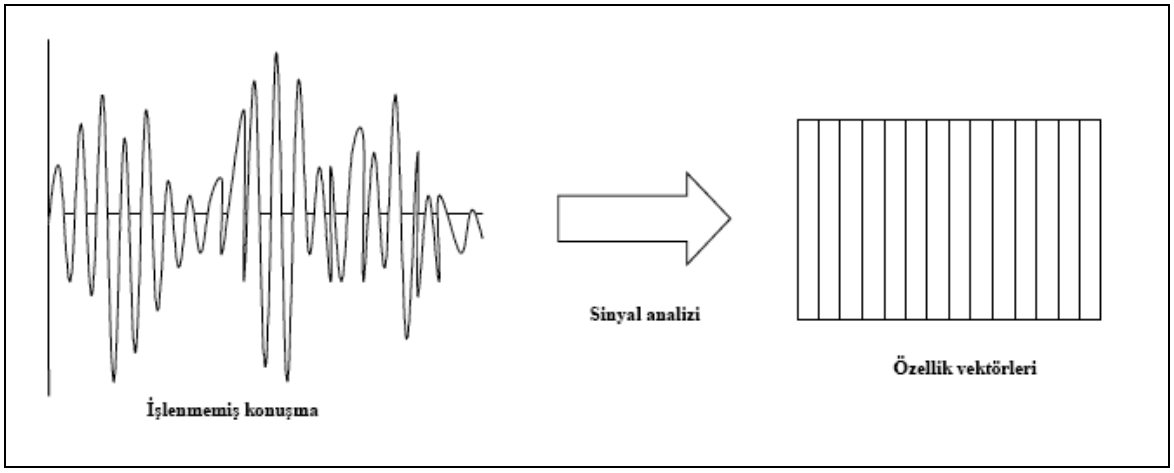
Delta Modülasyonu dalga formu , kodlamada alternatif olan en basit tiptir. Bir delta modülatör giriş dalga formunun yerel bir kopyasını üretmek için iletilen sayısal kodları kullanmakta ve kodlayıcı kısıtları ile mümkün olabilecek en uygun giriş dalga formunun kopyasını üretmek için ardışık sayısal kodları seçmektedir. Nicemleyicinin (Kuantalayıcı) orijinal ve en basit formu her örnek için sadece bir bit kullanılmakta ve bir kuantum ile sadece ön görülen değerin arttırılıp azaltılamayacağı gösterilmektedir. Böyle bir kodlayıcı çok basit donanım uygulaması olanağı sunmaktadır (Monson H. Hayes 1998).Uygulama Şekil 1-2 Basit bir delta modülatör blok diyagramıŞekil 1-2 Basit bir delta modülatör blok diyagramında gösterilmektedir.



Şekil 1-2 Basit bir delta modülatör blok diyagramı

1.1.2.2 Sinyal İşleme Teknikleri

Ses sinyaline, tanımada gerekli olan faydalı özelliklerini ortaya çıkarmak için sinyal işleme teknikleri uygulanır. Ses tanıma sistemleri genelde ses sinyallerinin analizinden faydalanmaktadırlar. Ses sinyalinin analizi sonucunda bu frekans ve genlik bilgilerini içeren özellik vektörleri oluşur. Bir özellik vektörü genelde her bir kısa zaman aralığındaki (10 milisaniye) bir ses sinyali penceresinden (20~30 milisaniye)'den hesaplanır. Söylenen kelime bu özellik vektörlerinin bir dizisi olarak gösterilir. Sonraki aşamada bu özellik vektörleri tanıyıcıya giriş olarak verilir (Monson H. Hayes 1998).



Şekil 1-3 Ses sinyalinin özellik vektörlerine dönüştürülmesi

Bazı sinyal işleme teknikleri herhangi bir önemli veri kaybı olmadan ayırıcı özellikleri bulduğu ve sıkışmış veriyi açabildiği için daha kullanışlıdır. En popülerleri aşağıda açıklanmıştır (Monson H. Hayes 1998).

- Hızlı Fourier Dönüşümü (Fast Fourier Transform-FFT) gözle görülebilecek biçimde yorumlanabilen zamandaki ayrık frekansları verir. Frekanslar düşük düzeyde lineer olan ama yüksek düzeyde logaritmik olan "Mel scale" kullanılarak ve insan kulağının fiziksel karakteristiklerine uygun olarak sınıflandırılırlar. Fourier dönüşümü ile genlik-zaman boyutu, frekans-genlik boyutuna dönüştürülür.
- Algısal Doğrusal Ön Görümlü Kodlama (Perceptual Linear Predictive-PLP) aynı zamanda fizyolojik olarak harekete geçirilir, ama katsayılar açıkça yorumlanamaz. Algısal Doğrusal ön görümlü kodlama, Ayrık Fourier Dönüşümü (Discrete Fourier Transform-DFT) ve Doğrusal ön görümlü Kodlama (Linear Predictive Coding-LPC) tekniklerinin birleştirilmesi ile sesin parametrelerinin hesaplanmasıdır.
- Doğrusal Ön Görümlü Kodlama (Linear Predictive Coding-LPC)'da temel fikir, bir ses örneğinin kendisinden önceki ses örneklerinin doğrusal kombinasyonu kullanılarak tahmin edilmesidir. Gerçek ses örnekleri ile tahmin edilen örnekler arasındaki hata minimumlaştırılarak öngörü katsayılarından oluşan parametre değerleri elde edilir. Kodlama yöntemleri içinde belki de en yaygın olanı ve en çok kullanılanı bu kodlama olmuştur. Gırtlak yapısını örnek alan diğer modellerin aksine bir filtre grubu değil de tek girişli ve tek çıkışlı bir filtre modeli benimsemiştir.
- Kepstrum (Cepstral Analysis) güçlü sinyal spektrumu logaritmasında Fourier dönüşümün tersi bir işlem yapar.

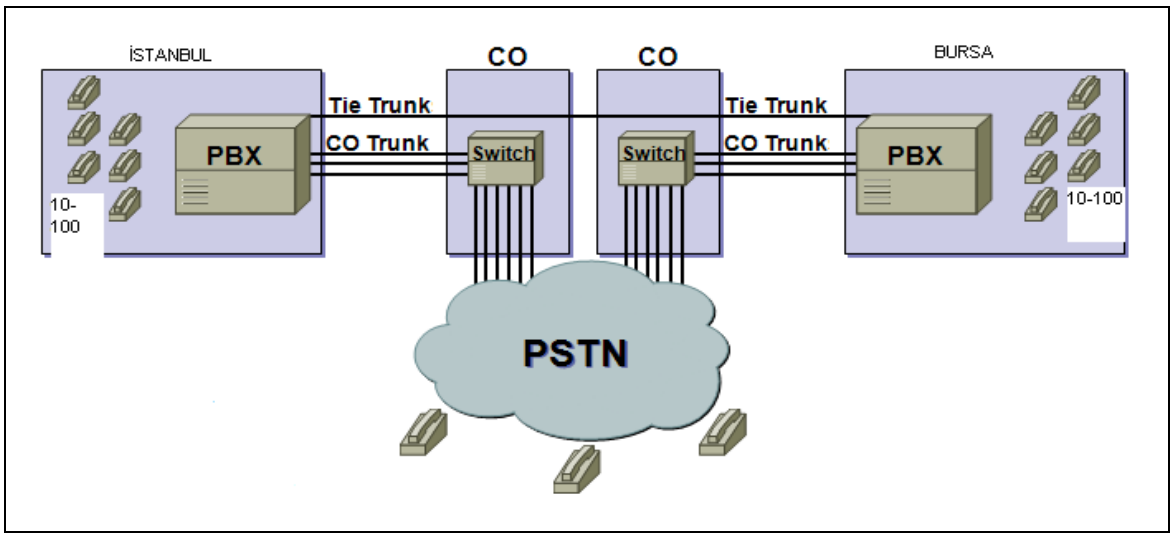
1.1.3 Yerel Çevrim ve Veri Hatları

Günümüz PSTN (Public Switched Telephone Network) şebekeleri kullanıcılarına her çağrı için uçtan-uca bir devre bağlantısı sağlamaktadır. Arayan ve aranan tarafların numarasına göre, arayan tarafın bağlı olduğu santralden başlayarak, aradaki santraller ve diğer uçtaki santrale kadar bir devre kurulmaktadır. Bu santraller arasındaki sinyalleşme temel olarak çağrı

kurma, çağrı yönetimi ve sonlandırılması işlemlerinden oluşmaktadır.

Anahtarlamalı telefon şebekelerine kamusal telefon ağı denmektedir. Bu ağ abone, yerel çevrim, santral ve trunk bileşenlerinden oluşur. Ağa bağlı kullanıcı aygıtlar aboneler ve ağın anahtarlama merkezleri de santrallerdir. Santraller arasındaki bağlantılar trunklardır. Trunk bağlantıları; Özel Trunk Hatları (Tie Trunks), CO Trunk Hatları (PSTN Trunk) ve CO'lar arası Trunk Hatları (Interoffice) olarak üç sınıfa ayrılır. CO santralleri yerel çevrimleri sonlandırır, elektrik sağlar, hatta akım olup olmadığını kontrol eder, zil sesi üretirler ve numara kayıt ederler . Yerel çevrim kullanıcılar ve santraller arsındaki iki telli bağlantılardır. Bu tel çifti tip ring olarak adlandırılmaktadır.

PBX'ler yerel kullanıcılar arasında bağlantı oluşturur ve sesli posta gibi ek servisler sağlarlar. Trunk hatları ile CO santraller ile bağlantı sağlarlar. Bu bağlantılar Şekil 1-4 Telefon şebekeleri için temel bileşenlerde gösterilmiştir (Harte, L. 2003).



Şekil 1-4 Telefon şebekeleri için temel bileşenler (Harte, L. 2003)

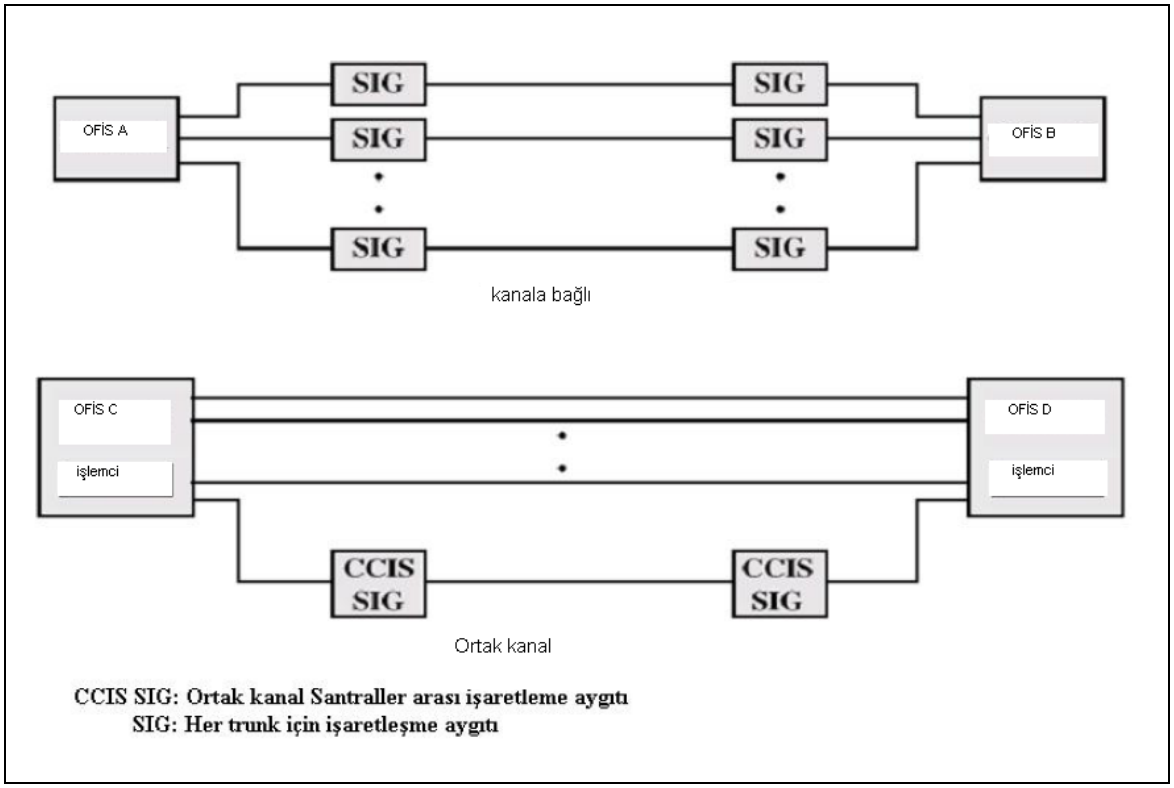
1.2 Temel Telefon İşaretleşmesi

Kamusal telefon şebekelerinde abone ve bağlı olduğu uçlar arasında, anahtarlama noktalarında ve ağ yönetim merkezlerinde kontrol işaretleşmesi gereklidir. PSTN kontrol işaretleri; denetleyici, adres, çağrı bilgisi ve ağ yönetimi olarak dört sınıfa ayrılır. Bu

işaretleşme aboneden ağa doğru ve ağ içinde gerçekleşebilir. Temel kontrol işaretleşmesi aşağıda belirtilen fonksiyonları yerine getirmektedir:

- Çevir sesi, zil çalma sesi, meşgul sesi v.s.
- Çevrilen numaranın iletimi
- Çağrının tamamlandığının belirtilmesi
- Telefon çaldırma işaretinin üretilmesi
- Ücretlendirme bilgisi
- Cihaz ve hat durumu bilgisi
- Test ve sorun giderme bilgisi

İşaretleşme, arayan ve aranan abone ile santral arasında, santral içindeki birimler arasında veya iki santral arasında yapılabilir. Santraller arası işaretleşmede işaretleşme bilgileri konuşmanın yapılacağı hat üzerinden yapılıyorsa buna kanala bağlı sinyalleşme denir. Bu işaretleşme türünde çağrı ve işaretleşme için aynı kanal kullanılır. Şayet santraller arası işaretleşmede konuşma ayrı bir kanaldan işaretleşme bilgileri ayrı bir kanaldan yapılıyorsa bu tip sinyalleşmeye ise ortak kanal sinyalleşmesi diye adlandırılır. Bu sinyalleşmede sinyalleşme kısmı konuşma kısmından ayrıdır ve ayrı bir birim üzerinden sinyalleşme yapılır. Sinyalleşmenin yapıldığı kısım iletim kanalı olarak adlandırılır. Konuşmanın yapıldığı birim ise hatlardır. Bir kontrol kanalı birden fazla abone kanalına ilişkin kontrol bilgileri taşır. Kontrol kanalı zengin bir içerik kümesini desteklemek için yeterli bant genişliğine sahip olacak şekilde tasarlanmaktadır. Kontrol işaretleri ses kanlarlının iletildiği yoldan doğrudan kontrol işaret işleyicilere gönderiliyorsa bu birleşik durum; işaret düğüm noktalarından ses ve kontrol işaretleri olarak iki grupta gönderiliyorsa bu birleşik olmayan durumdur.



Şekil 1-5 Ortak kanal ve kanal bağlı işaretleşme (Harte, L. 2003)

Anahtarlama teknolojilerindeki kilometre taşı ITU.T tarafından standartlaştırılmış birleşik olmayan ortak kanal işaretleşme yapısı numara 7 işaretleşmesi (Common Channel Signaling System 7 ;CCS7)" ile sağlanmıştır. Şekil 1-5 Ortak kanal ve bağlı ve bağlı işaretleşmede bu ilişki gösterilmiştir. Ağ üzerinde ilerleyen tüm bilgilerin hepsi iki kategoride incelenmektedir. Bunlar, mesajların sinyalleşmesi ve telefon konuşmalarındaki sesin ağ üzerindeki yükü olarak düşünülebilir. Geleneksel olarak bu iki kategori hep birlikte ve aynı kanalda taşınır. 1970'li yılların sonlarında mesajların sinyalleşmesi ve taşınması farklı kanallarda yapılamaya başlanmıştır. Bu sinyalleşme sistemi, CCS7 veya "Signaling System 7 (SS7)" 1980 yılında ulusal iletişim tarafından standartlaştırılmıştır. Birleşik devletlerde şuan birçok uzun mesafe taşınması ve Bell firmasının operasyonları CCS7 ağlarına taşınmıştır. Bu dünyadaki ilk standart uygulama olmuştur. Ayrılmış sinyal kanalı ağ üzerinde geniş bilgi için kapı açmıştır. Bu yeni bilgi geniş alanda gelişimi mümkün kılmıştır.

Bu standart, Kamusal Anahtarlamalı Telefon Ağındaki (PSTN) ağ birimlerinin sayısal bir işaretleşme ağı üzerinden kablosuz (Hücresel) ve karasal çağrı kurulumu, yönlendirilmesi ve denetimini sağlamak için yöntem ve protokolleri tanımlamaktadır.

SS7 ağı ve protokolleri,

- Temel çağrı kurulumu, yönetimi ve bitirilmesi,
- GSM gibi kablosuz hücresel hizmetler, kablosuz dolaşım (Roaming) ve mobil kullanıcı doğrulaması.
- Yerel Numara Taşınabilirliği (Local Number Portability, LNP)
- Karasal ücretsiz (Toll-free, 800/888) ve ücretli (Toll, 900) hizmetler.
- Çağrı yönlendirme, arayan tarafın numara/adının görüntülenmesi, telekonferans
- Dünya çapında yüksek servis sürekliliği ile güvenli iletişim gibi amaçlarla kullanılır.

1.2.1 İşaretleşme Bağlantıları

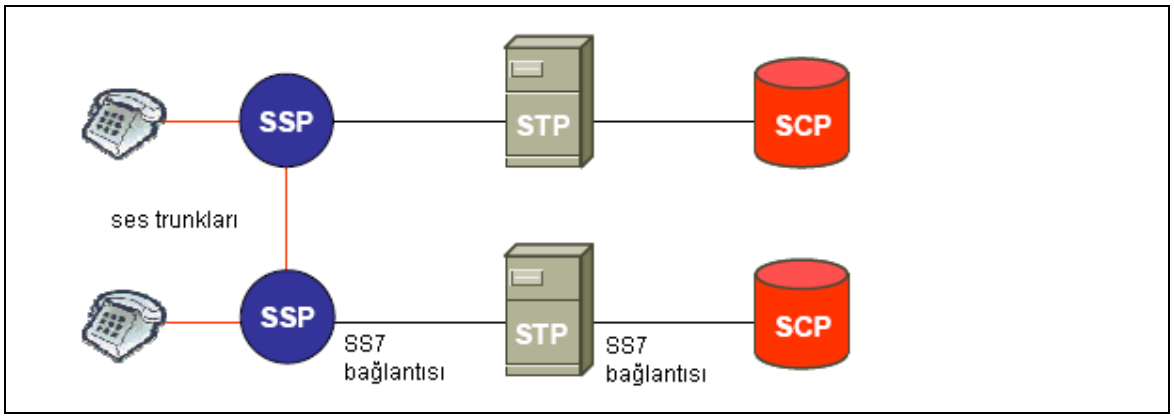
SS7 mesajları ağ birimleri arasında 56 Kbps ya da 64 Kbps'lik işaretleşme bağlantıları ile iki yönlü hatlar üzerinden veri alış verişi gerçekleştirilmektedir. İşaretleşme; ses kanalları ile birlikte değil, harici bir kanal üzerinden taşınmaktadır.

1.2.1.1 İşaretleşme Noktaları

SS7 ağındaki her işaretleşme noktası sayısal bir nokta kodu ile benzersiz olarak belirtilir. Nokta kodları (Point Codes) işaretleşme noktaları arasında alış verişi gerçekleştirilen her mesajda kaynak ve alıcı noktaları belirlenebilmesi için taşınmaktadır. Her işaretleşme noktası, her mesaj için uygun bir işaretleşme yolu seçmek için bir yönlendirme tablosu kullanır.

SS7 ağında üç tür işaretleşme noktası bulunmaktadır. Şekil 1-6 SS7 işaretleşme noktalarıŞekil 1-6 SS7 işaretleşme noktaları :

- Hizmet Anahtarlama Noktası , (SSP, Service Switching Point)
- İşaret Aktarım Noktası, (STP, Signal Transfer Point)
- Hizmet Denetim Noktası , (SCP, Service Control Point)



Şekil 1-6 SS7 işaretleşme noktaları (Harte, L. 2003)

SSP'ler çağrıları başlatan, sonlandıran ya da bağlayan santrallerdir. Bir SSP bir çağrının tamamlanabilmesi amacıyla ses devrelerinin kurulması, yönetilmesi ve kaldırılması için diğer SSP'lere işaretleşme mesajlarını gönderir. Bir SSP ayrıca merkezi bir veritabanına (Bir SCP) bir çağrıyı (Örneğin ücretsiz 800 çağrıları) nasıl yönlendireceğine dair bir sorgulama gönderebilir. SCP de çağrıyı başlatan SSP' ye, aranan numara ile ilişkilendirilmiş yönlendirme numaralarını içeren bir cevap gönderir. Eğer birincil numara meşgul ya da çağrı belirlenen bir zaman içinde cevapsız kalırsa alternatif yönlendirme numaraları SSP tarafından kullanılabilir. Çağrı özellikleri şebekeye göre farklılıklar gösterebilir. İşaretleşme noktaları arasında ağ trafiği STP adı verilen bir paket anahtarı tarafından da yönlendirilebilir. Her STP, gelen her mesajı SS7 mesajı içinde taşınan yönlendirme bilgisine göre dışarı yönlü bir işaretleşme bağlantısına yönlendirmektedir. STP bir ağ birleşim noktası (HUB) görevi görür. İşaretleşme noktaları arasında doğrudan bir bağlantı gereksinimini ortadan kaldırdığından SS7 ağının daha verimli olarak kullanılabilmesine olanak tanımaktadır. Bir STP; işaretleşme noktasının, işaretleşme mesajında mevcut rakamlardan belirlendiği genel etiket çevrimi işlevini (Global Title Translation) de yerine getirebilmektedir. Bir STP ayrıca diğer şebekelerle alış verişi gerçekleştirilen mesajlar izlemek için bir güvenlik duvarı gibi de davranabilir. SS7 ağı çağrı işleme işlemleri için hayati öneme sahip olduğundan SCP ve STP'ler, olası arızaların işletimi engellememesi için farklı fiziksel noktalarda eşli çiftler olarak konuşlandırılırlar. İşaretleşme noktaları arasında bağlantılar da çiftler halinde kurulur. Ağ trafiği bağ kümesi içinde paylaştırılarak aktarılır (Yük dengeleme). Eğer bağlantılardan biri arızalanırsa tüm trafik diğer bağlantı üzerinden aktarılır (Yedekleme). SS7 protokolü, işaretleşme noktaları veya ara bağlantılarda arıza durumlarında servis sürekliliği için hata düzeltme ve yeniden iletim yeteneklerini sahiptir.

1.3 PSTN Hizmetleri

Uzun mesafe haberleşmesi tipik olarak anahtarlama noktalarından oluşan ağlar üzerinden yapılır. Anahtarlama noktaları ve bağlantıların oluşturduğu topluluğa haberleşme ağı denir. Veri ağ üzerinde bir anahtarlama noktasından diğerine anahtarlanarak yönlendirilir, anahtarlar verinin içeriğiyle ilgilenmezler. Anahtarlama noktaları yalnızca diğer noktalara bağlı olabileceği gibi uç cihazlar olan istasyonlara ve diğer anahtarlama noktalarına da bağlı olabilir. Anahtarlama noktaları arasındaki genellikle çoğullanmış olan bağlantılara trunk adı verilir. Bu haberleşme ağındaki bağlantılarda devre anahtarlama ve paket anahtarlama olmak

üzere iki tür anahtarlama yöntemi kullanılır.

1.4 Paket ve Devre Bağlaşmalı Ağlar

Eğer iki nokta arasında kurulan iletişim kanalı veri aktarımı tamamlanana kadar kesintiye uğratılmadan açık bırakılıyor, yalnızca iki kullanıcının haberleşmesi için ayrılıyorsa bu tür iletişime devre anahtarlamalı iletişim (circuit switched communication) denir. Bir nevi iki nokta arasında sanal bir kablo varmış gibidir.

Paket anahtarlamalı bir ağ altyapısı ise öncelikle veri transferi maksadıyla kurulmuş bir altyapıdır. Paket anahtarlamalı yapılarda veriler paketler olarak adlandırılan küçük parçalara bölüştürülmüştür ve parçalar iki nokta arasındaki yollardan hangisi o an için en uygunsa o yolu tercih ederek hedefe ulaşırlar. Bu durumda gönderilecek verimizden bir kısım paketler belli bir yolu tercih etmiş durumdayken bir kısım paketler başka bir yoldan hedefe yönlendirilmiş olabilirler. Bu tür bir durumda, hedefe ulaşıldığı noktada paketlerin sırası karışmış da olabilir. Hedefteki alıcı bu paketleri, kullanılan protokolde tanımlanan yöntemlere göre orijinal sıralarına koymakla yükümlüdür.

Paket anahtarlamada bazen bir takım paketlerimizin taşındığı yol üzerinde geçici aksaklıklar yaşanabilir ve bu veri transferinde geçici kesilmelere sebebiyet verebilir. Fakat veri transferi bu tür kısa gecikmelere karşı son derece toleranslıdır. Halbuki ses, video ve benzeri zaman-kritik uygulamalarda, yerine zamanında ulaşmayan bir veri paketi, seste çatlama/bozulma vb. problemlerle görüntüde de kayma,atlama ve benzeri bozulmalara sebep olabilmektedir.

1.5 PSTN ve VOIP Arasındaki Karşılaştırmalar

VoIP en basit anlamda, ses aktarımının klasik PSTN sistemindeki devre anahtarlamalı protokollerden farklı olarak paketler halinde veri ağları (IP protokolü) üzerinden yapılabilmesi olarak tanımlanabilir. VoIP**;** mevcut telefon şebekeleri, intranet, internet ve WAN bağlantılarındaki ses ve verinin birleşmesiyle birlikte yönetim maliyetlerini düşüren aynı zamanda servis ve gelir fırsatları yaratan, kullanım kolaylığı sağlayan bir teknolojidir.

VoIP teknolojisinin üzerinde kurulduğu temel kavram, bağlantı ağlarının iletim esnasında verileri sayısallaştırılması ve bu sayısallaştırılmış verinin belirli ölçüdeki paket ya da kısımlara bölünerek taşınmasıdır. Bu durum VoIP teknolojisinin devre anahtarlamalı PSTN telefon görüşmelerine olan bir üstünlüğü olarak kabul edilmektedir. Bunun yanı sıra, veri

iletimi esnasında aradaki bağlantının sürekli açık kalma zorunluluğunun olmaması, her iki taraftaki kullanıcı bağlantılarını tamamen meşgul etmemekte ve başka bağlantıların kurulabilmesine olanak sağlamaktadır. Son kullanıcı cihazlarının yönetimi ve ağ üzerine bütünleştirilmesi de bu sayede basitleşmiştir. Geleneksel devre anahtarlamalı telefon ağları ses trafiğini taşımak üzere her görüşme için konuşma yapılıp yapılmadığına bakılmaksızın bütün bir kanalı ayırmakta ve ağ bant genişliğini verimsiz bir şekilde kullanmaktadır. Ayrıca bu bağlantılarda hem ses hem de görüntü taşımak istenirse iki ayrı ağ bağlantısına da yatırım yapılması gerekmektedir. Dolayısı ile bu iki ağın yönetilmesi zor ve yatırım maliyetleri yüksek olmaktadır. Bu durumda, kullanıcıya çoklu ortam veri servislerinin kullanmak, yani IP ağlarında ve internette kullanılan paket teknolojileri ile çözüme gitmek veri akışı ve kullanılabilirliği bakımından oldukça cazip hale gelmektedir. İkinci bir önemli avantaj ise uygulama çeşitliliğidir. Voip ile tek bir numara altında telefon, tele-sekreter, faks, e-mail, video konferans ve benzeri uygulamaların verilebilmesi imkanı artmaktadır.

VoIP'in belirgin bir diğer avantajı da kullanım maliyetlerinin düşük olmasıdır. Belirli bant genişliğine sahip data hatları için ödenen ücret sabittir. Bu hatlar üzerinden VoIP ekipmanları ve protokolleri kullanılarak istenilen miktarda telefon görüşmesi yapılabilir. Bu durumda sabit bir ücret ve kurulum maliyetleri ile telefon hatlarından yapılabilecek görüşmenin kalitesine çok yakın bir kalitede çok daha ucuza telefon görüşmesi yapma imkanı oluşmaktadır. Bununla birlikte karşı tarafın da VoIP kullanıyor olması durumunda aynı anda birden fazla kişiyle konuşulması mümkün olmaktadır.

VoIP'in bir başka avantajı da SIP ve H323 gibi oturum başlatma protokolleri vasıtası ile fiziksel adreslere bağımlı olunmamasıdır. Bu sayede sistemler farkı zamanda farklı IP adresleri ile yapılandırıldıklarında da ulaşılabilir olurlar. DHCP (Dynamic Host Configuration Protocol) , dinamik olarak bilgisayar veya IP telefona bir IP numarası atar. Dolayısıyla statik olarak IP adresinin bu aygıtlar üzerinde ayarlanmasına gerek yoktur. SIP protokolü REGISTER metodu ile vekil sunucuya DHCP'den aldığı ağ adresini kayıt ettirmek suretiyle, ağdaki yerini sürekli güncel tutar.

Günümüzde büyük hacimli firmalar ile daha küçük çaplı firmalar örneğin KOBİ'ler, merkez ofisleri ile diğer ofisleri arasında da WAN bağlantıları üzerinden VoIP teknolojisi kullanabilmektedirler. VoIP kullanımı işletmelere de aşağıda belirtilen avantajları sağlamaktadır:

- Ses ve veri hizmetlerinin bir arada verilebilmesi: Mevcut sistemde kamusal telefon ağı üzerinden verilen ses hizmetinin yanı sıra görüntü yada veri taşıma işlemi aynı anda

yapılamamaktadır. Her bir hizmet için farklı bir haberleşme kanalı gerekmektedir. IP ağlarının da ise ses de sayısallaştırılıp veriye çevrilip iletilmektedir. Bu nedenle sesli, görüntülü görüşme ve dosya paylaşımı gibi uygulamalar aynı anda tek bir bağlantı ile yapılabilmektedir.

- Güvenlik**:** SSL gibi şifreleme ve L2TP tünelleme teknolojileri VoIP sinyalleşmesini ve trafik akışının devamını etkin ve güvenli bir şekilde gerçekleştirir.
- Etkili bir maliyet indirimi**:** Geleneksel PSTN kullanımında, hattı sağlayan ve yöneten şirkete genel olarak hattın kullanım süresi kadar para ödenir. Ve ayrıca aynı anda birden fazla kişi ile konuşmak mümkün olmaz. Belirli bant genişliğine sahip data hatları için ödenen ücret sabittir. Bu hatlar üzerinden VoIP ekipmanları ve protokolleri kullanılarak istenilen miktarda telefon görüşmesi yapılabilir.
- Üretkenliğin ve ölçeklenebilirliğin arttırılması: Bu uygulama yazılım temelli olduğundan bilgisayar ve iletişim teknolojilerindeki gelişmelere kolayca adapte olabilecek yapıdadır.
- Servis sağlayıcılar için gelirlerini arttırma fırsatı: Farklı birimlerde farklı santraller kullanılmasına gerek kalmamaktadır. Merkezi anahtarlama mantığı ile çalışır. İşletmesi daha kolaydır. Faturalandırma, numara tesisi ve iptali v.s işlemler merkezi olarak yapılmaktadır. Sonuç olarak kurulum ve operasyon maliyetleri düşer.
- Uygulama kolaylığı: VoIP teknolojileri sayesinde, uzaklık ya da bölge fark etmeksizin, görüşmelerin kayıt edilmesi, iki kullanıcının görüşmesi esnasında üç yada daha fazla kullanıcının görüşmeye katılabilmesi ve/veya konferans görüşme şeklinin oldukça basitleştirilmesi sağlanmaktadır.

IP üzeri ses teknolojisinin sağladığı göz ardı edilmez avantajların yanında, halen aşması gereken problemleri de bulunmaktadır.

- Konuşmanın kalitesi ağın trafik yoğunluğuna bağlıdır. Bugünkü telefon ağıyla aynı kaliteyi sağlayabilmek için, ağ üzerinde servis kalitesi (QoS) garanti edilmelidir. Bu sebeple, Multi-Protocol Label Switching (MPLS) ve IP Type of Service(ToS) protokolleri geliştirilmiştir.
- IP üzeri ses standartları halen geliştirilme aşamasındadır: H.323 V2.0 - International Telecommunication Union (ITU), Media Gateway Control Protocol (MGCP) - Internet Engineering Task Force (IETF), Session Initiation Protocol (SIP) - IETF gibi birçok kurumun geliştirdiği değişik standartlar mevcuttur.
- Şu an kullandığımız telefonlar için gerekli elektrik, santral tarafından sağlanmaktadır. Herhangi bir elektrik kesintisinde dahi telefonunuz acil hatlara (polis, hastane, v.b.) erişebilmektedir. IP telefonlarında gerekli elektrik, kullanıcı tarafında sağlandığından bu durum gerçekleşmez. Fakat, General Bandwidth şirketinin bu yıl sonunda piyasaya süreceği ürün ile santraller elektrik kesintisi durumunda IP telefonlara gerekli elektriği sağlayabilecekler.

2. VOIP TEKNOLOJİSİNE GİRİŞ

İnternet'in hayatımız girmesinden önce iletişim kamusal anahtarlamalı telefon ağı (PSTN) aracılığıyla yapılıyordu. Veri iletimi, özellikle uzun mesafeler için oldukça pahalıydı.

PSTN şebekeleri her kullanıcıya uçtan uca bir devre anahtarlamalı bağlantı sağlamaktadır. Arayan ve arananın numarasına göre arayan tarafın bağlı olduğu santralden başlayarak diğer uçtaki santrale kadar bir devre kurulmaktadır. Ancak buna paralel olarak veri trafiği için ayrı şebekeler oluşturulmuştur. Doğal olarak ayrı ses ve veri şebekeleri servis sağlayıcılar için ilave yük, aboneler için de ilave maliyet anlamına gelmektedir. PSTN trafiği her geçen gün daha fazla veri içerikli olmaya yüz tuttukça ses ve veri şebekelerinin tek bir platforma indirgenmesi gerekliliği daha fazla belirgin hale gelmiştir.

1995'de modemlerin 14,4 Kbps hızına erişmesi aynı anda 8 Kbps bant genişlikli kodlayıcıların (öncelikle GSM için geliştirilmiştir) kullanılabilir hale gelmesiyle internet protokolü (IP) üzerinden ses iletimi (VoIP) mümkün hale gelmiştir. 1995'te ilk küçük internet protokolü üzerinden ses iletim uygulaması geliştirilmesinden sonra 1996'da ilk VoIP standartları kabul edilmiştir.

İnternet üzerinden ses iletimi (VoIP) mevcut telefon şebekesi ağ mimarisi üzerinde yapılan geliştirme çalışmaları sonucunda ortaya çıkan bir teknolojidir. VoIP, ses'i (genellikle insan sesini) IP paketleri halinde internet üzerinden taşımaktır. Bu sistem gerçek zamanlı paket iletişimini gerektirir.

İnternet üzerinden ses iletimi ilk başlarda kişisel kullanımlar amacıyla kullanılmaktaydı. Günümüzde kamu ve iş dünyasında da kullanılmaya başlanması ile yeni servislere ihtiyaç duyulmaya başlandı. Bu birçok servisten bir tanesi bu çalışmada inceleyeceğimiz internet üzerinden ses görüşmelerini kayıt edilmesidir. Bu servis öncelikle telefon hatları üzerinden hizmet veren çağrı merkezleri ve bankalar açısından büyük önem taşımaktadır. Müşterilerin güvenliği ve servis kalitesinin arttırılabilmesi için ses görüşmelerini kayıt edilmesi ve saklanması gerekmektedir. Bu sistemin nasıl çalıştığını anlayabilmek için temel internet protokolünün yapısının iyi anlaşılması gerekmektedir.

Kamusal anahtarlamalı telefon ağından farklı olarak VOIP de kullanıcılar yada ağ ekipmanları

ağ adresleri ile tanımlanırlar. Kamusal anahtarlamalı telefon ağlarında da adresleme mevcuttur fakat bu adresler telefon hatlarının hangi santralin hangi bağlantı noktasına bağlı olunduğu bilgisini içerip kendi kendine değişebilir bir yapıya sahip değildir. VOIP de ise kullanıcılar ağlar arasında dolaşım yetisine sahiptir. VoIP'le çalışan bir cihaz sahip kullanıcı farklı bir ağa girdiği zaman o ağdan alacağı bir ağ adresi ile kendi adresini güncelleyecektir. Bu durumda bu kullanıcı haberleşme sisteminde kayıtlı olan ağ adresini güncellemek zorundadır. Aksi taktirde bu kullanıcıya gelen aramalar ulaştırılamayacaktır. Buradan da anlaşılacağı gibi bir VOIP ağında kullanıcıların ağ adreslerini tutan bir veri tabanı olmak zorundadır. Bu veri tabanları aynı zamanda her bir aramanın hangi durumda olduğu bilgisini de takip etmektedir. Arama yapılmadan önce bu veri tabanından aranılan kullanıcının adresi sorgulanmalıdır. Arama kontrolcüsü olarak adlandırılan bu sistemler kullanılan protokol türüne göre değişik mimariler göstermektedirler.

VOIP son kullanıcı programları ise ses işaretlerini alıp sayısallaştırabilme yetisine sahip olmalıdır. VOIP de işaretler sadece sayısal olarak iletilebilmektedir. Bu sayısallaştırılma yapılırken aynı zamanda düşük bant genişliği kullanmak amacıyla sıkıştırma da yapılmalıdır.

2.1 IP Temelleri

Bu bölümde VOIP konusunun rahatlıkla anlaşılabilmesi için gerekli olan genel bilgiler verilecektir. Bu bilgiler arasında TCP /IP modeli, OSI referans modeli ve IP adreslemesi genel hatlarıyla anlatılacaktır.

2.1.1 OSI Referans Modeli

Bilgisayarlar arası iletişimin başladığı günden itibaren farklı bilgisayar sistemlerinin birbirleri arasındaki iletişim daima en büyük problemlerden birisi olmuş ve bu sorunun üstesinden gelebilmek için uzun yıllar boyunca çeşitli çalışmalar yapılmıştır.

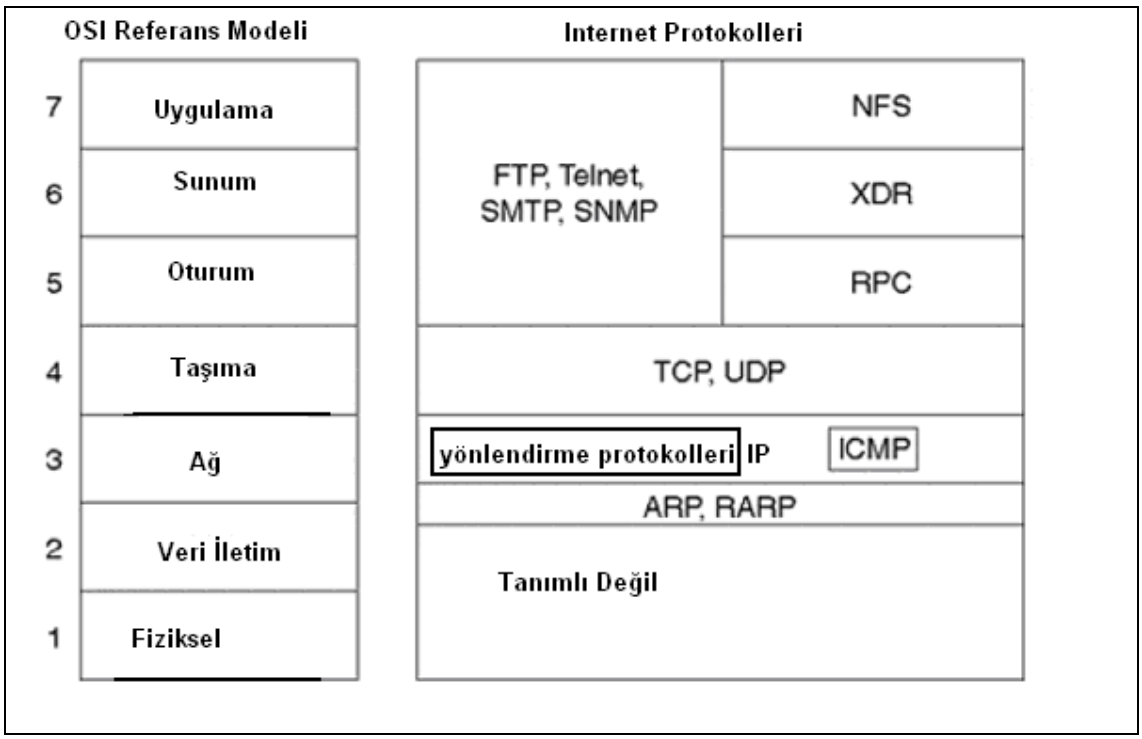
OSI referans modeli 1980'lerin başında ISO (International Standards Organization) tarafından bilgisayar sistemlerinin birbirleri ile olan iletişiminde ortak bir yapıya ulaşmak yönünde çabaları sonucunda geliştirilmiştir. Ve şimdi bu model, bilgisayar iletişimini sağlayan protokollerin geliştirilmesi için bir standart haline gelmiştir. Bütün protokollerin bu modeli takip etmemesine rağmen yine de yeni protokollerin öğrenilmesi ve geliştirilmesi için OSI referans modelini kullanılmaktadır. Bu model sayesinde değişik bilgisayar firmalarının ürettikleri bilgisayarlar arasındaki iletişimi bir standarda oturtmak ve farklı

standartlar arası uyumsuzluk sebebi ile ortaya çıkan iletişim sorununu ortadan kaldırmak hedeflenmiştir.

OSI referans modeli, sistemler arası iletişimdeki problemleri çözmek için 7 katmana ayrılmıştır. Her bir katman diğer sistemlerdeki karşılığı ile iletişim sağlama görevi yapar. Ek olarak her bir katman kendinden üstteki katmana servis hizmeti sunar. Aynı zamanda kendisinin altındaki katmanlardan servis hizmeti bekler (Zimmermann, H. 1977).

Bu katmanlı yapı ile birlikte her bir katman, bilginin küçük bir parçasını tutar ve veri üzerinde gerekli olan değişikliği yapar. Katmanlı yapının en altında bulunan fiziksel katman en son olarak veriyi 1 ve 0 şeklinde elektriksel sinyaller haline getirir.

Bu katmanlı yapının anlaşılması için, IP yönlendirmesinin nasıl çalıştığı ve IP'nin katmanlar üzerindeki farklı ortamlarda nasıl taşındığı görülmelidir.



Şekil 2-1 OSI referans modeli

2.1.1.1 Uygulama Katmanı

Kullanıcıya en yakın olan katmandır. Bu katmanda çalışan uygulamalara örnek olarak, FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), e-mail uygulamaları verilebilir. Uygulama katmanı için bir diğer örnek HTTP'tir. HTTP çalıştırılan bir program değil bir protokoldür. Yani bir kurallar dizesidir. Bu dizeye göre çalışan bir web tarayıcı, aynı protokolü kullanan bir web sunucuya erişir.

2.1.1.2 Sunum Katmanı

Bir sistem üzerindeki uygulama katmanından gönderilen bilgilerin bir başka sistemin uygulama katmanı tarafından okunabilmesini sağlar. Bu katmanda gelen paketler bilgi haline dönüştürülür. Bilginin karakter set çevrimi veya değiştirilmesi, şifreleme vs. görevlerini bu katman üstlenir. Bu katmanda tanımlanan bazı standartlar ise şunlardır; PICT, TIFF, JPEG, MIDI, MPEG.

Sunum katmanı günümüzde çoğunlukla ağ ile ilgili değil, programlarla ilgili hale gelmiştir. Örneğin eğer iki tarafta da .gif formatını açabilen bir resim gösterici kullanılıyorsa, bir makinenin diğeri üzerindeki bir .gif dosyayı açması esnasında sunum katmanına bir iş düşmemektedir. Dosya istekte bulunan sisteme iletilip dosyayı açacak uygulama tarafından formatı belirlenip açma işlemi gerçekleştirilmektedir.

2.1.1.3 Oturum Katmanı

Bu katman yardımı ile farklı bilgisayarlardaki kullanıcılar arasında oturumlar kurulması sağlanır. Bu işlem oturumların kurulmasını, yönetilmesini ve bitirilmesini içerir. İletişimin kopması durumunda oturumun devam etmesi için eş zamanlama (synchronization) bilgileri tutulur. Oturumlara farklı kalitede servisler de sunabilir. Bu katmanda çalışan protokollere örnek olarak NFS (Network File System), SQL (Structured Query Language), RPC (Remote Procedure Call), ASP (Apple Talk Session Protocol), DNA SCP (Digital Network Architecture Session Control Protocol) ve X Window verilebilir.

2.1.1.4 Taşıma Katmanı

Ağ üzerinde taşınan bilginin güvenilirliğinden sorumludur. Akış ve hata kontrolünü sağlar. Veri sıralaması yapar. Tekrar iletimi sağlar. TCP ve UDP bu katmanda çalışan protokollere örnektir. TCP (Transmission Control Protocol) gibi bazı taşıma katmanları ağ üzerindeki karmaşıklığı çözmek için bir mekanizmaya sahiptir. TCP yeniden iletim zamanlayıcısını

ayarlar. Mesela bir ağ üzerinde tıkanıklık olduğu zaman TCP bu ağ trafiğini azaltır ve tekrar normal hale geldiğinde veriyi gönderir.

Taşıma katmanı alt katmanlar (Transport Set) ve üst katmanlar (Application Set) arasında geçit görevini görür. Alt katmanlar verinin ne olduğuna bakmandan karşı tarafa yollama işini yaparken üst katmanlarda kullanılan donanım ile ilgilenmeden verinin kendisi ile uğraşabilirler.

2.1.1.5 Ağ Katmanı

Bu katman, veri paketlerinin ağ adreslerini kullanarak bu paketleri uygun ağlara yönlendirme işini yapar. Yönlendiriciler bu katmanda tanımlıdırlar. Bu katmanda iletilen veri blokları paket olarak adlandırılır. Bu katmanda tanımlanan protokollere örnek olarak IP ve IPX verilebilir. Bu katmandaki yönlendirme işlemleri ise yönlendirme protokolleri kullanılarak gerçekleştirilir. Yönlendirme protokollerine örnek olarak RIP, IGRP, OSPF ve EIGRP verilebilir. Burada dikkat edilmesi gereken önemli bir nokta da yönlendirme protokolleri ile yönlendirilebilir protokollerin farklı şeyler olduğudur. Bu katmanda kullanılan yönlendirme protokollerinin görevi, yönlendirilecek paketin hedef'e ulaşabilmesi için geçmesi gereken yolun hangisinin en uygun olduğunu belirlemektir. Yönlendirme işlemi yukarıda bahsettiğimiz yönlendirme protokollerini kullanarak dinamik bir şekilde yapılabileceği gibi, yönlendiricilerin üzerinde bulunan yönlendirme tablolarına sabit olarak kayıt girilerek de paketlerin yönlendirilmesi gerçekleştirilebilir.

2.1.1.6 Veri Bağlantı Katmanı

Bu katman fiziksel katmana güvenilir taşımayı sağlar. Bağlantı katmanı kendi adresleme şemasına sahiptir. Bu adresleme şeması fiziksel bağlantı ve veri bağlantı katmanı adres tabanlı çerçevelerin taşınması ile ilgilidir.

Bu katmanda veri paketlerine hata kontrol bitleri eklenerek çerçeve halinde fiziksel katmana iletilir. Ayrıca iletilen çerçevenin doğru mu yoksa yanlış mı iletildiğini kontrol eder, eğer çerçeve hatalı iletilmişse çerçevenin yeniden gönderilmesini sağlamak da bu katmanın sorumluluğundadır. Bu katmanda, iletilen çerçevenin hatalı olup olmadığını anlamak için CRC (Cyclic Redundancy Check) yöntemi kullanılır. Anahtarlayıcılar ve köprüler bu katmanda tanımlıdırlar. Bu katmanda çalışan protokollere örnek olarak HDLC, PPP, ATM ve "Frame Relay" gösterilebilir.

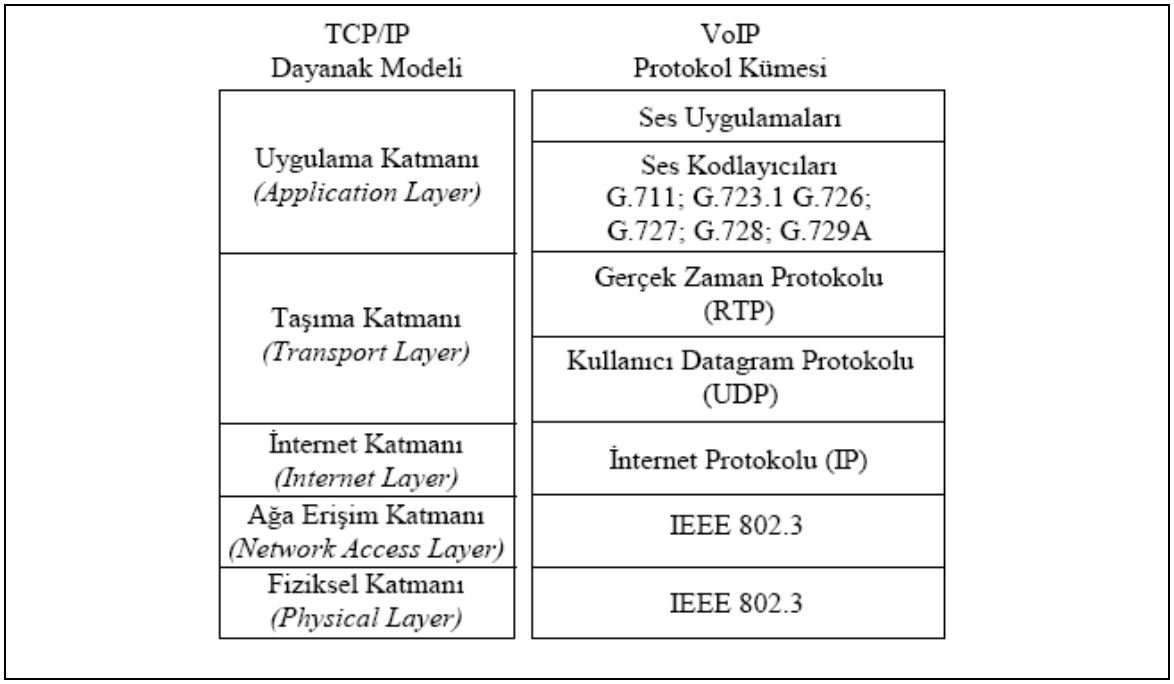
2.1.1.7 Fiziksel Katman

Verilerin fiziksel olarak gönderilmesi ve alınmasından sorumlu katmandır. Hub'lar fiziksel katmanda tanımlıdırlar. Bu katmanda tanımlanan standartlar taşınan verinin içeriğiyle ilgilenmezler. Daha çok işaretin şekli, fiziksel katmanda kullanılacak bağlantı noktası türü, kablo türü gibi elektriksel ve mekanik özelliklerle ilgilenir. Örneğin V.24, V.35, RJ45, RS-422A standartları fiziksel katmanda tanımlıdırlar.

OSI referans modeli bir ağ uygulaması değildir. OSI sadece her katmanın görevini tüm detayları ile tanımlar. Bu modeli bir gemi ya da bina projesine benzetebiliriz. Nasıl gemi planını alıp farklı firmalar gemi yapabilirse OSI modeli de böyledir. Nasıl ayni gemi planından iki farklı firma gemi ürettiğinde örneğin kullanılan çiviler farklı yerlere çakılabilirse, OSI modeli de ürün gerçekleştiren firmadan firmaya farklılık gösterebilir.

2.1.2 TCP / IP Modeli

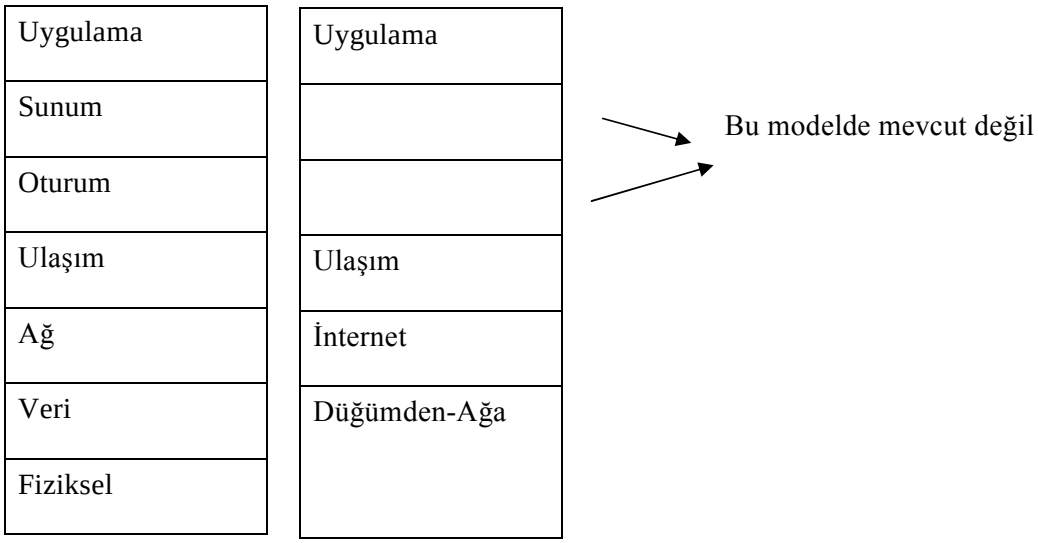
Bir başka referans modeli de TCP/IP'dir. Bu modelin temelini ABD Savunma Bakanlığı İleri Proje Araştırmaları Ajansı (DARPA) tarafından desteklenerek geliştirilen ARPANET oluşturur. ARPANET'te amaç heterojen (telli, telsiz) alt ağların oluşturduğu bir ortamda kesintisiz bir bağlantı oluşturmaktı. Önem verilen bir diğer nokta ise bazı hatların kopması ya da düğümlerin bozulması sonrasında bile alternatif yolların bulunarak bağlantıların yaşatılmasını sağlamaktı. TCP/IP referans modelinin yapısı (Postel, J. 1980a) ve voip protokolleri ile ilişkisi Şekil 2-2 TCP-IP referans modelinin yapısında verilmiştir.



Şekil 2-2 TCP-IP referans modelinin yapısı

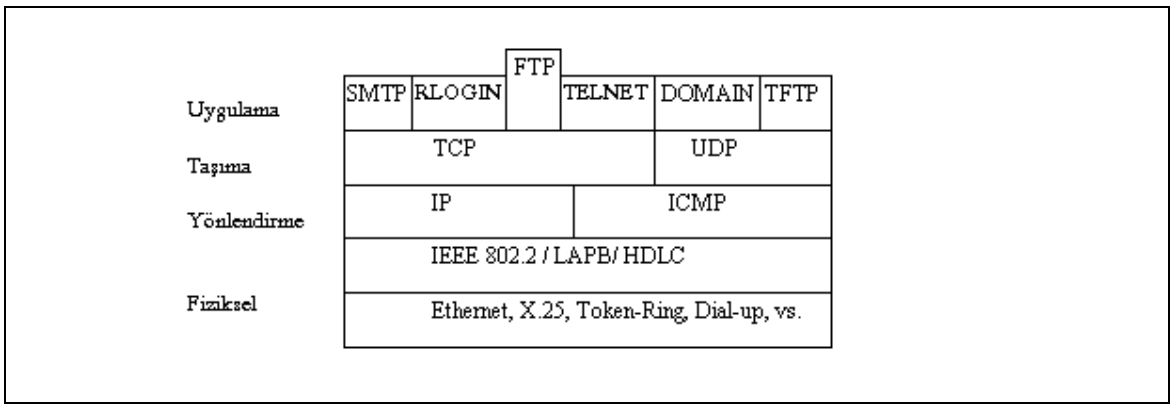
Fiziksel katman sayısal haberleşmeyi 1'lerin ve 0'ların voltaj referansları ile ifade edildiği anlatmaktadır. Ağa erişim katmanı 10mb/s, 100mb/s, 1000mb/s hızındaki değişik ağ arayüz aygıtlarını tanımlamaktadır. İnternet katmanı bir paket yapısı ve IP (Internet Protocol) adı verilen protokol tanımlamaktadır. Paketlerin oluşturulması, yönlendirilmesi, ortamdaki tıkanıklıkların giderilmesi bu protokolün görevindedir.

İnternet katmanının üzerinde ulaşım katmanı çalışır. Ulaşım katmanında kullanılmak üzere iki adet uçtan-uca protokol tanımlanmıştır. Bu protokoller: RFC 761 ile tanımlanan TCP (Transmission Control Protocol) (Postel J. 1980a) ve RFC 768 ile tanımlanan UDP'dir (User Datagram Protocol) (Postel j. 1980b). TCP/IP referans modelinde de uygulama katmanı tanımlanmıştır. Bu katman OSI referans modelinde olduğu gibi, ağa erişmek için gerekli uygulama protokollerini içerir. OSI ve TCP/IP referans modelleri şekil 2-3 deki gibi karşılaştırılabilir:



Şekil 2-3 OSI ve TCP-IP modellerinin karşılaştırılması

Şekil 2-3'te de görüldüğü gibi TCP/IP referans modeli sunuş ve oturum katmanlarına sahip değildir. OSI referans modelindeki veri bağı katmanı ve fiziksel katmanın işlevleri TCP/IP referans modelinde düğümden-ağa katmanında gerçeklenmiştir. TCP/IP modeli ilk önerildiğinde içinde yer alan protokoller ve ağlar şekil 2-4 de gösterilmiştir.



Şekil 2-4 İlk TCP modeli

2.1.3 İnternet Protokolü (IP) Adresleme

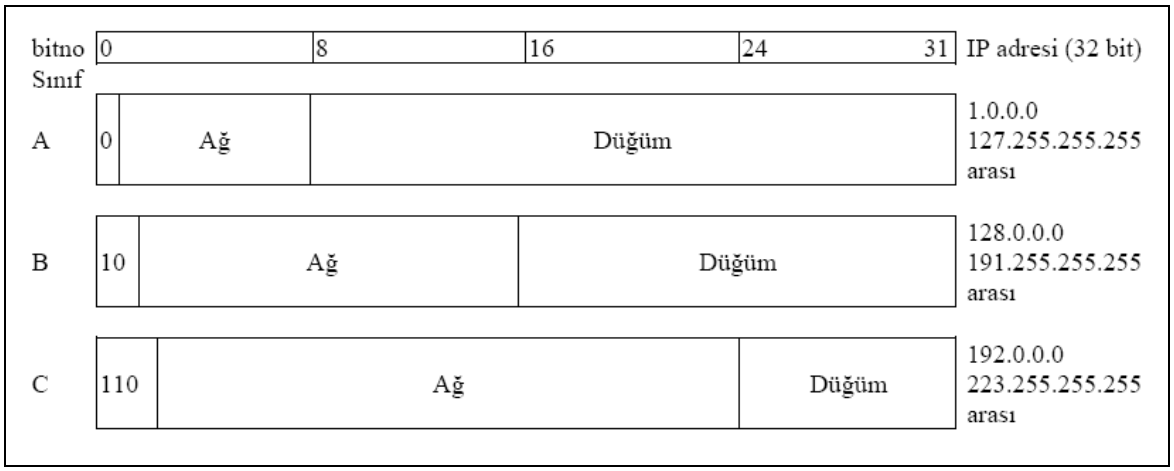
İnternette bağlanan her bilgisayara bir IP adresi atanmaktadır diğer bilgisayarlar bu bilgisayara bu adres ile ulaşmaktadır. Yani iki farklı cihaz aynı yerel ağda olmasa dahi, IP adresi birbirleri ile iletişim kurabilmelerine olanak sağlamaktadır. IP adreslemesini anlamak

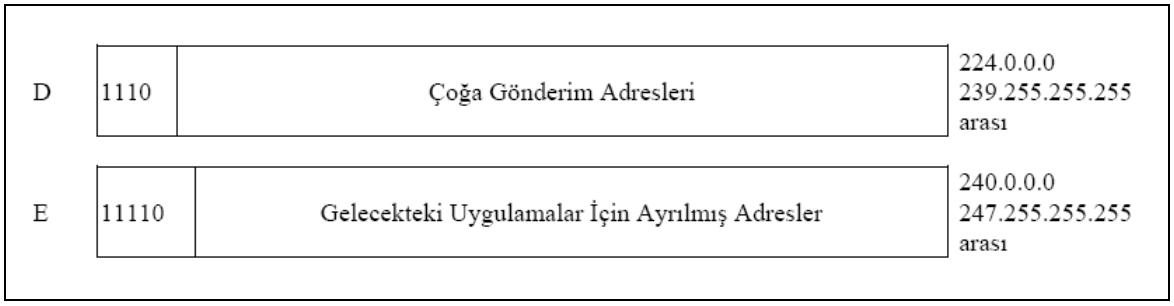
önemlidir. Çünkü IP altyapısının üzerinde aygıtların nasıl etkin bir şekilde iletişime geçtiğini anlamak için ağ yapısının nasıl oluşturulduğunu kavramak gerekir. Bu iletişimde çok fazla protokol mevcuttur ve her biri farklı adresleme şemasına sahiptir.

Ağ katmanlı adresleme normal olarak hiyerarşiktir. OSI referans modelinin 3. katmanında bulunur. Bu katman da, benzer mantıksal adreslemeye sahip bilgisayar gruplarını oluşturur. Yönlendiriciler trafiği, 3. katman veya ağ katmanı adresi tabanlı yönlendirir. IP adresleme RFC 791 de (Postel, J 1980a) aşağıda görülen beş ağ sınıfını şeklinde açıklanmıştır :

- A Sınıfı (Class A) ağları, bir kaç tane geniş ağ için kullanılır. Çünkü bunlar, yalnızca 7 biti ağ adres alanı olarak kullanır.
- B Sınıfı (Class B) ağları, 14 biti ağ adres alanı, 16 biti de host adres alanı olarak kullanır.
- C Sınıfı (Class C) ağları, 21 biti ağ adres alanı olarak kullanırken sadece 8 biti host adres alanı olarak kullanır. Bununla birlikte her bir ağdaki host sayısı belirli bir limite sahiptir.
- D Sınıfı (Class D) adresleri RFC 1112 içerisinde resmi olarak tanımlanmış çoğa gönderimli gruplar için ayrılmıştır.
- E Sınıfı (Class E) adresleri IP tarafından tanımlanmıştır. Fakat gelecekteki kullanım için ayrılmıştır.

Her adres sınıfı özel bir bit dizisi ile başlar. Adreslerin dağıtılması ICANN (Internet Corporation for Assigned Names and Numbers) tarafından organize edilir. Her ülkede ICANN'ye bağlı olarak çalışan yerel birimler vardır. Aynı zamanda IP ağlarını "Alt ağ (subnet)"olarak adlandırılan daha küçük parçalara bölebiliriz. Alt ağlar yönetimi için daha fazla esneklik sağlar. IP adresleri türleri Şekil 2-5 A,B,C adres sınıfı formatlarında gösterilmiştir.





Şekil 2-5 A,B,C adres sınıfı formatları

Bazı IP adreslerinin özel anlamı vardır. 0.0.0.0 adresi bazı sistemlerin ön yüklemesi (boot) sırasında kullanılır. Ağ adresi olarak 0 verilen IP adresleri içinde bulunulan IP ağını ifade etmektedir. 255.255.255.255 IP adresi içinde bulunulan ağa geniş yayım (broadcast) için kullanılır. Bir ağ adresi belirttikten sonra adresin kalan kısmı 1'lerle doldurulursa, bu da belirtilen ağ adresine yayını ifade eder. 127 öneki ile başlayan tüm adresler döngü sınaması (loopback test) için kullanılır. Bu adrese gönderilen paketler ağa çıkarılmaz. Yerel olarak işlenir ve ağdan gelmiş bir paket gibi davranılır.

2.1.4 Yönlendirme Protokolleri

Yönlendirme protokolü, veri taşıyan bir paketlerin doğru adreslere iletilmesini sağlamakla görevlidir. IP paketleri yönlendirilirken atlamalı-yönlendirme (hop-by-hop routing) tekniği kullanılır. Bir yönlendirici aldığı paketin varış adreslerine bakar, kendi yönlendirme tablolarındaki maskeleri kullanarak varılmak istenen ağ adresine en çok benzeyen tablo adresini bulur ve paketin aktarılacağı ağ arayüzü bilgisine erişir. Paket, yönlendiricinin bağlı bulunduğu ağlardan biri üzerindeki ağ ara yüzüne gönderilmişse, doğrudan o ara yüzün adresine gönderilir. Aksi halde gitmesi gereken yöndeki düğüm ya da anahtarlama noktasından bir sonraki yönlendiriciye ulaşması için aktarılır.

IP ağlarında çeşitli yönlendirme protokolleri kullanılır. Günümüzde iki ana tip yönlendirme protokolü yaygınlık kazanmıştır. Bunlar; mesafe-vektör yönlendirmesi ve bağlantı-durum yönlendirmesidir.

Basit bir şekilde açıklarsak; mesafe-vektör yönlendirmesi, kaç tane yönlendiriciden geçildiği ile ilgilenir. Bağlantı-durum yönlendirmesi ise, temel olarak yönlendiricinin desteklediği ara yüzlerin durumuyla ilgilidir. Bu iki yönlendirme protokolü iç ve dış yönlendirme protokolleridir.

İç yönlendirme protokolleri, genellikle tek bir yönetimsel izin altında yönlendiricilerin

güncellenmesi için kullanılır.

Dış yönlendirme protokolleri, farklı otonom sistemlerin içerisindeki ağların, yönlendirme güncellemelerini alarak oluşturur. Dış yönlendirme protokollerinin en iyi örneği, internet üzerinde kullanılan BGP'dir.

2.1.4.1 Mesafe-Vektör Yönlendirmesi

Yönlendiricilerin en iyi yönlendirmeyi seçebilmesi için kullanılan bir algoritmadır. Bu algoritma en az bir tane yönlendiriciyi, hedefe gidilebilecek en iyi yolu belirlemek için kullanır. RIP, IGRP, EIGRP birer mesafe-vektör yönlendirme protokolüdür.

2.1.4.2 Bağlantı-Durum Yönlendirmesi

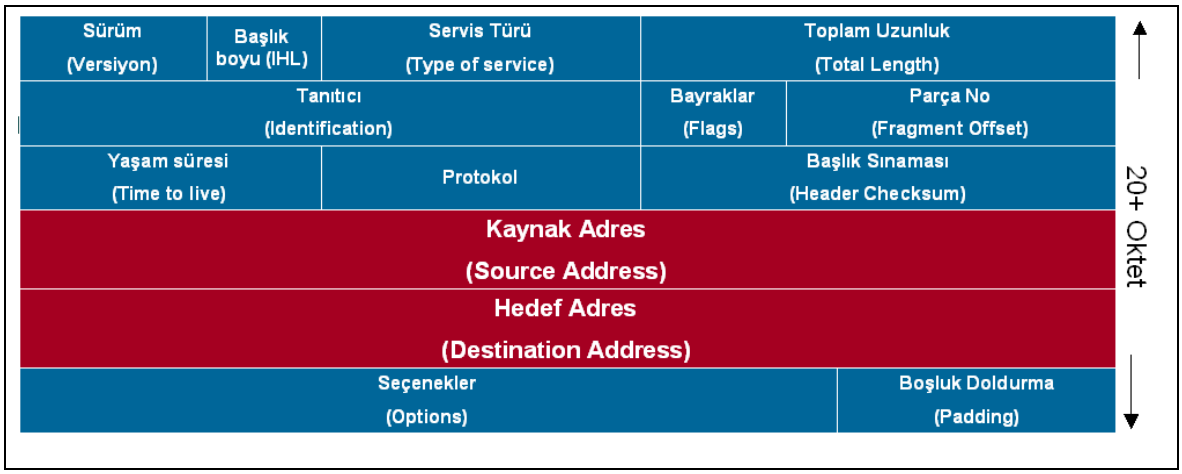
Bunun mesafe-vektör yönlendirmesinden farkı, sadece bir arayüz değişikliği olduğu zaman yönlendirme güncellemesi yapar. Bunun anlamı; bir arayüz oluştuğunda veya kaybolduğunda trafik ve bant genişliği değişir. OSPF, EIGRP, BGP, IS-IS ve NLSP birer bağlantı-durum yönlendirme protokolüdür.

2.1.5 IP Paket Yapısı:

IP paketlerine datagram da denmektedir. IP paketlerini 32 bitlik satırlar (words) halinde düşünülebilir. Paketteki bazı alanların içeriği açıktır. Diğerleri için bu bölümde kısa açıklama aşağıda yapılmıştır. IPv4 paket başlık yapısı Şekil 2.6 da, IPv6 paket başlık yapısı ise Şekil 2.7 de gösterilmiştir.

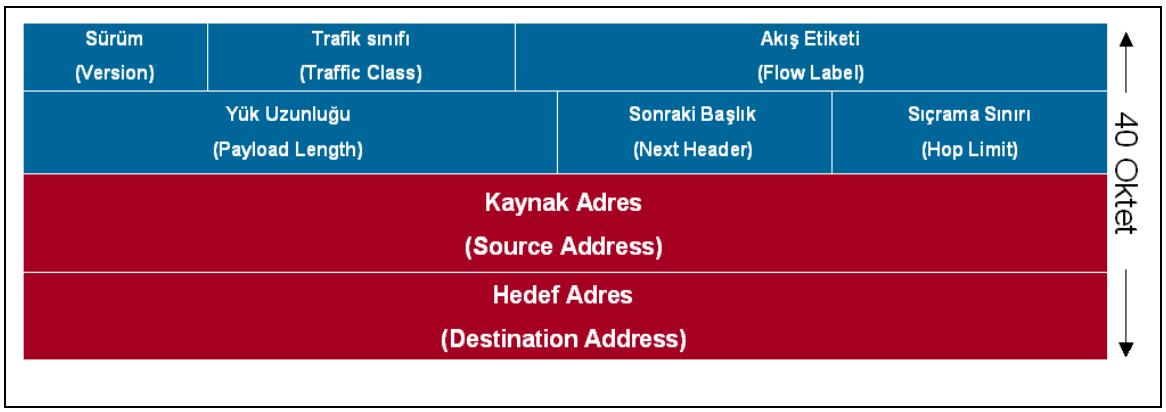
- Başlık uzunluğu satır cinsinden verilir. En kısa başlık beş satır uzunluğundadır.
- Servis tipi paketin servis sınıfını belirtir.
- Toplam Uzunluk başlık ve verinin toplam uzunluğunu byte cinsinden verir.
- Tanıtıcı parçalanmış IP datagramlarının birleştirilmesinde yardımcı olur. DF (Don't Fragment) biti datagramın parçalanmaması gerektiğini gösterir. MF (More fragments) biti arkadan aynı datagrama ait başka bir parça gelip gelmediğini gösterir. Son parça dışındaki tüm parçalarda 1 değerine sahiptir. Parça numarası (bazen parça kayıklığı olarak da adlandırılır) ilgili parçanın bütündeki yerini gösterir.
- Yaşam Süresi (TTL) alanındaki değer her atlamada bir azaltılır. Değer sıfıra eriştiğinde paket hala varış düğümüne ulaşmadıysa yok edilir.
- Protokol alanı hangi ulaşım protokolünün kullanıldığını gösterir.
- Başlık Sınaması başlıktaki hataları fark etmek için kullanılır. Hatalı bir başlığa sahip olan paket yok edilir.
- Seçenekler alanı protokolün daha sonraki sürümlerine kolaylık tanımak için tasarlanmıştır. Sürüm 4 için planlanan seçenekler güvenlik, kaynak yönlendirme, yolun kaydedilmesi, zaman bilgilerinin tutulması içindir. İlgili bilgiler gerektiğinde seçenekler bölümüne

eklenir.



Şekil 2-6 IPv4 Paket başlık yapısı

İnternet kullanıcı sayısındaki aşırı artış IP adresi yetersizliğinin ortaya çıkmasına neden olmaktadır. Günümüzde kullanılmakta olan IPv4 sistemi, internet omurgasına bağlı ağ trafiğini sınıflandırmak için bir adres hiyerarşisi kullanmaktadır. IP adreslerinin tükenmesiyle IP V.6 geliştirilmiştir. 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.



Şekil 2-7 IPv6 paket başlık yapısı

IPv6 , IPv4 dün sunamadığı aşağıdaki olanakları sağlamaktadır:

- 128-bit adresleme ile daha geniş adres alanı 32 –bit adresleme kullanana versiyon 4 e göre

çok daha fazla adresleme kapasitesine sahiptir.

- Esneklik, otomatik adresleme, otomatik konfigürasyon, tak çalıştır özellikleri versiyon 4 de oldukça gerçekleştirilmektedir. Örnek olarak IPSec uygulaması gösterilebilir.
- Uçtan uca uygulama desteği, güvenlik
- İnternet mobil uygulamaları için uygun altyapı
- Geleceğin mimarisi =Yeni İnternet Protokolü
- Daha basit IP başlığı ile verimli ve yüksek performanslı Yönlendirme

IPv6'nın yaygınlaşası ile NAT gibi ip adres çoklamak için kullanılan protokollerin rafa kaldırılacağı öngörülmektedir. Bunun sonucu olarak daha hızlı iletişim ve uçtan uca güvenlik sağlanması ön görülmektedir.

3. İNTERNET PROTOKOLÜ ÜZERİNDEN SES İLETİMİNDE(VOIP) TEMEL KAVRAMLAR

İnternet veya geniş alan ağları üzerinden ses iletiminde elde edilen sesin kalitesi 2 bileşene bağlıdır. Bunlar ses sıkıştırması için seçilen algoritma ve sesin taşındığı ağ ortamının sağladığı servis kalitesi (QoS) özellikleridir. Her üreticinin kendi ürününün en iyi ses kalitesini verdiğini söylediği bir ortamda, üreticilerin ses kalitesini karşılaştırmak için objektif bir ölçüt belirlenmesi zorunlu hale gelmişti. Bunun sonucunda ortaya çıkan ortalama fikir skoru (MOS, Mean Opinion Score) değerlendirmesi ses kalitesini ölçmek için kabul gören bir yöntem olmuştur. Bu değerlendirmede çok sayıda kişinin sesi dinleyerek verdiği puanlar ile oluşturulmaktadır. Normal telefon konuşması (MOS değeri 4.1) referans alınarak ses kalitesi derecelendirilmektedir

3.1 Servis Kalitesi (QoS)

VoIP uygulamalarında gerçek zamanlı veri akışına ihtiyaç duyulmaktadır. Etkileşimli ses ve veri değişimi için veri transferini gerçek zamanlı olması büyük önem taşımaktadır. Gerçek zamanlı iletişim teknik olarak mümkün olmamakla birlikte insan kulağının ve gözünün algılayamayacağı gecikmeler gerçek zamanlı olarak kabul edilmektedir. Haberleşmeyi hızlandırmak için VOIP ağlarında yapılabilecek birkaç iyileştirme bulunmaktadır:

- TCP yerine UDP yi tercih etmek :TCP/IP paketlerin gerçek zamanlı iletilmesinden ziyade hatasız iletilmesine çalışır. Bu nedenle daha az güvenli olan ama daha hızlı olan UDP protokolü ses ve görüntü iletiminde tercih edilmektedir. TCP gibi güvenli ve oturum odaklı bir protokol, uç istasyonlar arasında sinyalleşme kanallarını taşımak için kullanılabilir. UDP üzerinde yapılanmış olan RTP, sesin gerçek zamanlı iletimi için kullanılır. Bunun sebebi de çeşitli doğrulama mesajlarını göndermediği için TCP den daha hızlı bir iletim sağlamasıdır.

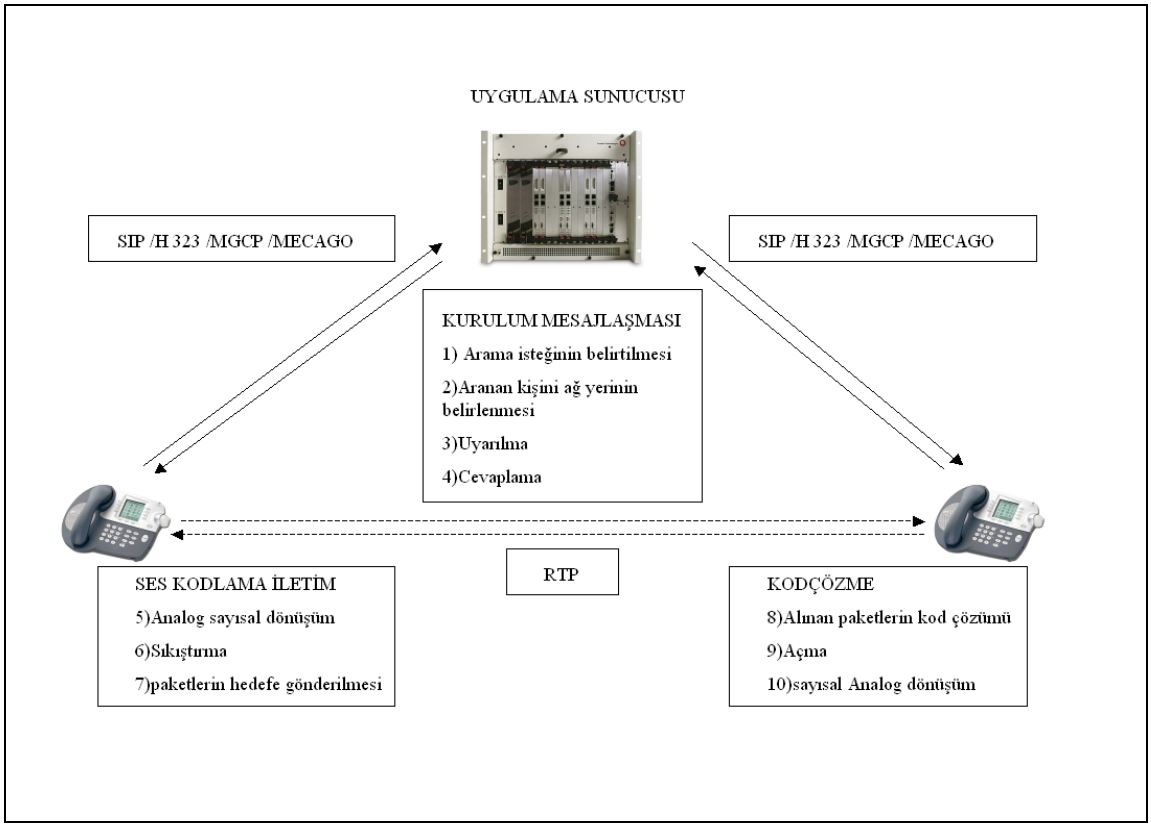
- Ses paket önceliğinin arttırılması**:** IP protokolündeki paket önceliğini belirten TOS biti bir ile beş arasında bir değere ayarlanarak ağ yönlendiricileri üzerinde daha öncelikli olarak yönlendirilmeleri sağlanabilmektedir. Yüksek değer, düşük önem anlamına gelir. Ve çok düşük bir değer ise bize daha çok gerçek zamanlı akış sağlar.
- Parçalama : FTP protokolünde olduğu gibi uzun paket boyutlarına sahip veriler daha küçük boyutlu paketlere ayırarak yollanmalıdır. Bu durumda yönlendiriciler paket iletilene kadar blok edilmez. Ses paketleri gibi gerçek zamanlı paketler aradaki boşluklardan akabilme fırsatı bulmaktadır. Buda ses kalitesinde oldukça belirgin bir etki yaratmaktadır.
- Veri boyutunu küçük tutmak: Aynı bilgiyi daha küçük veri birimler ile taşımak kullanılan

ağı daha az meşgul edeceği için ağ yoğunluğuna bağlı olan gecikmeler azalacak buna bağlı olarak da servis kalitesi daha fazla olacaktır. Bunu sağlamak için veri sıkıştırma yöntemlerine ihtiyaç duyulmaktadır.

3.2 Veri Sıkıştırma

Ses sıkıştırması için kullanılan algoritma elde edilecek sesin kalitesini belirleyen etkenlerden birisidir. Sesin sayısal olarak iletilmesi ilk olarak, G.711 PCM algoritması ile sağlanıyordu. Bu yöntem sesi sıkıştırmadan 64Kbps ile iletilmektedir. Halen birçok telefon operatörü, normal telefon konuşmalarını iletmek için bu yöntemi kullanmaktadır. Bu nedenle G.711'in MOS değeri 4.1 ses kalitesi için referans olarak kabul edilmektedir. Bu ses kalitesi telefon kalitesi (toll quality) olarak isimlendirilmektedir. Sesi sıkıştırmak için ilk olarak kullanılan G.726 ADPCM ve G.728 LD-CELP algoritmaları gerekli bant genişliğine paralel olarak ses kalitesini de düşürmektedir. Daha sonraları, sesi sıkıştırmak için kullanılan DSP teknolojisindeki gelişmeler ile insan sesinin özelliklerine göre sıkıştırma yapılmaya başlanmıştır .Bu sayede ses kalitesini düşürmeden çok düşük bant genişlikleri ile sesi iletme imkanı ortaya çıkmıştır. Örneğin G.725.1 MP-MLQ algoritması, G.726 ADPCM' e göre 5 kat daha fazla sıkıştırma sağlarken, aynı zamanda daha iyi bir ses kalitesi sunmaktadır. Günümüzde VoIP hem düşük bant genişliği, hem de yüksek ses kalitesi sağlaması yaygın olarak tercih edilme sebeplerini başında gelmektedir. Bu çerçevede G.729 ve G.723.1 algoritmaları sıklıkla kullanılmaktadır. Ancak her zaman en düşük bant genişliği sağlayan algoritma en ideal seçeneği oluşturmamaktadır. Kullanılacak algoritma seçilirken, istenen ses kalitesi, mevcut bant genişliği, DSP özellikleri, izin verilen gecikme süresi, paket boyutu, saniyedeki paket sayısı gibi bir çok faktörün göz önünde bulundurulması gerekmektedir.

Ses paketlerinin oluşturulabilmesi için öncelikle analog ses sinyalinin sayısallaştırılması gereklidir. Bu olay analog-sayısal dönüştürücüler sayesinde kolaylıkla yapılabilmektedir ve bunun için kullanılacak en basit donanımlar bilgisayarlardaki ses kartlarıdır. Bu işlem darbe kod modülasyonu (PCM) diye anılır.



Şekil 3-1 VoIP Blok diyagramı

Bu işlem örnekleme, kuantalama ve kodlama aşamalarından oluşur. PCM işaretler daha sonra ITU-T'nin G764 tavsiyesine uygun olarak paketlenir ve kanaldan kodlanarak karşı tarafa iletilirler.

3.2.1 Analogdan Sayısala Dönüştürme

Bu işlem donanım ile gerçekleştirilir, genellikle ses kartlar üzerindeki ADC'ler ile yapılmaktadır. Günümüzde bütün ses kartları 16 bit – 22050 Hz dönüşüme destek vermektedir (Örnekleme için Nyquist kuralına göre 44100 Hz'e ihtiyaç duyulur). Gerekli bant genişliği ise : 2 Byte * 44100 (sn. 'deki örnekleme) = 88200 byte/sn, stereo için176.4 Kbyte/sn. VoIP'de ses yollamak için 176 Kbyte gibi bir bant genişliğine ihtiyacımız olmaz. Sonraki bölümlerde göreceğimiz kodlama seçenekleri ile bunu düşürmekteyiz.

- PCM, Pulse Code Modulation, ITU-T G.711 Ses bant genişliği 4 KHz, örnekleme bant genişliği 8 KHz (Nyquits'e göre) Her örnekleme 8 bit'tir (Bu 256 ayrı değer demek). Net hız : 8000 Hz * 8 bit = 64 kbit/sn, yani tipik sayısal telefon hattıdır. Gerçek uygulamalarda Kuzey Amerika için mu-law ve Avrupa için a-law türleri olan ve logaritmik olarak 12 yada 13 bit analog sinyalleşme kullanılır.

- ADPCM, Adaptive differential PCM, ITU-T G.726 32 Kbps gerektiren ses paketi ile gerçek paket arasındaki farkı çeviren sıkıştırma tekniğidir.
- LD-CELP, ITU-T G.728
- CS-ACELP, ITU-T G.729 ve G.729a
- MP-MLQ, ITU-T G.723.1, 6.3Kbps, Gerçek Zamanlı Konumsa
- ACELP, ITU-T G.723.1, 5.3Kbps, Gerçek Zamanlı Konumsa
- LPC-10, 2.5 Kbps!!

Son olarak sıralanan protokoller oldukça önemli olup, düşük bant genişliği kullanımını garanti etmektedirler. Özellikle G.723.1 çok yüksek bir MOS değerine sahiptir.

3.3 Ses Taşımada Karşılaşılan Problemler

Ses taşımada karşılaşılan problemleri şu başlıklar altında inceleyebiliriz:

3.3.1 Gecikme

Günümüzün telefon ağlarında, üç tip gecikme görülmektedir. Propagasyon gecikme, Seri gecikme ve İşleme gecikme. Seri gecikmenin gerçekte etkisi 1 bit veya 1 byte olduğu için gecikmeye etkisi minimaldir.

3.3.1.1 Yayınım Gecikme (Propagation Delay)

Propagasyon gecikmesine bakır tellerde elektronların, fiber tabanlı ağlar içerisinde ise ışığın hızı sebep olur. İnsan kulağı bu gecikmeyi fark edemez. Propagasyon gecikme, işleme gecikme ile birleştiğinde belirgin bir soruna sebep olur.

3.3.1.2 İşleme Gecikme (Handling Delay)

İşleme gecikmesine ise gerçek paketleme, sıkıştırma ve paket anahtarlama gibi farklı nedenler sebep olmaktadır. Aygıtların ağ içerisinde bilgileri yönlendirmesi sırasında oluşur. İşleme gecikmeleri geleneksel telefon ağlarında etkilidir. Bu gecikmeler, paketlenmiş ortamlar için daha geniş bir konudur.

3.3.1.3 Kuyruklama Gecikme (Queuing Delay)

Paket temelli ağlarda gecikmeler farklı nedenlerden dolayı daha fazladır. Bunlardan ikisi; gerçek paketlerin kuyruğa konması için gerekli zaman ve kuyruk gecikmeleridir.

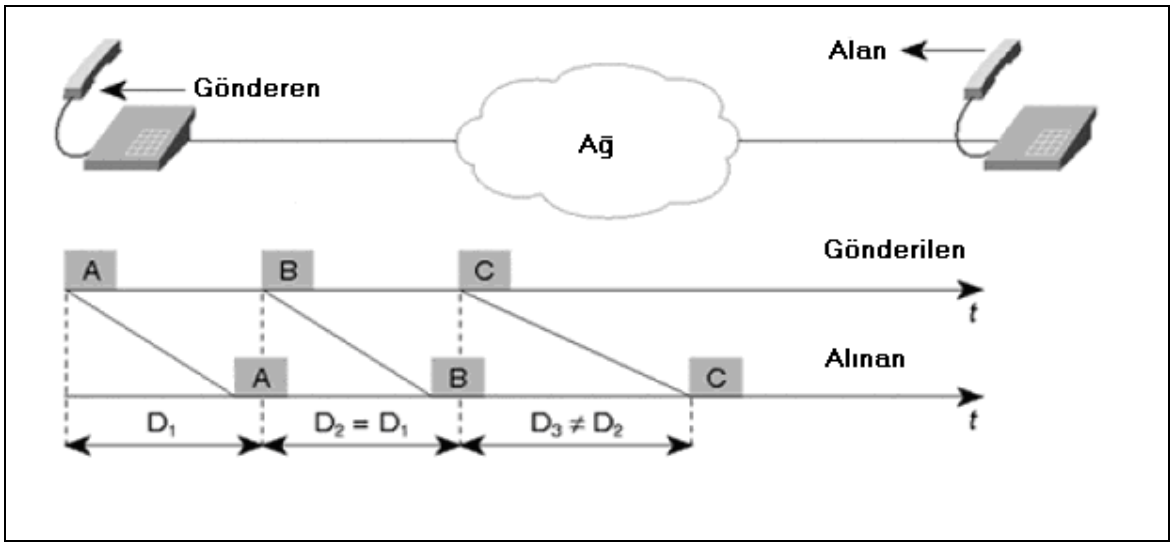
Paketler kuyrukta tutulur çünkü çıkış ara biriminde yoğunluk vardır. Buna kuyruk gecikmesi neden olur. Kuyruk gecikmesi belli bir zamanda , ara birimin tutabileceğinden daha fazla

paketin gönderilmesi ile oluşur. Kuyruk gecikmesi yalnızca uçtan uca gecikme bileşenidir.

3.3.2 Sarkma (Jitter)

Bir ses iletim ortamında bir paket gönderildiği zaman kullanıcı, düzenli bir zaman aralığında ses paketlerinin güvenilir bir şekilde iletimini bekler. Bu iletim sırasında bütün gecikmelerin toplamı ses paketlerinin paket ağı içerisinde gecikmesine ve alıcı istasyonun aynı anda alamamasına neden olur. Bu zaman aralıkları düzenli olduğunda bu gecikmenin algılanması çoğu zaman zordur. Bu düzenli gecikme zaman aralıklarındaki düzensizleşme sarkma(jitter) problemine neden olmaktadır. Sarkma arttığında kanalda patlama ve kesinti şeklinde rahatsız edici parazitler hissedilmektedir. Eğer veri ağı iyi dizayn edilirse jitter büyük bir problem oluşturmaz.

Jitter ve toplam gecikme süresi aynı şey değildir. Bir ağ içerisinde jitter çok fazla olursa o ağ içerisindeki toplam gecikme süresi değişkendir.



Şekil 3-2 Jitter (Sarkma)

3.3.3 Kayıplar

Diğer haberleşme yöntemlerinde görülen çeşitli kayıp türleri VoIP'de de görülmektedir:

3.3.3.1 Modülasyon Kayıpları

Analog iletişim, insan iletişimi için ideal olmasına rağmen hat gürültüsünü önleme konusunda pek sağlıklı değildir. Önceleri telefon ağlarında , analog iletimde sinyalleri güçlendirmek için amplifikatörler kullanılırdı. Ancak bu aynı zamanda hat gürültüsünün de güçlenmesine yol açmaktaydı. Bu da sıklıkla bağlantının kullanılamaz hale gelmesine neden olmaktaydı.

Hat gürültüsünü ayrıştırmak 1 ve 0 bitlerden oluşan sayısal örneklerde daha kolay olmaktadır. Analog sinyaller sayısal hale dönüştürüldüğü zaman hat gürültüsü etkilerinden arınmış bir haberleşmeye imkan sağlanmaktadır.

Birinci kısımda anlatılan işaretin sayısallaştırılması sırasında değerler gelen işaret filtrelenmektedir. İnsan sesi 20 kHz bandına kadar çıkabilmekteyken sadece 4 kHz bandına kadar olan frekanslar modülasyona tabi tutulur. Bu kısım ses de taşınan bilgini yaklaşık %80 ini taşımaktadır. Bu filtreleme ses verisinde kayba neden olur. Bundan sonra gelen örnekleme yi takiben kuantalama kısmında ayrık analog işaretler sayısallaştırılırken aşağı yuvarlama yukarı yuvarlama ve en yakına yuvarlama yöntemleri ile sayısal değerlere yuvarlanmaktadırlar. Bu yuvarlamalar modülasyon kayıplarının doğmasına neden olmaktadır.

3.3.3.2 Sıkıştırma Kayıpları

64 Kbps PCM kodlamada iki temel yöntem ortak kullanılmaktadır. Bunlar ; μ-law ve a-law kodlamalarıdır. Bunların 8 bitlik PCM kalitesini 12-13 bitlik kaliteye çıkarmalarındaki başarıları ve kullandıkları mantıksal sıkıştırma metotları çok benzerdir. Uzak mesafe çağrısı yapıldığı zaman μ-law ile a-law kodlama yöntemini kullanan farklı kullanıcılar arasında iletişim yapılabilmesinden μ-law kodlamasına sahip ülke sorumludur.

Sıklıkla kullanılan diğer bir sıkıştırma metodu da ADPCM'dir (Adaptive Differential Pulse Code Modulation). PCM den farklı olarak 4 bitlik konuşma genişliğini direkt olarak kodlanamayışıdır.

CELP , MP-MLQ, PCM ve ADPCM kodlama şemalarını standardize eden ITU-T bu işlem için kendisine ait G-serilerini önermektedir. Telefon ve ses paketleri için en popüler ses kodlama standartları şunlardır ;

- G.711
- G.726
- G.728
- G.729

- G.723.1

G711 kodlayıcı ailesi dışındaki diğer kodlayıcılar kayıplı kodlayıcılardır. Kodlanan ve kodu çözülmüş veri arasında farklılıklar bulunmaktadır. Bu farklılıklar kodlama kayıpları olarak adlandırılmaktadır.

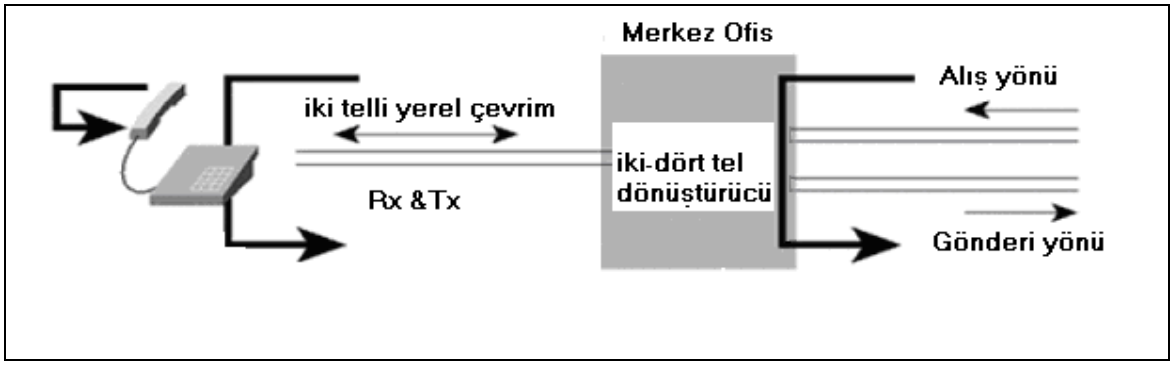
3.3.3.3 Paket Kayıpları

Paket kayıpları veri ağlarında sıklıkla karşılaşılan ve kimi belirli ölçüler dahilinde olduğunda kabul edilebilir kayıplardır. Çoğu veri protokolü gerçekte paket kayıpları ortadan kaldırma için yeniden gönderme metodunu kullanır.Dosya transferi gibi uygulamalarda bir paketin kaybı bile dosyayı kullanılmaz hale getirmektedir. Bu nedenle kayıp paketlerin yeniden gönderilmesi gerekmektedir fakat ses verisi iletimi için yeniden gönderme bir çözüm değildir. Bunun sebebi ses verilerinin gerçek zamanlı olarak iletilmesi gerekmektedir.

Veri ağları üzerinde kritik bir trafik oluştuğunda ağ içerisinde paket kayları artacaktır. Paket kayıp oranını düşük tutmak ses kalitesi açısından ses verisi taşıyan ağlar için oldukça önemlidir.

3.3.4 Yankı

Telefonla konuşurken aynı anda kendi sesini duyması , kullanıcı için bir rahatlık sağlarken , Kullanıcın kendi sesini birkaç saniye sonra duyması oldukça rahatsız edici olmaktadır. Yankının temel sebebi kullanıcının sesinin karşı taraftaki telefon cihazı tarafından tekrar kullanıcıya geri gönderilmesidir. Günlük hayatta kullandığımız telefon cihazlarının hoparlör birimini kulağımız ile kapattığımız için bu durumla pek karşılaşılmaz. Fakat konferans telefonları yada bilgisayarımızdan kulaklık ve mikrofon takımı kullanmadan yaptığımız aramalarda bu durum haberleşmeyi imkansız kılacak derecede rahatsız edici olabilir. Üreticiler bu soruna çare bulmak için yankı giderici (echo cancellation) algoritmaları geliştirmişlerdir.



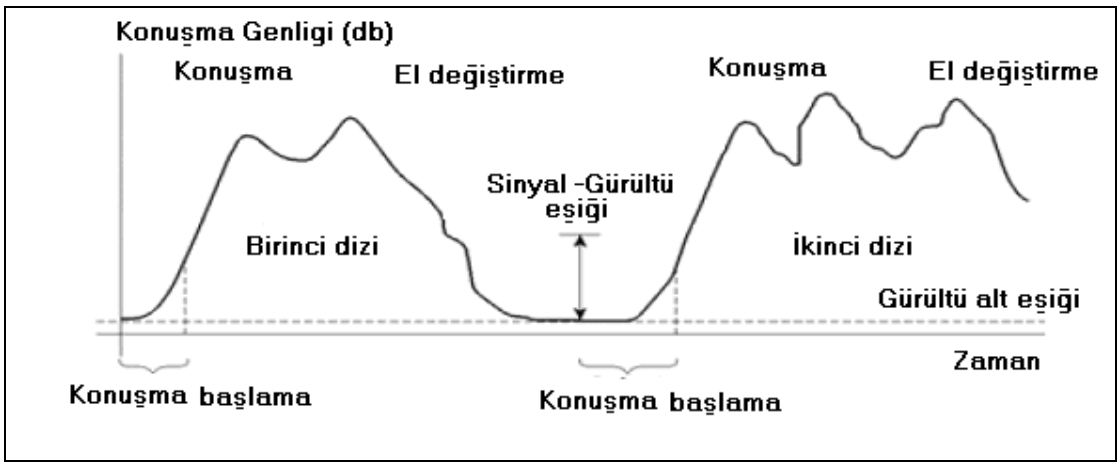
Şekil 3-2 Yankının oluşumu

3.4 Ses Aktivite Tespiti (Voice Activity Detection)

Normal sesli iletişimde bir taraf konuşurken diğer taraf dinlemektedir. Bundan kaynaklanan sebeplerden dolayı konuşma sırasında kullanılan bant genişliğinin yaklaşık yarısı etkin bir şekilde kullanılamamaktadır. Hatta iyi bir istatistik yapıldığı zaman , aslında kullanılamayan bant genişliğinin daha fazla olduğu gözlemlenebilmektedir

VoIP kullanıldığında ; ses aktivitesi tespiti yapılırsa , çöpe giden bu bant genişliği başka amaçlar için hizmet verebilir.

Konuşma genişliğinin düştüğü tespit edildiğinde ; VAD , konuşma yapılarının paketlenmesini durdurmadan önce zaman oranının sabitlenmesini bekler. Sabitlenmiş bu zaman aralığına *Hangover* denir.



Şekil 3-3 Ses aktivite tespiti

Daha sonra konulmanın başlaması ile kodlama ve gönderme işlemine devam edilecek, böylelikle konuşmanın yapılmadığı zaman aralıklarında boş paketler gönderilerek veri ağı gereksiz yere meşgul edilmeyecektir.

4. VOIP İŞARETLEŞME PROTOKOLLERİ

VoIP, teknik olarak ses veya görüntünün VoIP cihazları sayesinde sıkıştırılarak eş zamanlı bir şekilde hedef noktaya kadar internet üzerinden veri olarak gönderilmesi, hedef noktada sıkıştırılmış olarak gelen verinin sağlıklı ve eş zamanlı olarak açılarak görüşmenin yapılmasını sağlayan protokollerin bütünüdür.

VoIP teknolojisinde haberleşmeyi başlatmak için diğer haberleşme sistemlerinde olduğu gibi bir dizi sinyalleşmeye ihtiyaç duyulmaktadır. Örnek olarak Q.931 protokolü çağrı kurulumu ve H.323 ağ geçitleri veya son kullanıcılar arasındaki çağrıları sonlandırmada kullanılır.

H.225 de hemen hemen Q.931 ile aynı göreve sahiptir. RTCP (Real Time Control Protocol) ses akışı başladıktan sonra güvenli bir şekilde bilgi iletimini sağlar.

H.254 kontrol sinyalleşmesi, kanalların kullanımı ve kapasitesini değerlendirir. Ses iletiminde kullanılan belirli protokollerin hangi katmanda çalıştıkları katmanlar Tablo 4-1 OSI katmanları ve kullanılan protokollerde gösterilmiştir.

Tablo 4-1 OSI katmanları ve kullanılan protokoller

OSI KATMANLARI	KULLANILAN PROTOKOL
Presentation	G.711, G.729, G.729a, v.s
Session	H.323, H.245, H.225, RTCP,SIP
Transport	RTP, UDP
Net	IP, RSVP, WFQ
Link	RFC1717(PPP/ML), Frame, ATM, v.s

İnternet üzerinden ses taşımada iki önemli faz bulunmaktadır. Bunlar işaretleşme ve veri aktarım fazlarıdır. İşaretleşme esnasında güncel olarak iki önemli protokolden söz etmek mümkündür. Bunlar ITU'nün bir standardı olan H.323 ve IETF'in bir standardı olan oturum başlatma protokolü SIP'dir (Session Initiation Protocol). Bunlara ek olarak geçit yönetme protokolleri MGCP ve MEGACO da yaygın işaretleşme protokollerindendir. Veri aktarım fazı ise; işaretleşmeyle anlaşmaya varan ve senkronize olan iki uç birim cihazının birbirleriyle

gerçek zamanlı haberleşmeye başlamasıyla gerçekleşir. Veri aktarım protokolleri gerçek zaman kontrol protokolü RTP (Real time Transfer Protocol) ve kaynak ayırma protokolü (Resource Reservation Protocol- RSVP) ‘dür.

4.1 H.323

H.323, bir IP ağındaki ses, görüntü ve veri aktarımını sağlayan, Uluslararası Telekomünikasyon Standardizasyon Sektörü (ITU-T) ‘nün bir standardıdır. H.323 ‘ü kullanan cihazlar ve uygulamaları, birbirleri ile iletişim kurabilir ve ortak çalışmada bulunabilirler. H.323 standardı, çağrı iletişim ve kontrolünü, çoklu ortam (multimedia) iletimini ve kontrolünü, ayrıca noktadan noktaya ve noktalar arası konferanslar için bant genişliği kontrolünü yapar. H.323 standardı her son zamanlardaki revizyonlarla beraber daha bir bütünlük arz etse de, uzun zamanlı görüşmelerin kurulum zamanı, tam özellikli konferans görüşmeleri, her geçiş denetleyicisine bileşenlerinin aşırı sayıda özellik gerektirmesi ve ölçekleme gibi konularda yaşanan sıkıntılardan dolayı yavaş yavaş kullanımdan kalkmaktadır. PSTN bağlantısı için yüksek yoğunluklu ağ geçitlerine ihtiyaç duyulduğu zaman basit geçit kontrol protokolleri SGCP (Simple Gateway Control Protocol) ve MGCP (Media Gateway Control Protocol) gibi alternatiflere bakılması gerekecektir. Bu alternatif kontrol yöntemleri, daha etkili ve ölçeklenebilir çözümler sağlamaktadır. Bunlar gibi SIP de akıllı son noktalar kullanarak H.323’teki bazı problemleri çözebilmektedir ve günümüzde bir alternatif olarak gelişmektedir. H.323 standardında kullanılan protokoller Tablo 4-2 H323 bileşenlerinde listelenmiştir:

Tablo 4-2 H323 bileşenleri

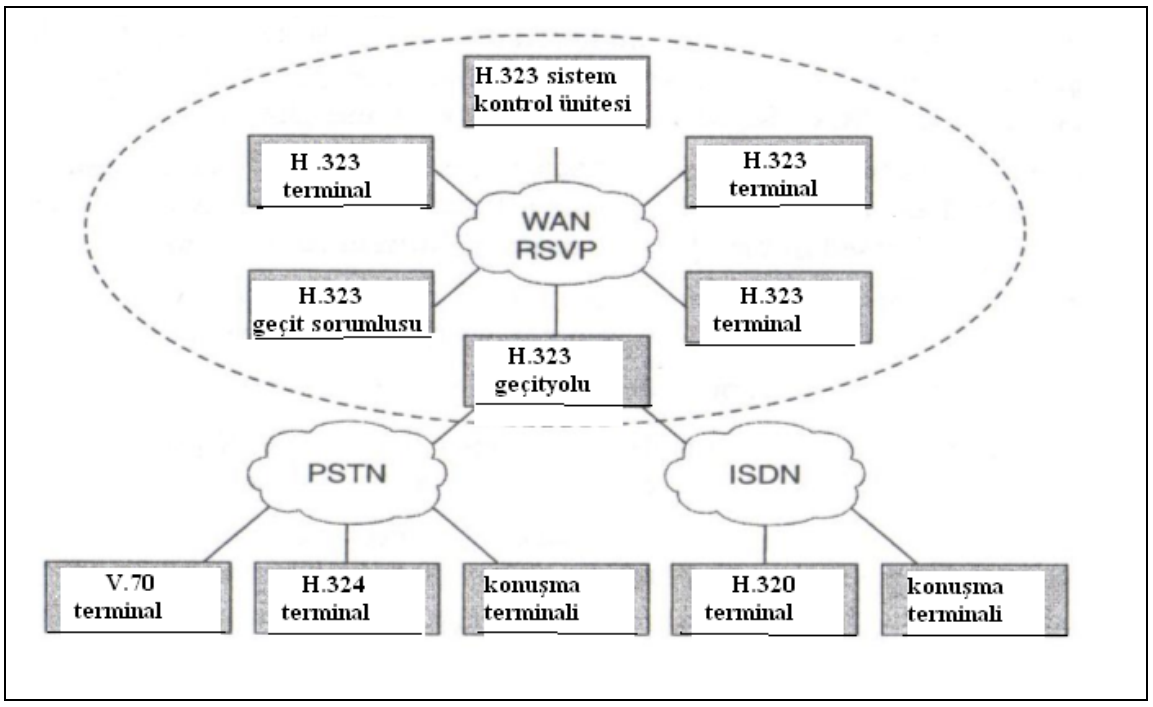
Özellik	Protokol
Çağrı sinyalizasyonu	H.323
Medya kontrolü	H.245
Ses Kodlayıcıları	G.711, G.722, G.723, G.728, G.729
Görüntü Kodlayıcıları	H.261, H.263
Veri Paylaşımı	T.120
Medya Aktarımı	RTP/ RTCP

H.323 sistemi üç bölümde incelenebilir;

- H.323 elemanları
- H.323 protokol takımı
- H.323 çağrı akışı

Şekil 4-1 H.323 ağının elemanları gösterilmektedir. Bu elemanlar; terminaller, geçitler (Gateway), geçiş denetleyicisine (Gatekeeper) ve çok noktalı kontrol ünitesi (MCU) 'dir.

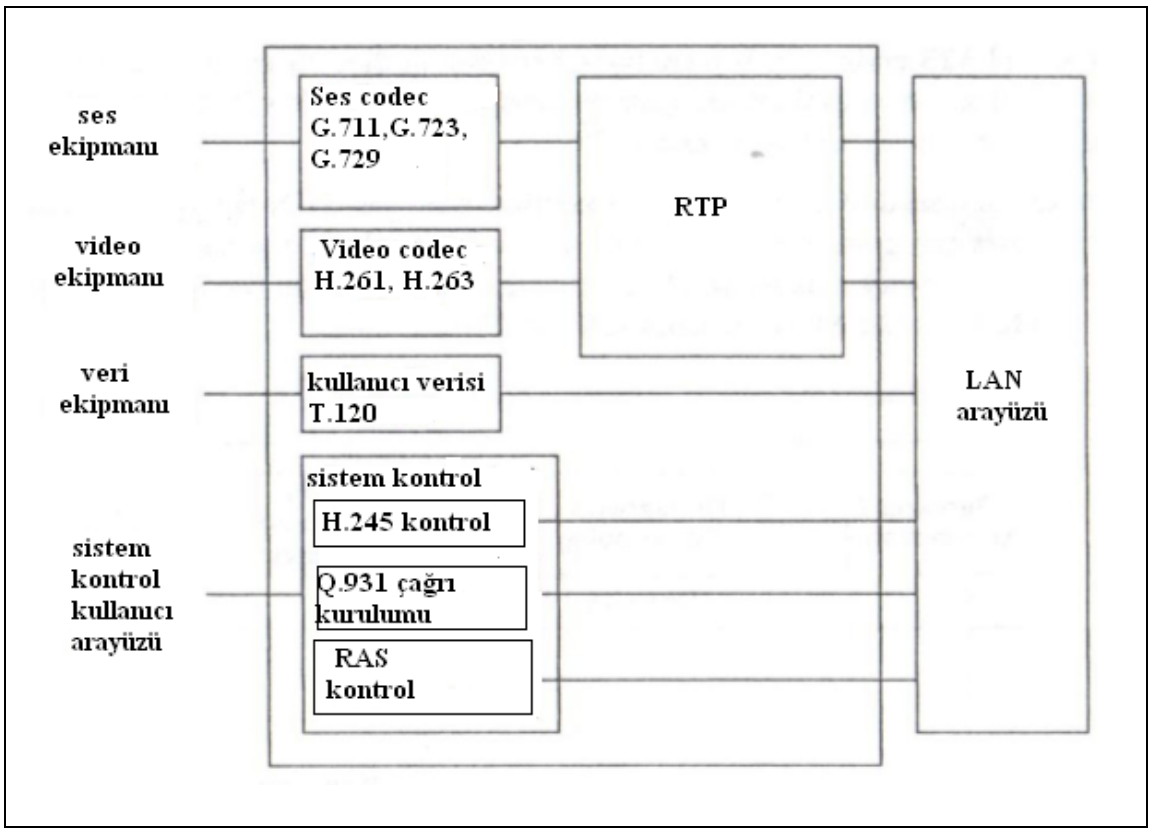
Terminaller; noktadan noktaya veya çok noktalı, ses ve isteğe bağlı olarak görüntü ve veri konferansını sağlar. Geçitler; PSTN veya ISDN ağlarına H.323 son nokta ortak çalışmaları için bağlanır. Geçiş denetleyicileri , terminaller ve geçitler için giriş kontrolü ve adres çevrimi aktarımı hizmetlerini verirler. Çok noktalı kontrol üniteleri (MCU), iki ya da daha fazla terminal ya da geçidin ses veya görüntü yoluyla konferansını sağlarlar.



Şekil 4-1 H.323 ağının elemanları

4.1.1 H323 Terminal

Şekil 4-2 H.323 bileşenlerinin ilişkisiŞekil 4-2 H.323 bileşenlerinin ilişkisi verilmiştir. H.323 terminali; sistem kontrol ünitesi, medya iletimi, ses kodlayıcısı ve paket tabanlı şebeke ara yüzüne sahip olmak zorundadır. İsteğe bağlı olarak video kodlayıcısı ve kullanıcı veri uygulaması içerebilir.



Şekil 4-2 H.323 bileşenlerinin ilişkisi

H.323 terminalinin fonksiyonları aşağıda açıklanmıştır:

- Sistem kontrol ünitesi: H.225 ve H.245 çağrı kontrolünü, kapasite değişimini, terminalin operasyonları için komutların sinyalizasyonunu ve mesajlaşmayı sağlar.
- Medya İletimi: İletilen ses, görüntü, veri ve kontrol akışlarını, mesajları biçimlendirir ve şebeke ara yüzüne gönderir. Aynı zamanda tüm bu bilgileri şebeke ara yüzünden alabilir.
- Ses Kodlayıcısı: Ses cihazından gelen sinyali iletim için şifreler ve gelen ses şifresini çözer. Gerekli fonksiyonları, ses şifreleme ve şifre çözme (G.711 , a-law ve μ-law kodlayıcıları) formatlarının iletimi ve alımıdır. İsteğe bağlı olarak şifreleme ve şifre çözme için G.722, G.723.1, G.728 ve G.729 kullanılabilir.
- Şebeke Ara yüzü: Paket tabanlı bir ara yüz; iletim kontrol protokolü (TCP) ve kullanıcı datagram protokolü (UDP) teke ve çoğa gönderim hizmetlerini sağlayabilir (unicast, multicast).

- Video Kodlayıcısı: İsteğe bağlı olarak bulundurulabilir ama H.261 QCIF ile uyumlu şifreleme ve şifre çözümü yapabilmelidir.
- Veri Kanalı: T.120 belirlenmiş veri tabanı erişimi, dosya transferi ve ses-grafik konferansı gibi uygulamaları destekler.

4.1.2 Ağ Geçiti (Gateway)

Ağ geçiti, ses içeren IP paketlerini ses ağının anlayabileceği biçime sokarak, iki kullanıcı arasındaki bağlantıyı kurar. VoIP ağ geçitleri PSTN ile veri ağı arasındaki geçiş noktasını göstermektedir. Ağ geçiti, yerel telefon santraliyle IP ağı arasında bir köprü görevi yapmaktadır. Ağ geçiti, yerel telefon santralından çevrilen bir telefon numarasını veri ağındaki bir adrese (IP adresi) dönüştürmektedir. IP ağ üzerinde kullanılan uygun protokollerin de yardımıyla bu telefon çağrısını algılayan hedef VoIP ağ geçiti aranan telefon numarasına yine yerel telefon santralı üzerinden bağlantıyı kurmaktadır. Ağ geçiti, PSTN ağları ile IP ağları arasındaki arayüz ya da geçiş elemanları olarak çalışan, birlikte çalışma fonksiyonlarını yerine getiren birimlerdir. Bir ağ geçiti, paket anahtarlamalı bir ağ üzerindeki H.323 uyumlu terminaller ile devre anahtarlamalı bir ağdaki diğer elemanlar veya diğer bir ağ geçiti arasında gerçek zamanlı çift yönlü trafik sağlayan bir ağda son nokta olarak çalışır. Ağ geçiti üç fonksiyonel birimden oluşur.

- Sinyalleşme Geçidi (Signalling Gateway; SG): SG, IP temelli ağ ile SCN (Switched Circuit Network) arasında işaretleşme bilgilerinin aktarımından sorumludur.
- Medya Geçidi (Media Gateway; MG): IP ağındaki kullanılan medya ile (örneğin /RTP/UDP/IP üzerinden taşınan medya) SCN ağda kullanılan medya (örneğin PCM kodlanmış ses ya da GSM vb.) arasındaki eşleme ve birbirine dönüşüm işlemlerinden sorumludur.
- Medya Geçit Kontrolcüsü (Media Gateway Controller; MGC): MGC; MG, SG ve geçiş denetleyicisine arasındaki iletişimleri düzenler. Ağ geçiti için gerekli çağrı işleme işlemlerini sağlar. MG'leri kontrol eder. SG'den gelen SCN işaretleşmeleri ve geçiş denetleyicisinden gelen IP işaretleşmeleri de MGC'ye gelir.

4.1.3 Geçiş Denetleyicisi (Gatekeeper):

Terminallerin ve ağ geçitlerinin kayıt, kabul ve statü (Registration, Admission and Status -RAS-) takibinden sorumlu olan ağ modülüdür. Geçiş denetleyicileri çağrı işleme/işaretleşme işlevlerini yerine getirirler. Aranan telefon numaralarının iletileceği ağ geçitlerinin IP adresleri geçiş denetleyicisinde ya da yazılımlar kullanılarak tutulur. Geçiş denetleyicileri aşağıda açıklanan fonksiyonları yerine getirirler.

- Adres Çevrimi: H.323 ve E.164 IP adreslerini sağlar.
- Giriş Kontrolü: ARQ, ACF, ARJ giriş mesajlarını kullanarak H.323'e etkili erişim sağlar.
- Bant Genişliği Kontrolü: BRQ, BCF, BRJ mesajlarını kullanarak bant genişliği son noktası kullanımını sağlar.

- Bölge İdaresi: Kayıtlı terminaller, ağ geçitleri ve MCU'lar için hizmet sağlar.
- İsteğe bağlı olarak, çağrı kontrol sinyalizasyonu, çağrı izni, bant genişliği idaresi ve çağrı idaresi gibi hizmetler de sağlayabilir.

4.1.4 Çok Noktalı Kontrol Ünitesi (Multi-point Control Unit -MCU)

MCU ağda ikiden fazla terminalin ya da ağ geçitinin çoklu bir konferansa katılımlarını sağlamaya yarayan cihazlardır. Sonradan çoklu bir konferansa dönüşebilecek ikili görüşmeler de MCU'lar aracılığı ile sağlanabilir. MCU iki kısımdan oluşur. Bunlar çoklu nokta kontrolü (Multipoint Controller; MC) ve çoklu nokta işlemcisi (Multipoint Processor; MP) olarak adlandırılır. MC'nin bulunması zorunlu iken MP'nin bulunması zorunlu değildir. MC konferansa katılacak bütün terminallerin ortak iletişim seviyelerinde bulunmalarını sağlamak için çağrı süreçlerine, iletişim parametreleri üzerindeki uzlaşmaları (negotiation) sağlar. MP, MC'nin denetiminde medya akışlarının işlenmesi (harmanlama, anahtarlama vb.) görevlerini yürütür. MP, yürütülen konferansın tipine göre tek bir bağlantıyı ya da daha çok bağlantıyı işleyebilir. En basit hali ile MCU tek bir MC'den oluşur.

4.1.5 Vekil Sunucu (Proxy Server)

H.323 vekil sunucular H.323 protokolü için özel olarak tasarlanmışlardır. Vekil sunucu uygulama katmanında çalışmaktadır ve iletişim halindeki iki uygulama arasındaki paketleri kontrol etmektedir. Vekil sunucular bir konuşmanın gidişini belirleyebilir ve istenirse bağlantıyı kurabilir. Vekil sunucular aşağıda açıklanan işlevleri sağlamaktadırlar:

- RSVP'yi desteklemeyen terminaller vekil sunucu ile doğrudan veya LAN üzerinden erişim sağlayabilirler ve benzer kalitede servis hizmeti alabilirler.
- Vekil sunucu H.323'ün trafiğini ASR'in normal trafiğinden ayırmayı sağlarlar.
- Vekil sunucu ağ adres çevrimiyle uyumludur ve H.323 düğümlerinin özel adres boşlukları ile ağların uygun yerlerine yerleştirilmesine olanak verir.
- Vekil sunucunun güvenlik duvarı olmadan ya da güvenlik duvarından bağımsız olarak belli bir güvenlik sağlar. Bunun nedeni sadece H.323 trafiğinin vekil sunucu üzerinden akmasıdır.

4.1.6 H.323 Protokol Takımı ve Kullandığı Mesajlar

H.323 Protokol takımı Tablo 4-2 H323 bileşenlerinde görülen birçok protokol üzerine kuruludur. Protokol ailesi; H.323 sistemlerindeki çağrı girişleri, çağrı kurulumu, çağrı durumu, çağrının kesilmesi, medya dizgilerini ve mesajları desteklemektedir. Protokoller hem güvenilir hem de güvenilir olmayan paket iletim mekanizmaları tarafından desteklenmektedir. H.323 uygulamalarının çoğu iletim mekanizması için TCP'yi kullansa da H.323 versiyon 2

UDP iletimini olanaklı kılar. Uzmanlar halen güvenilir UDP mekanizmaları üzerine çalışmaktadırlar.

H.323 protokol takımı üç ana kontrol sahası üzerinde çalışır.

- RAS sinyalizasyonu: Ağ tabanlı H.323 geçiş denetleyicisinde çağrı öncesi kontrolü sağlar.
- Çağrı kontrol sinyalizasyonu: Son noktalar arasındaki bağlantıyı kurmada, korumada ve sonlandırmada kullanılır.
- Medya kontrol ve iletimi: Medya kontrol mesajı taşıyan güvenilir bir H.245 kanalı sağlar. İletim güvenilir olmayan bir UDP dizgisi üzerinden gerçekleşir.

4.1.7 Ras Sinyalizasyonu

RAS sinyalizasyonu geçiş denetleyicileri için H.323 şebekesinde çağrı öncesi kontrolü sağlar. RAS kanalı ağ üzerinde, son noktalar ve geçiş denetleyicileri arasında bulunur. RAS kanalı diğer kanallardan daha önceden açılmıştır ve çağrı kontrol sinyalizasyonu ve de medya iletim kanallarından bağımsızdır. Güvenilir olmayan bu UDP bağlantısı; kayıt, giriş, bant genişliği değişimleri, bant genişliği durumları ve serbest prosedürleri gerçekleştiren RAS mesajlarını taşır.

4.1.8 Geçiş Denetleyicisi Keşfi

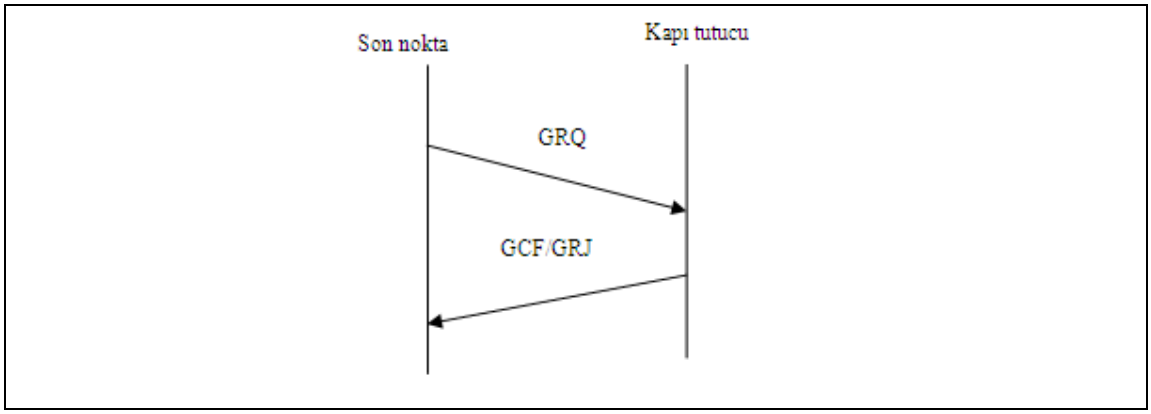
Geçiş denetleyicisi keşfi hangi geçiş denetleyicisinde kayıtlı olunduğunu bulmak için kullanıcı tarafından yada otomatik işlem yapan bir son nokta tarafından gerçekleştirilmektedir. Kullanıcı tarafından olan yöntemde son noktalar geçiş denetleyicileri nin IP adresiyle yapılandırılmıştır. Dolayısıyla kayıt işlemine sadece önceden tanımlanmış geçi denetleyicileri ile başlanabilir. Otomatik metotta ise zamanla değiştirilebilmesi için son noktalar ve geçiş denetleyicileri arasında bir ilişkiye olanak sağlanır. Ama bunu yapabilmek için “otomatik keşif (auto discovery)” olarak bilinen bir mekanizmaya ihtiyaç duyulur.

Otomatik keşif; kendi geçiş denetleyicisini tanıyamayan bir son noktaya, çoğa gönderim (multicast) mesajı ile kendi geçiş denetleyicisini keşfetmesini sağlar. Çünkü son noktaların statik bir tasarımı yoktur ve geçiş denetleyicisi için tekrar tasarlanmamışlardır. Geçiş denetleyicisi keşfi çoğa gönderim adresi 224.0.1.41, Geçiş denetleyicisine UDP keşif portu 1718, ve geçiş denetleyicisine UDP kayıt ve statü portu 1719’dur. Aşağıda açıklanan üç RAS mesajı H.323 geçiş denetleyicisine otomatik keşfi için kullanılır.

- Geçiş denetleyicisine isteği (GRQ): Geçiş denetleyicisine arayan bir son nokta tarafından gönderilen çoğa gönderim mesajı.
- Geçiş denetleyicisine Teyidi (GCF): Geçiş denetleyicisinin RAS kanalının iletim

adresini içeren ve son noktanın GRQ isteğine cevap veren bir mesaj.

- Geçiş denetleyicisine Reject (GRJ): Son noktaya, geçiş denetleyicisinin son noktanın kayıt isteğini reddettiğine dair mesajdır. Bu olayla genelde, ağ geçiti veya geçiş denetleyicisine üzerinden yapılan bir tasarım nedeniyle karşılaşılır.



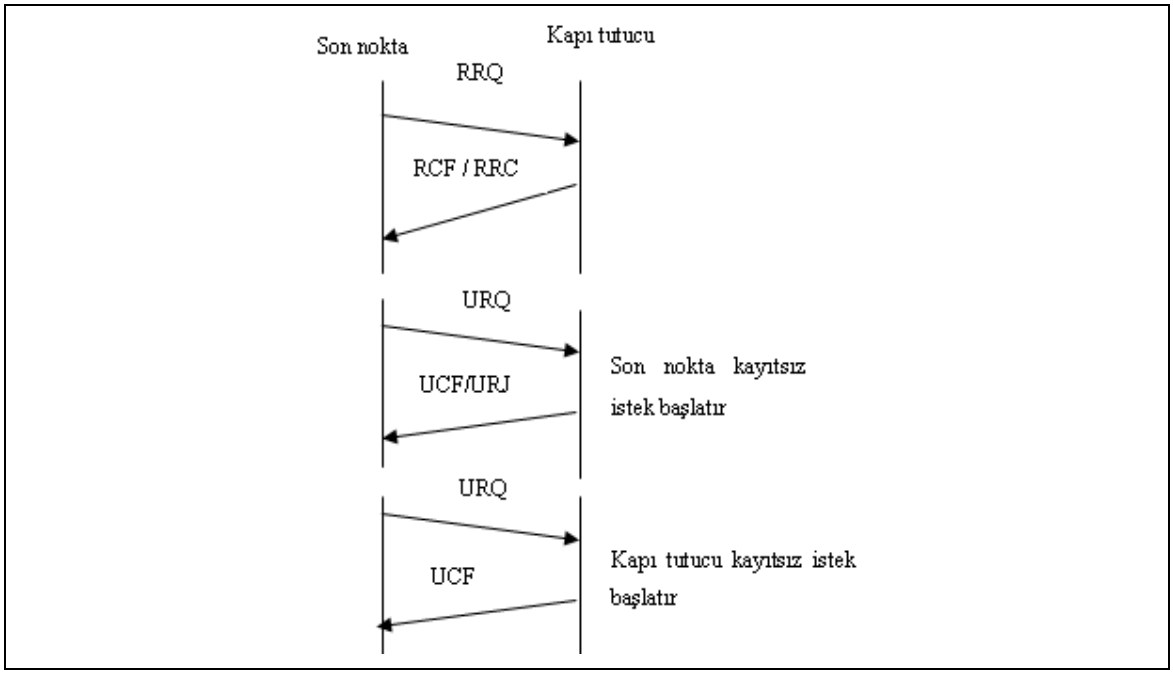
Şekil 4-3 Otomatik keşif ile mesajlaşma ve oluşan işlemler zinciri.

Geçiş denetleyicisine, GCF mesajlarında alternatif geçiş denetleyicilerini keşfedebilir. Öncelikli geçiş denetleyicisine ile çalışılamazsa alternatifleri kullanılabilir.

4.1.9 Kayıt

Kayıt işlemi; ağ geçitlerin, son noktaları ve MCU'ları bir bölgeye toplar ve IP bilgileri ile takma (alias) adresler konusunda geçiş denetleyicisini bilgilendirir. Kayıt işlemi, keşif işleminden sonra gerçekleşir. Aşağıda belirtilen 6 adet mesaj, kayıt ve kaydın iptali için kullanılır.

- RRQ: Bir son nokta tarafından geçiş denetleyicisinin RAS kanal adresine yollanan kayıt istek mesajı.
- RCF: Geçiş denetleyicisine tarafından yollanan ve son noktanın kaydını doğrulayan mesaj.
- RRJ: Geçiş denetleyicisine tarafından yollanan ve son noktanın kayıt isteğini reddeden mesaj.
- URQ: Bir son nokta tarafından geçiş denetleyicisine yollanan ve kayıt isteğini iptal eden mesaj.
- UCF: Bir son nokta veya geçiş denetleyicisine tarafından yollanan ve kayıt iptalini doğrulayan mesaj.
- URJ: Son noktanın geçiş denetleyicisine ile ön kayıtlı olmadığını bildiren mesaj.



Şekil 4-4 Son nokta ve geçiş denetleyicisine arasındaki mesajlaşma.

4.1.9.1 Son Nokta Yeri

Son noktalar sadece takma (alias) bilgi ile arama başlatılmak istendiğinde aramayı sağlamak için geçiş denetleyicileri nden son nokta yerini sorgularlar. Yer adresleri geçiş denetleyicisin RAS kanal adresine ya da çoğa gönderimle geçiş denetleyicisinin keşif çoğa gönderim adresine yollanır. Geçiş denetleyicisine arayan son noktaya aranacak son noktanın kontak bilgisini gönderir. Aşağıda anlatılan üç mesaj son noktaların yerini sorgulamak için kullanılmaktadır:

- LRQ: Son noktanın ya da geçiş denetleyicisin kontak bilgisinin bir veya daha çok E.164 adresi için istenmesi.
- LCF: Geçiş denetleyicisine tarafından gönderilen ve çağrı sinyalizasyon kanalı veya kendinin ya da istekte bulunan son noktanın adresini içeren mesajdır. Geçiş denetleyicisi tarafından yönlendirilmiş arama sinyalleşmesi GKRCS (Gatekeeper Routed Call Signaling) kullanıldığında kendi, DECS kullanıldığında ise son noktanın adresini içerir.
- LRJ: Geçiş denetleyicisine tarafından LRQ'ya karşılık son noktanın kaydının yapılmadığını ya da ulaşılamaz kaynaktan olduğunu içeren mesajdır.

4.1.9.2 Kabul/Giriş

Son nokta ve geçiş denetleyicileri arasındaki çağrı ve bant genişliği kontrolü ile ilgili bilgi alışverişi yapılmaktadır. Geçiş denetleyicileri bir giriş isteğini kabul ederek veya reddederek

H.323 şebekesine erişimi denetlemektedirler. Aşağıda açıklanan mesajlar H.323 şebekesine giriş kontrolünü sağlamaktadırlar.

- ARQ: Bir son nokta tarafından, bir çağrı kabulü için girişimi gösterir.
- ACF: Geçiş denetleyicisine tarafından çağrı için izin verildiğini gösterir.
- ARJ: Son noktanın bu çağrı için şebekeye erişimine izin verilmediğini gösterir.

ACF mesajı, engelleyen ya da çağrıyı başlatan ağ geçitinin veya geçiş denetleyicisinin IP adresini içerir.

4.1.9.3 Durum Bilgisi

Geçiş denetleyicisine, RAS kanalını kullanarak herhangi bir son noktanın durum bilgisine ulaşabilir. Başarısız bir denemeden sonra son noktanın etkin ya da boşta olup olmadığını öğrenilebilir. Durum mesajları için tipik yoklama süresi 10 saniyedir. Aynı zamanda ACF mesajıyla geçiş denetleyicisine, son noktadan çağrı boyunca periyodik durum bilgisi isteyebilir. Aşağıdaki mesajlar bu işlemler için kullanılmaktadır:

- IRQ: Geçiş denetleyicisinden son noktaya gönderilen ve durum bilgisini isteyen ileti.
- IRR: Son noktadan geçiş denetleyicisine IRQ mesajının bir cevabı olarak yollanır. Bu mesaj aynı zamanda, geçiş denetleyicisinin son noktadan periyodik durum bilgisi istediği durumlarda yollanır.
- Status Enquiry: RAS kanalından çağrı sinyali kanalına yollanır. Bir son nokta veya geçiş denetleyicisine tarafında, başka bir son noktaya çağrı durumunu doğrulamak için yollanır. Genel olarak geçiş denetleyicileri tarafından kullanılan bu mesaj çağrıların aktif olup olmadığını kontrol eder.

4.1.9.4 Bant Genişliği Kontrolü

Bant genişliği kontrolü öncelikli olarak bir son nokta ile geçiş denetleyicisine arasında ARQ/ ACF/ ARJ mesaj dizisi ile gerçekleştirilir. Bant genişliği çağrı esnasında değişebilir. Aşağıda açıklanan mesajlar bant genişliğini değiştirmek için kullanılmaktadır:

- BRQ: Son nokta tarafından geçiş denetleyicisine yollanan ve çağrı bant genişliğini azaltmak veya arttırmak için kullanılan mesaj.
- BCF: Geçiş denetleyicisine tarafından yollanan ve bant genişliği değişikliği isteğinin kabul edildiğini ileten mesaj.
- BRJ: Geçiş denetleyicisine tarafından bant genişliği isteğinin reddedildiğini ileten mesaj. (istenen bant genişliğin sağlanamadığı durumlarda gönderilir).

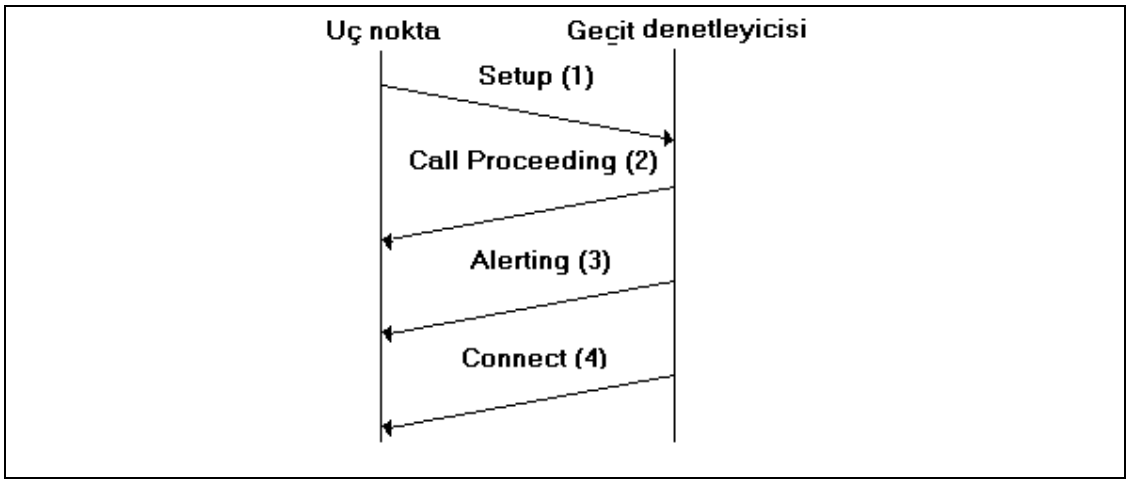
4.1.9.5 Çağrı Kontrolü

H.323 şebekelerinde çağrı kontrolü sinyalizasyon prosedürleri ITU tarafından önerilen H.225 temellidir. H.225, Q.931 sinyal mesajlarını destekler. IP şebekeleri ile TCP port 1720 arasında güvenilir bir çağrı kontrolü kanalı yaratılmıştır. Bu port, iki son nokta arasında

çağrıların bağlanmasını, bağlantının korunmasını ve bağlantının kesilmesini sağlayan Q.931 çağrı kontrol mesajlarının başlamasını sağlar.

Güncel çağrı kontrol mesajları, ilk çağrı kurulmasından sonra geçici portlara taşınırlar. Fakat port 1720; H.323 çağrıları için tanınan bir porttur. H.225 aynı zamanda ek hizmetler için Q.932 mesajlarının kullanımını belirler. Aşağıda açıklanan Q.931 ve Q.932 mesajları, H.323 şebekelerinde en çok kullanılan sinyalizasyon mesajlarıdır.

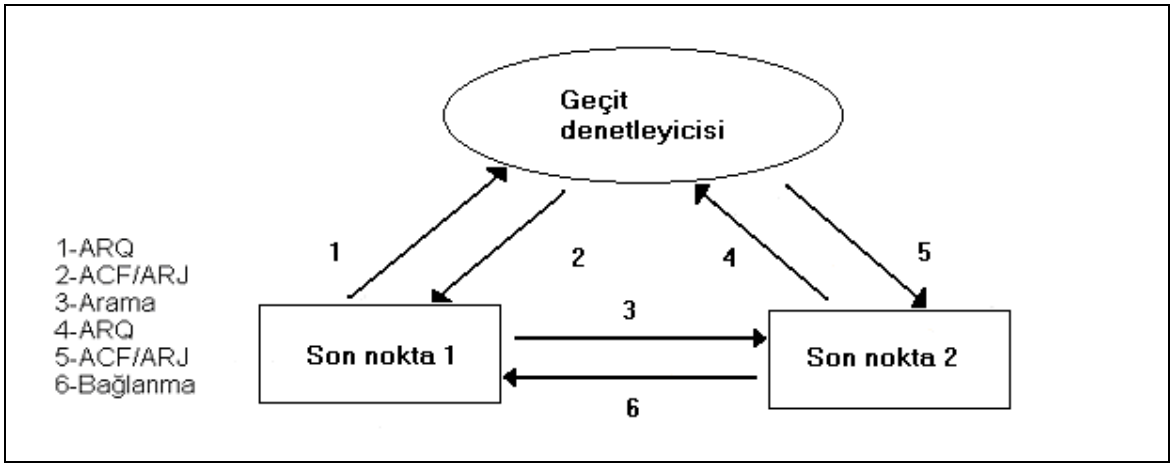
- Setup: Arayan H.323'ten, aranan H.323'e gönderiler ve bağlantı kurma girişimini gösterir. Bu mesaj, H.225'in TCP portu 1720 üzerinden iletilir.
- Call Proceeding: Aranan H.323 arayana cevap verir ve bağlantı prosedürlerinin kabul edildiğini gösterir
- Alerting: Aranan H.323; arayana, aranan cihazın çaldığını gösterir. (örneğin, telefon karşı tarafta çalıyor)
- Connect: Aranan H.323; arayana, aranan cihazda çağrıya cevap verildiğini iletiyor. (karşı taraftan telefon açılıyor)
- Release Complete: Son nokta tarafından bağlantının bittiğini belirtmek için yollanan mesajdır. Bu mesaj, sadece çağrı sinyalizasyon kanalının açık veya aktif olduğu zamanlarda yollanır.
- Facility: Ek hizmetler isteyen ya da aldığını bildiren bir Q.932 mesajıdır. Bu mesaj aynı zamanda bir çağrının doğrudan mı yoksa bir geçiş denetleyicisine üzerinden mi yapıldığını belirtir.



Şekil 4-5 Çağrı kurulumu için yapılan mesajlaşmalar

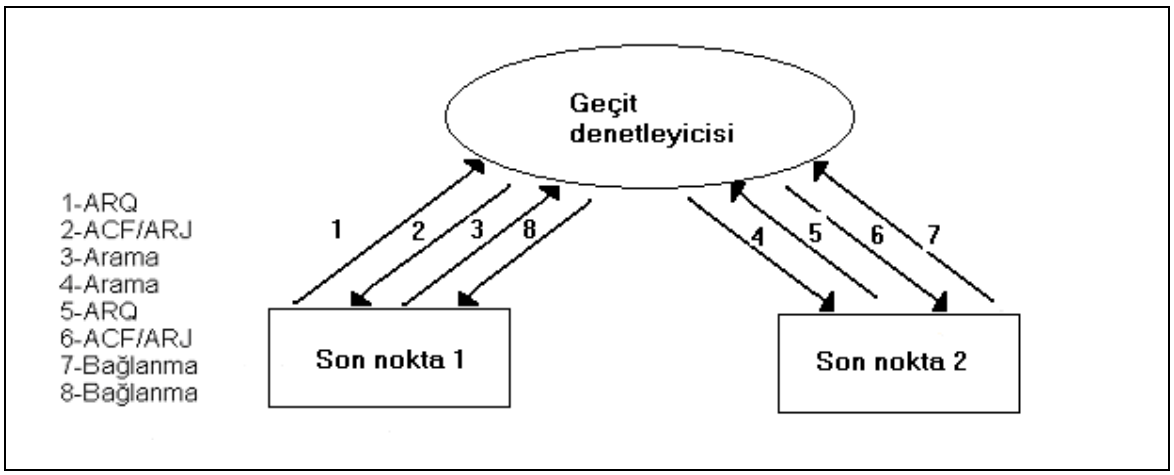
H.323 şebekesinde sinyalizasyon mesajlarını iki şekilde yönlendirilebilir.

DECS metodunda çağrı sinyalizasyonu mesajları doğrudan iki son nokta arasında kurulur.



Şekil 4-6 DECS türü çağrı kurulumu

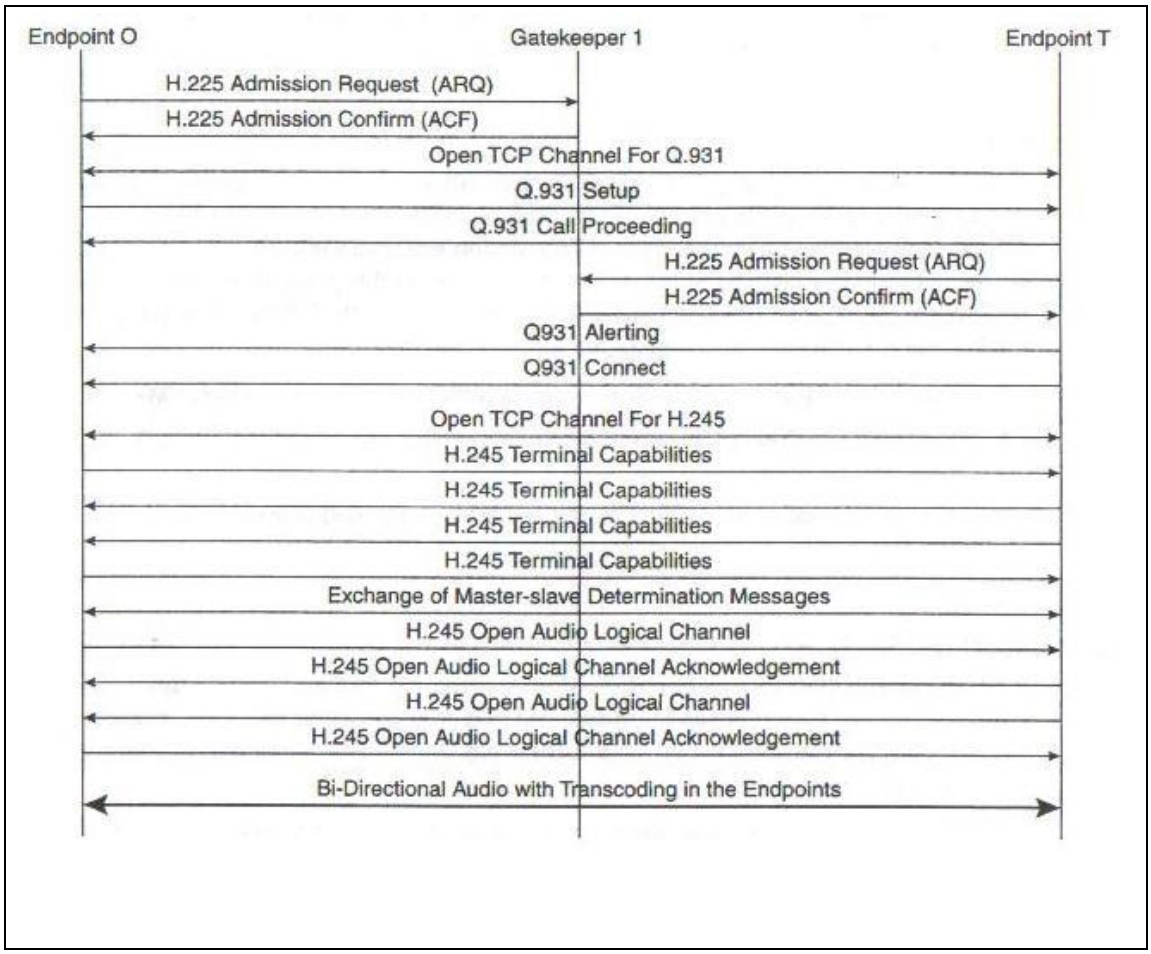
GKRCS metodunda ise, çağrı sinyalizasyonu mesajları geçiş denetleyicisine üzerinden iletilir.



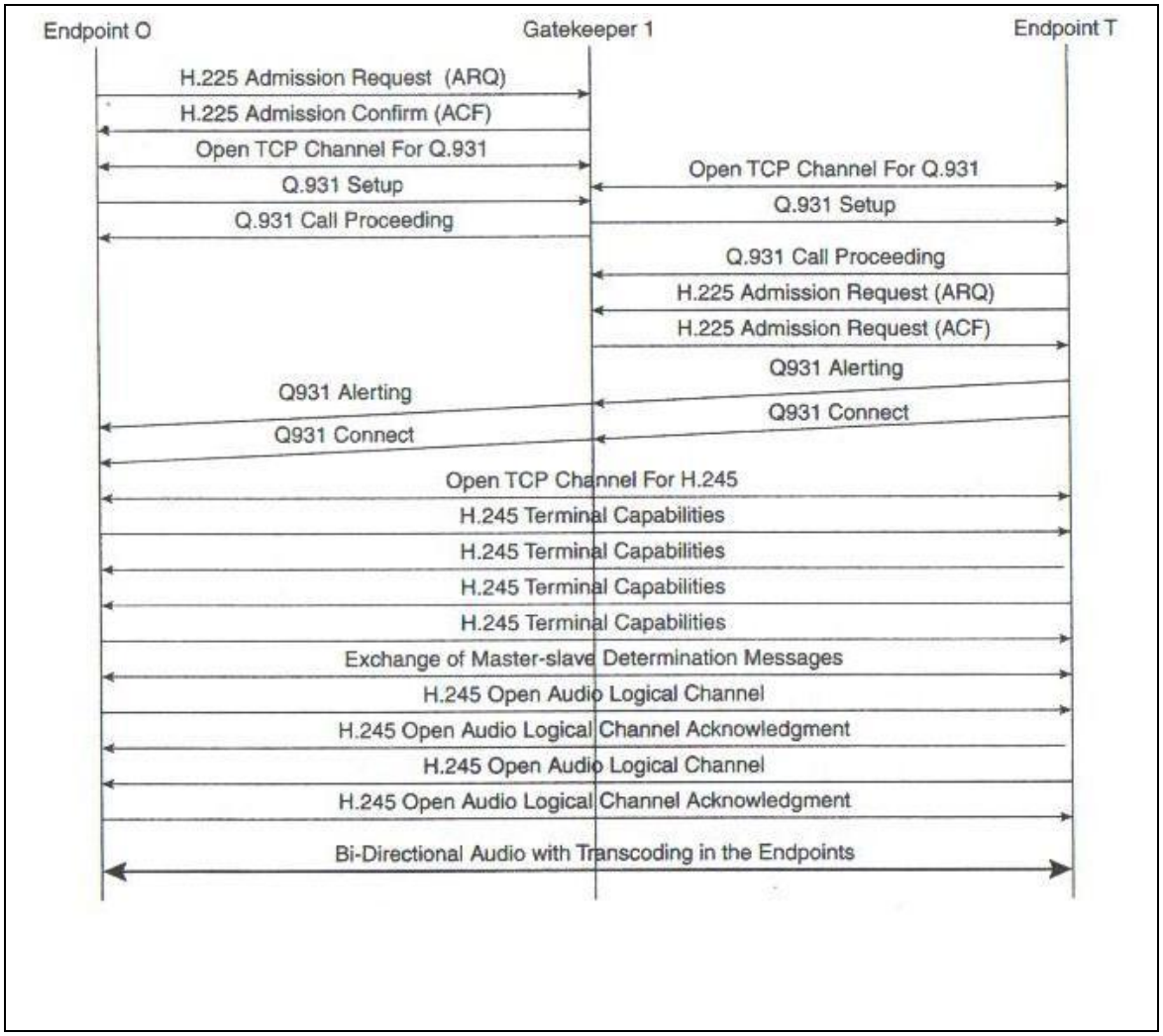
Şekil 4-7 GKRCS türü çağrı kurulumu

Şekil 4-6 DECSŞekil 4-6 DECS ve Şekil 4-7 GKRCSŞekil 4-7 GKRCS türü çağrı kurulumunu anlatmaktadır. 3 ve 6 mesajları çağrı sinyalizasyonu kanalı mesajlarıdır. Diğer mesajlar ise daha önce incelenen RAS kanal mesajlarıdır. Şekil 4-8 Bir geçiş denetleyicisi ile DECS sinyalizasyonuŞekil 4-8 Bir geçiş denetleyicisi ile DECS sinyalizasyonu, Şekil 4-9 Bir geçiş denetleyicisi GKRCS sinyalizasyonuŞekil 4-9 Bir geçiş denetleyicisi GKRCS sinyalizasyonu Şekil 4-10 İki geçiş denetleyicisi ile DECS sinyalizasyonuŞekil 4-10 İki geçiş denetleyicisi ile DECS sinyalizasyonu,

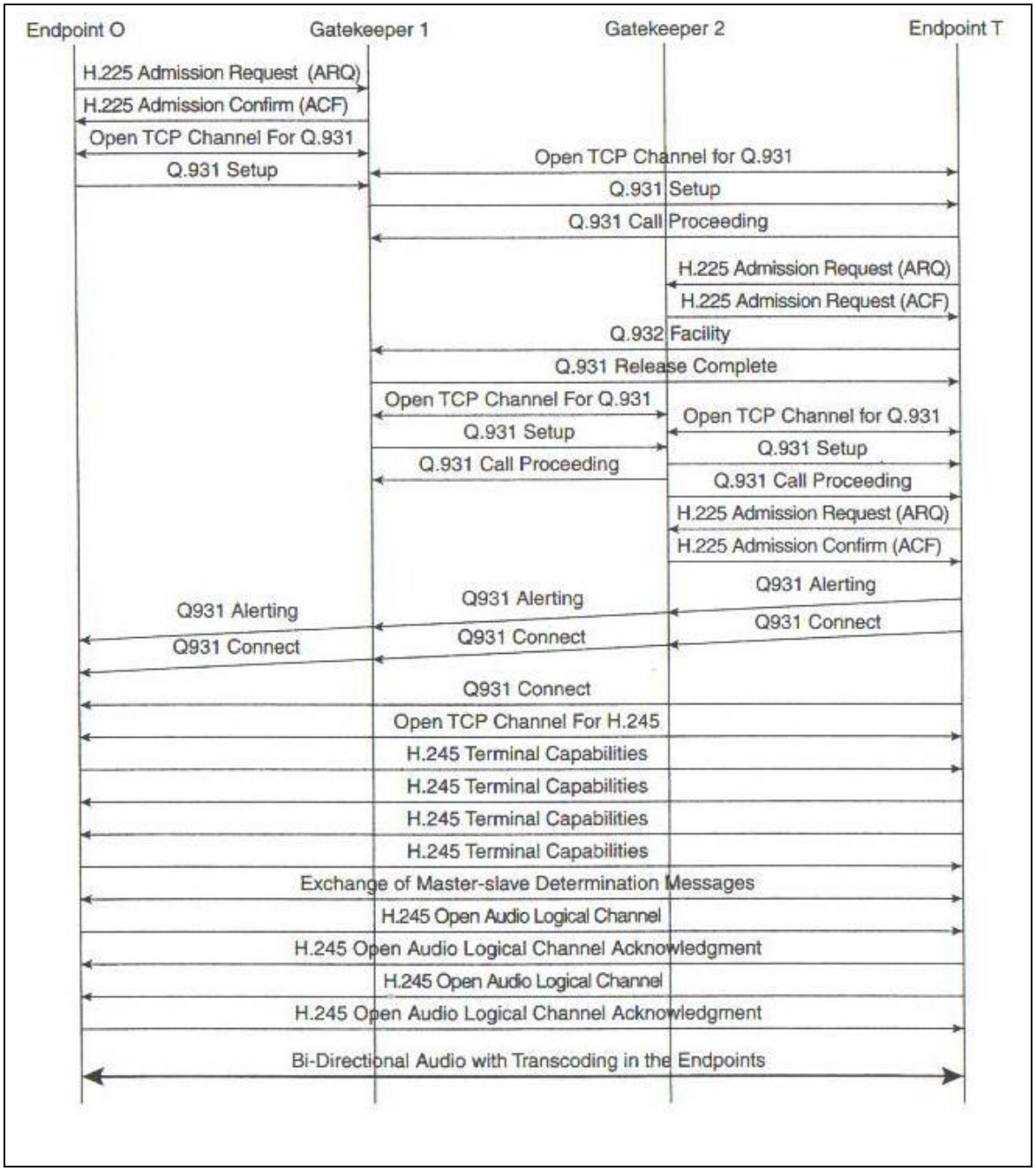
Şekil 4-11 İki geçiş denetleyicisi ile GKRCS sinyalizasyonuŞekil 4-11 İki geçiş denetleyicisi ile GKRCS sinyalizasyonu akışları örneklenmiştir.



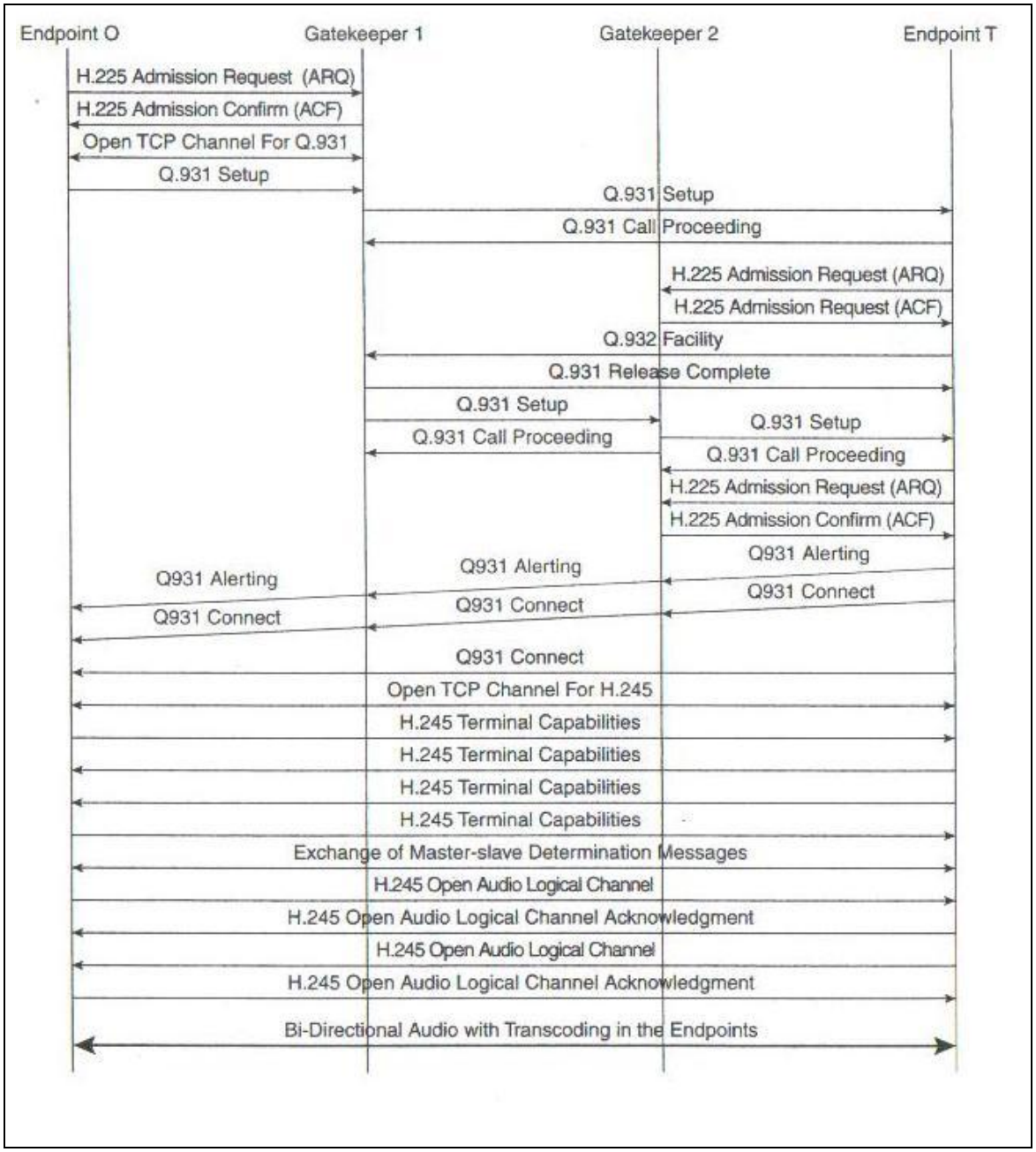
Şekil 4-8 Bir geçiş denetleyicisi ile DECS sinyalizasyonu



Şekil 4-9 Bir geçiş denetleyicisi GKRCS sinyalizasyonu



Şekil 4-10 İki geçiş denetleyicisi ile DECS sinyalizasyonu



Şekil 4-11 İki geçiş denetleyicisi ile GKRCS sinyalizasyonu

4.1.9.6 Ortam Kontrolü ve İletimi (H.245 ve RTP/ RTCP)

H.245, H.323'ler arası kontrol mesajlarını idare etmektedir. H.245 prosedürleri ses, görüntü, veri ve kontrol kanalı bilgisi iletimi için sanal kanallar kurmaktadır. Bir son nokta, temas kurduğu bir diğer son nokta için her çağrıda bir H.245 kanalı kurmaktadır. Son çağrı sinyalizasyonu ile IP üzerinden tahsis edilen bir TCP portu, güvenilir bir kontrol kanalı olarak yaratılmaktadır.

Bu kontrol kanalı ile sanal kanalların açılması ve kapanması, öncelikli yolların belirlenmesi ve mesaj kontrolü gibi işlemler gerçekleştirilir.

Aşağıdaki prosedürler ve mesajlar H.245 kontrolünü olanaklı kılar.

- Kapasite değişimi (Capability Exchange) : İki son nokta arasın kapasite değişiminin güvenli bir şekilde yapılabileceğini iletir. Bu mesaj; ses, görüntü ve veri iletimi için terminalin kapasitesini temas kurulan terminale iletir. Ses için, değişim kapasitesi G serilerinde; G.729 için 8 Kbps, G.728 için 16 Kbps, G.711 için 64 Kbps, G.723 için 5.3 veya 6.3 Kbps, G.722 için 48,56 ve 64 Kbps. ISO serileri için; IS.11172-3 ile 32,44.1 ve 48 KHz örnekleme hızı, IS.13818-3 ile 16, 22.05, 224, 32, 44.1 ve 48 KHz örnekleme hızı verir.
- Birincil ikincil saptaması (Master- Slave Termination) : Prosedürsel ortak bir arama için hangi noktanın birincil hangisinin ikincil oluğunu saptamak için kullanılır. Bu ilişki tüm çağrı boyunca korunur ve son noktalar arasındaki uyuşmazlıkları çözmek için kullanılır. Aynı zamanda birincil- ikincil ilişki kuralı , iki son noktanın aynı anda benzer işlemler istediği zaman kullanılır.
- Round- Trip gecikmesi : Prosedürler, arayan son noktayla aranan son nokta arasındaki gecikmeleri saptamak için kullanılır. ' RoundTripDelayRequest ' mesajı iki son nokta arasındaki gecikmeyi ölçer ve uzaktaki H.245 protokolü aktif midir tespitini yapar.
- Mantıksak Kanal Sinyalleşmesi (Logical Channel Signaling): Ses, görüntü ve veri bilgisi taşıyan mantıksal kanallar açılır ve kapanır . Kanal, terminallerin bilgi alma ve kod çözme işlemleri için hazır olduğunu garanti altına almak için mevcut gönderimden önce kurulmaktadır. Tek ve çok yönlü kanallarda da aynı sinyalizasyon mesajları kullanılmaktadır. Mantıksal kanal sinyalizasyonu başarılı bir şekilde kurulduktan sonra, RTP akışı son noktalar arasında ilerler. Aynı zamanda GKRCS modelini kullandığımızda bu nokta; mevcut UDP/IP adresinden sağladığımız ve ikinci son noktaya gönderdiğimiz RTP dizilerinin geçiş denetleyicisine tarafından yönünün saptırıldığı noktadır.

4.1.9.7 Çağrı Sonlanması

Herhangi bir son nokta çağrı sonlandırılması prosedürlerini başlatabilir. Öncelikli olarak bir son nokta ortam transferini durdurmalı ve tüm mantıksal kanalları kapatmalıdır. Daha sonra H.245 oturumunu sonlandırmalı ve sinyalizasyon kanalına bir mesaj yollamalıdır. Bu noktada geçiş denetleyicisine yok ise çağrı sonlandırılır. Eğer bir geçiş denetleyicisine mevcut ise, mesaj RAS kanalında çağrıyı sonlandırmak için kullanılır.

- DRQ : Bir son nokta ya da geçiş denetleyicisine tarafından çağrıyı sonlandırmak için yollanır.
- DCF : Bir son nokta ya da geçiş denetleyicisine tarafından yollanan ve bağlantının koptuğunu doğrulayan mesaj.
- DRJ : Bir son nokta ya da geçiş denetleyicisine tarafından yollanan ve bağlantının kopmasını reddeden mesaj.

4.2 SIP

SIP, çoklu ortam oturumlarını kurmak, korumak ve sonlandırmak için kullanılan kontrol protokolüdür. Çoklu oturumlar; internet telefonculuğu, konferanslar ve anında mesajlaşma dosya paylaşımı ve benzeri uygulamaları kapsamaktadır. Bu uygulamalar; ses, görüntü ve veri iletişimini gerektirmektedir. SIP' i birçok farklı türde oturumu başlatmak ve yönetmek için kullanılmaktadır. SIP tek noktadan tek noktaya yada çok noktadan çok noktaya oturumları başarıyla destekler.

RFC (Request For Comments) üzerine kurulu olan SIP, IETF (Internet Engineering Task Force) çoklu ortam mimarisinden yararlanan metin temelli bir protokoldür. SIP, H.323 gibi diğer sinyalizasyon protokolleri ile ortak çalışabilir.

İnternet telefonculuğu halen gelişmektedir ve ek sinyalizasyon uygulamalarına ihtiyaç duyulmaktadır. SIP' in gelişmesi bu diğer uygulamaların da gelişmesi demektir. SIP mesaj başlıkları çok yönlüdür ve ek düzenlemeler dahil edilebilir. Ayrıca SIP' in esnekliği gelişmiş telefon hizmetleri için bir olanak sağlamaktadır.

Bu bölümde SIP' in temelleri üzerinde durulacaktır. Bu temeller aşağıdaki üç konuyu kapsamaktadır.

- SIP' in genel şeması : Bileşenleri, adresleme ve çağrılar.
- Mesajlar : Başlıklar, talepler ve cevaplar.
- Temel çalışması : Vekil ve direk olmayan sunucu çalışması.

Sip aşağıdaki temel bileşenlerden oluşmaktadır:

4.2.1 Kullanıcı Araçları

Kullanıcı araçları, alıcı son nokta uygulamasıdır. Bir istemci alıcı aracı (user-agent client UAC), bir de sunucu alıcı aracı (user-agent server UAS) kısımlarından oluşmaktadır.

- Alıcı: SIP taleplerini başlatır ve kullanıcı çağrı cihazı olarak görev yapar.

- Sunucu : Talepleri alır ve istemciye cevap verir.

4.2.2 Ağ Sunucuları

İki tip SIP ağ sunucusu vardır. Vekil sunucular ve adres değiştiren sunucular (indirect servers).

4.2.2.1 Vekil Sunucu

Hem alıcı hem de sunucu fonksiyonlarını yerine getirmektedir. Bir vekil sunucu; bir kullanıcı sunucusundan gelen isteklerin başlıklarını diğer sunuculara göndermeden önce tercüme edebilmekte ve başlıkları yeniden yazabilmektedir. Başlıkların yeniden yazımı, vekil sunucuyu talep başlatıcısı olarak gösterebilmekte ve cevapların aynı yoldan gönderilmesini sağlayabilmektedir.

4.2.2.2 Adres Değiştiren Sunucular

SIP' in taleplerindeki alıcı ve sucu adreslerini değiştirme özelliklerine sahiptirler. Vekil sunucu adresini saklayarak olası saldırılara karşı güvenlik sağlamak amacıyla yaygın olarak kullanıl maktadır. Aynı zamanda ağ adres değiştirme protokolünden kaynaklanan problemleri gidermek amacıylada (NAT) kullanılabilmektedir.

4.2.3 Adresleme

SIP adresleri URL (Universal Resource Locater), user@hosts formundadır. E-mail adreslerine benzer şekilde bir SIP adresi user@hosts şeklinde tanınır. Adresin "user" olan kısmı kullanıcı adı veya telefon numarası olabilir, "host" kısmı ise alan adı olabileceği gibi bir şebeke adresi de olabilir. Bir kullanıcının SIP adresi e-mail adresinden bulunabilir. Aşağıda iki çeşit SIP adresi gösterimi vardır.

yildizpress@yildiz.com ya da 4085262222@171.171.171.1

4.2.4 Bir Sunucunun Yeri

Bir alıcı, bir SIP talebini direkt olarak yerel bir vekil sunucu üzerinden ya da uygun SIP adresinin IP adresine yollayabilir. İlk yöntem kolaydır ve son sistem uygulaması vekil

sunucuyu tanıyordur. İkinci yöntem ise aşağıdaki sebeplerden dolayı daha karışıktır:

- Alıcı talebin gönderildiği sunucunu IP adresini ve port numarasını bilmek zorundadır.Eğer port numarası talep edilen SIP adreslerinde yoksa görev yapamayan port 5060'tır.
- SIP adresindeki talepte protokol tipi belirtilmediyse, alıcı önce UDP'ye sonra TCP'ye bağlanmak zorundadır.
- Alıcı, sunucu IP adresi için DNS' e (Domain Name Server) sorgulama yapmalıdır. Eğer kayıtlarda adres bulunamazsa alıcı sunucuyu bulamaz ve işlemler devam edemez.

4.2.5 SIP Mesajlaşması

Adresleme halledildiği zaman, alıcı bir yada birden fazla SIP talebi gönderebilmekte ve belirlenen sunucudan bir veya daha fazla cevap alabilmektedir. Basitlik ve kapsam açısından mesaj başlığı hem talep hem de cevap mesajlarında yer alır. SIP mesajlaşmaları hem UDP hem de TCP üzerinden yapılabilmektedir. TCP ile, tüm talep ve cevapları ilgili bir SIP iletimi ile aynı TCP bağlantısı üzerinden yapabiliriz. Aynı zamanda farklı SIP iletimlerini de aynı TCP bağlantısı üzerinden yapabiliriz. UDP kullanırsa cevap, talep mesajının başlığında geçen adrese yollanır. UDP protokolü mesajın iletilmesini garanti etmediği için SIP de protokol seviyesinde güvenilirlik sağlanmaktadır. Gönderilen mesajın her biri için bir onay mesajı geri yollanmaktadır. Gönderilen SIP mesajı için belli bir süre içerisinde onay mesajı gelmezse mesaj iletilmemiş sayılır ve tekrarlanır.

4.2.6 Kullanıcı Yeri

SIP de kullanıcılar birden fazla değişik uç noktadan ağa bağlanabilmektedir. Kişi, evinde veya ofisinde bir yerel ağdan bağlı olabilir ya da halka açık bir yerden internete bağlı olabilir. Bundan dolayı SIP, IP son sistemlerinin esnekliğini ve hareketliliğini hesaba katmak zorundadır. Bu son noktaların ağ üzerindeki yerleri SIP sunucusuna kayıt ettirilmelidir.

4.2.7 SIP Mesajları

SIP mesajları, alıcıdan gelen talep ve sunucudan dönen cevap mesajları olarak ikiye ayrılır. Her mesaj iletişimin detaylarını içeren bir başlık içerir. SIP metin bazlı bir protokol olarak, mesaj yazımı ve başlık alanı HTTP (Hypertext Transfer Protocol) ile hemen hemen aynıdır. SIP mesajları TCP ya da UDP üzerinden yollanabilmektedir. SIP mesajlarını iki grup altında incelenebilir. Birinci grup istek mesajlarıdır:

- REGISTER: Kullanıcıların ağ adreslerini belli aralıklarla uygulama sunucusunda güncellemeleri gerekmektedir. REGISTER mesajı bu amaçla kullanılmaktadır

- INVITE: Bir arma başlatılmak istenildiğinde kullanılan mesajdır.
- BYE: Bir arama sonlandırılmak istendiğinde kullanılan mesajdır.
- CANCEL: Bir arama başlatma isteği aram gerçekleşmeden sonlandırılmak istendiğinde kullanılan mesajdır.
- OPTIONS: Uygulama ile ilgili seçeneklerin sunulduğu mesajdır.
- PRACK(RFC3262): "required:100rel" başlığını içeren mesajların onaylanmasında kullanılan onaylama mesajıdır.
- UPDATE(RFC3311): Kullanıcının ağ adresini güncellemek istediğinde kullandığı mesajdır.
- SUBSCRIBE(RFC3265): Kullanıcının kendi durumunu arkadaş listesindeki diğer kullanıcılara bildirmek istediğinde kullanılan mesajdır.
- NOTIFY(RFC3265): arama sırasında bir durum değişikliğinin iletilmesinde kullanılabilen bir mesajdır. Arama sırasında kodlayıcın değişimi buna örmek gösterilebilir.
- INFO(RFC2976): DTMF tonlarının SIP mesajları ile iletilmesi gibi uygulamalarda kullanılır.
- REFER

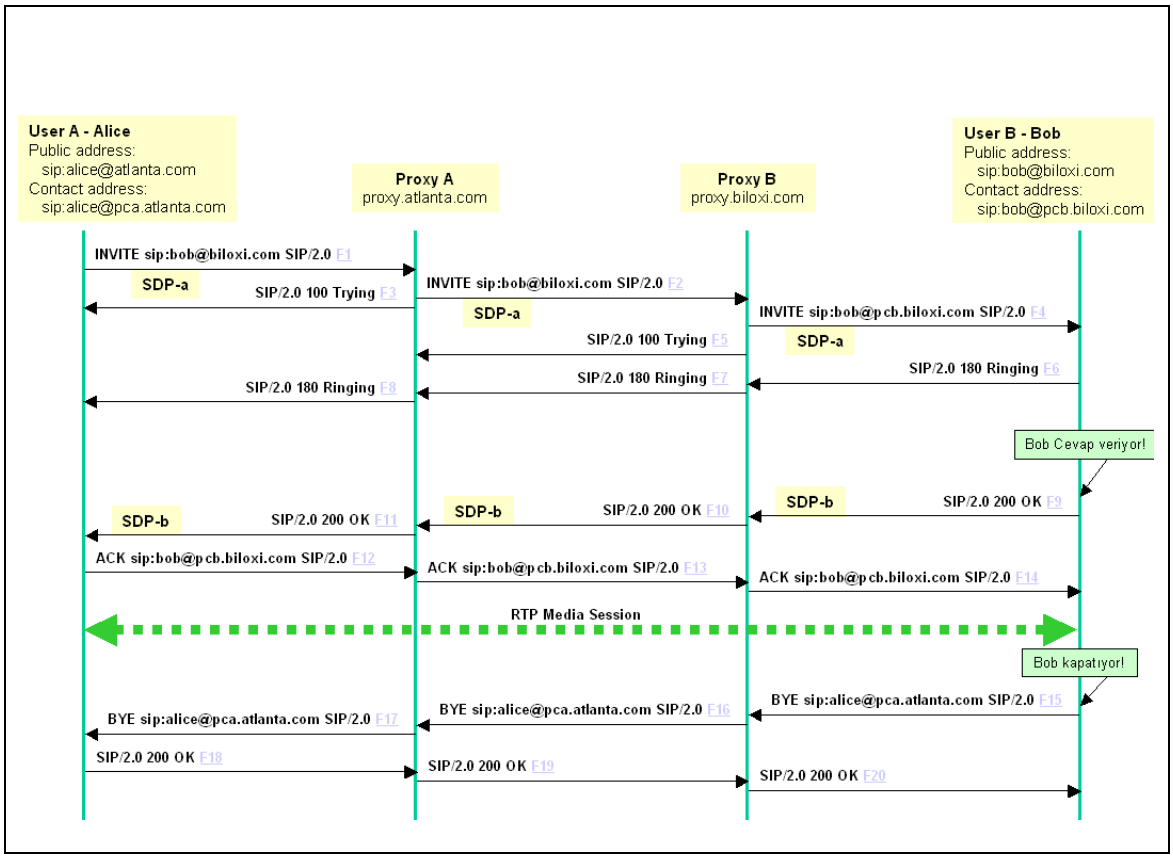
Aşağıdaki mesajlar ise bu istek mesajlarına dönülebilecek cevap mesajlarını içermektedir.

- 1XX: Bu mesajlar işlem durum hakında bilgi vermektedir:
  - 100TRYING bir isteğin alındığını yerine gerine getirilmek üzere çalışıldığını ifade etmektedir.
  - 180RINGING aranan kişinin cihazının çalma durumunda olduğunu ifaden eden işarettir. Bu masajı alan bir uç nokta yerel olarak "ring back tone" üretir.
  - 181CALL FORWARDED aranan kişinin bir yönlendirme yaptığını ifade eder.
  - 183RINGING bu mesaj arayan kullanıcıya bir anons yapılırken kullanılmaktadır.
- 2XX: 200 ailesi mesajlar bir isteğin başarı ile sonlandığını ifade etmektedir.
- 3XX türü mesajlar bir yönlendirmenin yapılmakta olduğunu ifade etmektedir.
  - 300 MULTIPLE CHOISES birden fazla yönlendirme seçeneği olduğunu ifade eder.
  - 301 MOVED PERMANATLY kullanıcıya başka bir uygulama sunucusu tarafından hizmet verileceği zaman kullanıcıyı hizmet verecek olan uygulama sunucusu ile irtibata geçirmek için bilgilendirmektedir kullanılmaktadır.
  - 302 MOVED TEMPORARLY kullanıcıya geçici bir süre başka bir uygulama sunucusu tarafından hizmet verileceği zaman kullanıcıyı hizmet verecek olan uygulama sunucusu ile irtibata geçirmek için bilgilendirmektedir kullanılmaktadır.
- 4XX türü mesajları kullanıcı ucu hata mesajlarıdır.
  - 400 BAD REQUEST gelen isteğin doğru olmadığını yada SIP mesajının bozulduğunu belirten hata mesajıdır
  - 401 NOTAUTHORIZED kullanıcının kullanıcı adı ve şifresini kullanması gerekirken bunları kullanmadan kendini kayıt ettirmeye çalıştığını ifade eden hata mesajıdır.
  - 403 FORBIDDEDN kullanıcının yanlış kullanıcı adı şifre kullanarak kendini sisteme kayıt ettirmeye çalıştığını ifade etmektedir.
  - 404 NOT FOUND Aranmak istenen kullanıcının, sistemin bildiği bir bölgede olmadığını ifade eden hata mesajıdır.
  - 486 BUSY HERE aranmak istenilen kullanıcının meşgul olduğunu bildiren hata mesajıdır.
- 5XX türü mesajlar sunucu tarafı hata mesajlarıdır.
  - 500 SERVER INTERNAL ERROR: Uygulama sunucusundan kaynaklanan bir hata olduğunu ifade eden bir hata mesajıdır.

- 503 SERVICE UNAVAILABLE:Uygulama sunucusunun veri tabanına ulaşamadığı aman döndürdüğü hata mesajıdır.
- 504 TIME OUT uygulama sunucusu üzerinde işlem yapılırken bir isteğin zaman aşımına uğraması sonucu oluşan hata mesajıdır.

- 6XX türü mesajlar global hata mesajlarıdır.
  - 600 BUSY EVERYWHERE
  - 603 DECLINE
  - 604 DOESNOT EXIST
  - 606 NOT ACCEPTABLE

Aşağıda temel en basit arama için gerçekleştirilen SIP mesaj akışı gösterilmiştir:



Şekil 4-12 SIP mesaj akış şeması (Cisco, 2003)

4.3 MGCP

CISCO ve TELCORDIA tarafından geliştirilmiştir. Çağrı kontrol elementleri ve telefon ağ geçitleri arasındaki mesajlaşmayı yöneten bir protokoldür. Tek başına uçtan uca çağrı kurulumunu gerçekleştiremez. Sadece H323 ve SIP gibi çağrı kontrol protokollerini kullanan telefon sistemlerine ağ geçitlerini daha iyi yönetme olanağı sunmaktadır.

Media Gateway Control Protocol (MGCP), IETF ve ITU-T (ITU-T Recommendation H.248) ortak iştiraki ile ortaya çıkmıştır.

Bu işi yapan bir diğer protokol ise MEGACO dur, IETF (RFC 3525) ve ITU' (Recommendation H.248-1) beraber geliştirdiği bir protokoldür. Her iki protokol de RFC 2805 de tanımlanan API "Media Gateway Control Protocol Architecture and Requirements", ı kullanır. Dağılmış sisteme en az bir CA (Call Agent) yada MGC (Media Gateway Controller), en az bir adet paket ve devre anahtarlama arasında dönüşümü sağlayan MG (Media Gateway) ve PSTN ne bağlanırken de en az bir adet SG (Singnalling Gateway) gerekmektedir.

CA, MG 'ye MGCP yi şu bilgileri iletmek için kullanır:

- CA' ya hangi olayların bildirileceği
- Uç noktaların birbirine nasıl bağlanması gerektiği
- Uç noktalarda hangi sinyallerin çalınması gerektiği

MGCP CA'nın bir MG üzerinde uç noktaların durumunun güncellenmesine rol oynar.

MG, MGCP'yi telefonun açılması veya numaraların çevrilmesi gibi durum değişikliklerini bildirmek için kullanır.

Genellikle işaretleşme Ağ geçiti(SG) ve veri Ağ geçiti(MG) ayni fiziksel birim üzerinde bulunsa da bu şekilde kullanılması için bir gereklilik yoktur. Arama kontrolcüsü (CA) , işaretleşme ağ geçidini (SG) uyarmak için MGCP kullanmaz. Bunun yerine SIGTRAN protokolü kullanılmaktadır.

MGCP de her bir komutun bir işlem numarası bulunur ve komutlar işetildiği zaman bu numarayı içeren bir cevap alınır.

MGCP paketlerinin yapısı diğer birçok protokolde kullanılan yapıdan farklıdır. Genelde UDP port 2427 kullanılarak iletilirler. MGCP de datagramlar TCP de ki gibi boşluk karakterleri içerecek şekilde düzenlenmişlerdir. MGCP paketleri ya bir komutu yada komuta dönülen bir cevabi içermektedirler.

MGCP de komutlar 4 karakterden oluşan karakter dizileri ile başlarlar. Bu komutlara gelen cevap mesajları ise üç karakterden oluşan diziler ile başlamaktadırlar. Sekiz adet komut başlığı bulunmaktadır:

- AUEP (Audit Endpoint) ve AUCX (Audit Connection) komutları CA'nın (Call Agent) MG'nin (Media Gateway) durumunu sorgularken kullandığı komutlardır.
- CRCX (Create Connection), DLCX (Delete Connection), MDCX (Modify Connection) komutları ise CA'nın (Call Agent) MG'e (Media Gateway) RTP bağlantısını yönetmek için kullanılır. MG (Media Gateway) DLCX komutunu yollayarak bağlantıları düşürebilir.
- RQNT (Request for Notification) komutu CA (Call Agent) tarafından bilgilendirme mesajlarının MG (Media Gateway) tarafından gönderilmesi isteği için kullanılır.
- NTFY (Notify) komutu MG'nin CA'nın daha önce hakkında bilgi gönderilmesini istediği bir durum ile karşılaşıldığını bildirmesi için kullanılır.
- RSIP komutu MG tarafından kullanılan bu komut CA'ya şu anda yeniden başlat prosedüründe olduğunu anlatmak için kullanılır.

4.4 MEGACO

"Media Gateway Control Protocol" yada MEGACO /H.248 bir MG (Media Gateway) ve MGC (Media Gateway Controller) arasında kullanılan bir protokoldür. PSTN-IP yada IP-IP ağlar arasında faks ve ses haberleşmesini kontrol etmeye yarayacak gerekli ekleri içermektedir.

Bu protokol IETF ve ITU'nin ortak iştiraki sonucunda geliştirilmiştir. Hem IETF'in RFC 3525 (RFC 3015 tarafından rafa kaldırılmıştır) hem de ITU-T'nin H.248-1 protokolünde tanımlanmıştır. Çalışması ek özellikleri ele almazsak MGCP ile aynıdır.

4.5 Ses Taşıma Protokolleri

Bir önceki bölümde ses iletimini kontrol eden yani durduran başlatan aranan kullanıcının yerini bulan protokolleri inceledik. Bu bölümde ise sesi kodlamaya yarayan IP paketleri ile iletilmesini sağlayan protokolleri inceleyeceğiz.

4.5.1 RTP/RTCP

Yıllar önce, uzak bir noktaya sayısal formda sinyal gönderme keşfedildi. Sinyal yollanmadan önce sayısal formata ADC (analog to digital converter – analogdan sayısal'a dönüştürücü) ile çevrilmekte ve karşı tarafa yollanmakta, karşı taraf sinyali aldığında tekrar analog formata çevirmek için DAC (Digital to analog converter – sayısaldan analoga dönüştürücü) kullanılmaktadır. VoIP'de bu şekilde çalışmaktadır, sayısal formattaki ses, veri paketleri olarak karşıya yollanmakta ve karşı tarafta tekrar sayısal ses haline dönüştürülmektedir. Sayısal format daha iyi kontrol edilebilmektedir: Sıkıştırabilmekte, yönlendirebilmekte, daha iyi bir formata çevrilebilmektedir. Bilindiği gibi sayısal sinyalin gürültü toleransı, analoga göre daha fazladır. (Örnek: GSM). TCP/IP ağlarında, IP paketleri iletişim kontrolü için başlık

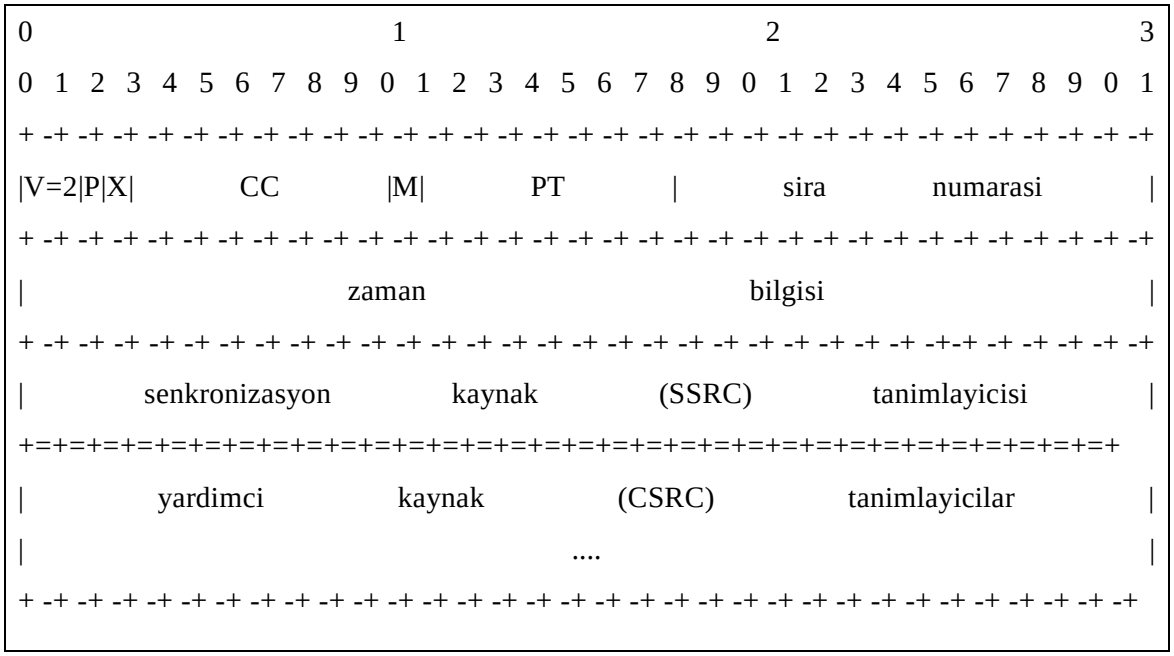
ve veri transferi için yük kısımlarını içerir. VoIP bunları ağda ilerletebilmek için ve hedefe ulaşmak için kullanılmaktadır.

4.5.1.1 RTP'nin Yapısı

Verinin analogdan sayısala nasıl dönüştürüldüğünü ve sıkıştırma yöntemleri bölüm 3 de incelenmişti. Bu bölümde ise RTP paketinin yapısı incelenecektir.

VoIP verileri, UDP-IP paketlerinin içindeki RTP paketinde yer alır. TCP yapısal olarak paketin doğruluğuna önem verir. Eğer pakette iletim sırasında bir bozukluk oluşmuşsa paketi yeniden gönderilmesini isteyebilir. VOIP de böyle bir şeye gerek yoktur. Paket bozulmuşsa bile yeniden gönderilmesine zaman yoktur. Çünkü gecikme de bozuk bir paketin gelmesi kadar büyük bir sorundur. Bu nedenden ötürü ses iletimi için UDP protokolü tercih edilmektedir. Fakat UDP protokolü yerince iyi değildir. Bu nedenle UDP paketini yük kısmından 12 baytlık bir bölüm RTP başlığı olarak kullanılmaktadır. RTP başlığını içeren UDP paketleri bundan sonra RTP paketleri olarak adlandırılacaktır. Bu başlıkta tutulan veriler:

- RTP versiyonu: İlk bölümde RTP versiyonu bulunmaktadır. Şu anda yaygın versiyon 1 dir.
- Kodlamada kullanılan kodlayıcı türü: Takip eden alanda yük kısmındaki ses datasını sıkıştırırken kullanılan kodlayıcı türü bulunmaktadır. Örnek olarak 0x00 g711a 0x08g711m 0x80 g729 u belirtmektedir.
- Paket sırası: RTP de paket sırası önemlidir. UDP protokolünde paketleri sıralamaya yönelik bir yapı bulunmadığından RTP başlığında paket sıralamasını belirten bir alan bulunmaktadır. Paketler dinamik yönlendirme protokolleri kullanan ağlarda değişik yollardan ulaştırılabileceği için farklı sırada gelebilmektedir. Eğer bu sırlama yapılmazsa ses kalitesinde belirgin düşme gözlemlenecektir
- Tanımlar:
  V : Kullanılan RTP'nin versiyonu;P : Padding ; X : Başlık ekleri CC : CSRC tanımlayıcılarının sayısını veren alan. CSRC alanının kullanım yeri örneğin konferans konuşmalarıdır. M : İşaret bit'i PT : Yük tipi; RSVP : VoIP'de RSVP gibi diğer bir takım protokollerde kullanılır. RSVP Servis Kalitesi'nin kontrolünde kullanılır (QoS – Quality of Service)
- RSVP bir sinyalleşme protokolüdür ve paketlerin uğrayacağı her noktadaki bant genişliği ve gecikme değerlerini tespit etmeye yarar. (Schulzrinne, H.,1996)



Şekil 4-13 RTP paketini yapısı

(Schulzrinne, H., Casner, S., Frederick, R. and V. Jacobson, 1996)

5. VOİP DİNLEME ve KAYIT SİSTEMİ TASARIMI

Bu bölümde ağ dinleme yöntemlerinden kısaca bahsedildikten sonra internet protokolü üzerinden yapılan ses görüşmelerini otomatik olarak kayıt edebilme yeteneğine sahip bir programın gereksinimleri ortaya koyulacak, çalışma prensibi ve geliştirilmesinde kullanılan yöntemlerden kısaca bahsedilecektir.

5.1 Ağ Trafiği Dinleme Yöntemleri

İnternet protokolü üzenden yapılan her tür haberleşmeyi dinlemek mümkündür. Son yılarda geliştirilen ses taşıyan IP paketlerini şifrelemeye yönelik olarak yapılan çalışmalar daha yaygınlık kazanmadığı için ses paketlerinin dinlenmesi şu anki yapıda oldukça kolaydır fakat bu imkanı kısıtlayan diğer bütün ağ dinlemelerinde de karşılaşılan yapısal kısıtlamalar bulunmaktadır. Bu kısıtlamalardan en önemlisi dinleme yapacak olan sistemin dinlenecek IP paketlerinin geçtiği bir ağda bulunması gerekmektedir. Başka bir deyişle sistem sadece bulunduğu ağdan geçen paketleri yakalayabilmektedir. İkinci en büyük kısıtlama ise sistemin bağlı olduğu anahtarlayıcının bir bağlantı noktasına gelen paketleri diğer bağlantı noktalarına da yönlendirebiliyor olmasıdır. “Hub” türü şu anda uygulamalarda pek kullanılmayan eski tür anahtarlayıcılar bunu kendi kendilerine hiçbir ayarlama gerekmeden yapabilmektelerdi. Tasarım gereği bu şekilde çalışıyorlardı. Fakat bu tasarımın getirdiği yüksek işlemci gücü gereksiniminden dolayı hub’lar çok büyük ve hızlı olamıyorlardı. Bu problemi aşmak ve kötü amaçlı dinlemeleri engellemek için “Switch” türü paket anahtarlayıcıları geliştirildi. Bu tür anahtarlayıcıların çalışma prensibine göre her portuna bağlanan cihazların donanım adresleri bir tabloda tutulmakta ve sadece akalı donanım adresine gelen paketler geçirilmektedir. Böylece her bir bağlantı noktası sadece oraya bağlı cihaza ait IP paketleri gönderebilmektedir. Buna karşılık “switch” üreticileri ağ problem giderme amaçlı dinleme yapılabilmesine olanak sağlayacak bazı özellikler eklemişlerdir. Bu özellikler üreticiden üreticiye değişmekte olup genelde iki şekilde karşımıza çıkmaktadır. Bunlardan birincisi “mirror port-ayna bağlantı noktası” özelliğidir. Sadece bir port diğer portlara gelip giden paketleri de yayımlama özelliğine sahiptir. Dinleme yapmak isteyen kişi sistemini bu porta bağlamak zorundadır. Bu da sisteme fiziksel bir erişim gerektirmektedir. İstenmeyen dinlemelere , sisteme fiziksel olarak erişim kısıtlamalarıyla engel olunmaktadır. İkinci özellik ise “port mirroring-port aynalama ” olarak adlandırılmaktadır. Gelişmiş anahtarlayıcıların konfigürasyon menülerinden yararlanılarak herhangi bir port diğer portlara gelip giden paketleri yayınlayacak şekilde

ayarlanabilir. Bu yöntemde ise ayarlama menüleri kullanıcı isimleri ve şifreler ile korunmaktadır.

Yasal dinleme yapılabilmesi için ağlarda kullanılan anahtarlayıcılar bu şekilde ayarlanmalıdırlar.

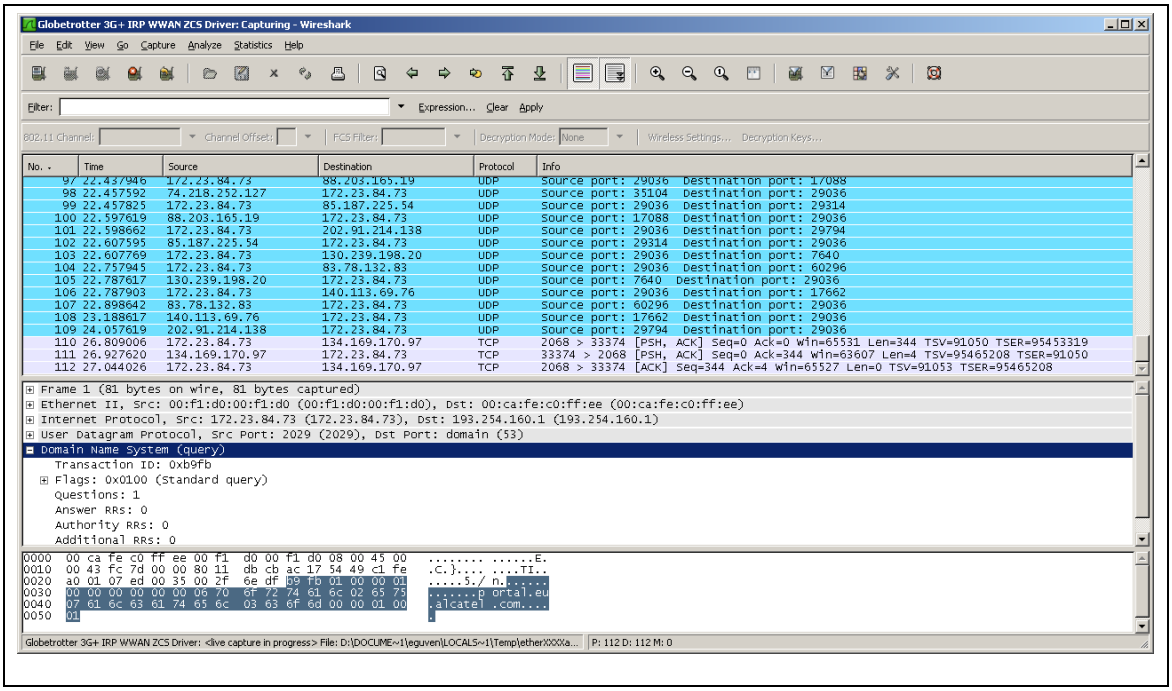
5.1.1 Yaygın Ağ Dinleme Araçları

Günümüzde yayın olarak kullanılan ağ dinleme araçları Ethereal, Tethereal, Tcpdump ve Snoop'dur. Bu programlar aslında birbirlerinden farklı yapıları olsa a , çalışma prensipleri aynıdır.

5.1.1.1 Ethereal

Ağ dinleme araçları denildiğinde ilk akla gelen ETHEREAL programıdır. Son sürümlerindeki ismi WIRESHARK olarak değiştirilmiştir. Hemen hemen bir rakibi yok gibidir. PCAP paket yakalama kütüphanesi üzerine inşa edilmiş bir özgür yazılımdır. Geliştirilmesi bir firmanın tekelinde olmayıp internet üzerinden bu programın geliştirilmesine katkı sağlamak isteyen birçok tasarımcı tarafından maddi bir çıkar güdülmeden yapılmıştır. İnternetten kolayca indirilip bir bedel ödemeden kolayca kullanılabilir. Sağladığı özellikler sayesinde ağ ve sistem problemlerini incelemek için oldukça faydalı bir araçtır.Yakaladığı ses paketlerini g711 kodlayıcı ailesi ile kodlanmışlarsa geri kodlama yapıp .au ve raw formatlarına çevirebilme yeteneğine de sahiptir.

Yakaladığı paketleri okunabilir formata dönüştürüp kullanıcının paket hakkında detaylı bilgi almasına olanak sağlar. Yakalanacak paketler arasında gelişmiş filtreleme yapma özelliklerine sahiptir.



Şekil 5-1 Ethereal programı arayüzü

5.1.1.2 Tethereal

Ethereal'ın komut satırından koşturulabilen versiyonudur. Grafik kullanıcı arayüzü kullanılmayan ara yüzlerde ve toplu işlem dosyaları içerisinde kullanılabilme özelliğine sahiptir. Bazı görsel özelliklerinde ve fonksiyonlarında kısıtlamalar bulunsa da, hemen hemen Ethereal ile aynı özelliklere sahiptir.

5.1.1.3 Tcpdump

Tcpdump aslen Linux işletim sistemlerinde kullanılmak üzere geliştirilmiş araçtır. Tethereal gibi komut satırından çalıştırılan kullanıcı arayüzü olmayan bir programdır. Ethereal gibi gelişmiş paket filtreleme, paketleri dosyaya kayıt etme ve kayıt edilmiş dosyadan açma özellikleri bulunmaktadır. Tcpdump da Ethereal gibi PCAP kütüphanesi üzerine inşa edilmiş bir araçtır. Tcpdump , Ethereal ile aynı dosya formatını kullanmaktadır. Tcpdump ile kayıt edilmiş paket dosyaları Ethereal ile açılıp görselliğe kavuşabilme özelliğine sahiptir. Tcpdump'ın Windows işletim sistemlerinde çalışabilen versiyonları da mevcuttur.

5.1.1.4 Snoop

Snoop Sun firmasını geliştirdiği SOLARIS işletim sistemlerinde kullanılabilen bir araçtır.

Snoop da Tethereal ve Tcpdump gibi komut satırından işletilen bir araçtır. Komut satırı Ethereal ve Tcpdump'a göre oldukça farklıdır. Bu da diğerleri gibi PCAP kütüphanesini kullanır.

5.2 Voip Görüşmelerinin Dinlenmesi

Voip görüşmelerinin dinlenmesi yukarıda bahsedilen araçlar voip paketlerini filtreleyecek şekilde konfigüre edildiğinde mümkündür. Voip paketleri UDP özelliği taşımaktadır. Sadece UDP paketlerinin yük kısmının ilk 12 byte'ı RTP ile ilgili olarak kullanılmaktadır. UDP paketlerini bu ilk 12 byte'ını RTP bilgisi, geri kalanını ise ses verisi olarak değerlendiren bir program ses verisini kolayca geri çözebilmektedir. Ethereal bu işlemi kolayca yapabilmektedir fakat, bazı kısıtlamalar içermektedir. G729 kod çözücüsü lisanslı bir yazılım olduğu ve telif hakları yasaları tarafından korunduğu için Ethereal'a G729 ile kodlanmış ses görüşmelerini geri kodlama özelliği kazandırılamamıştır. Bunun da ötesinde Ethereal, paket çözme işlemi içi kullanıcı ara yüzünden birtakım ayarlamalar yapılmasına ihtiyaç duymaktadır. RTP paketlerini yakaladığında bunları öncelikle UDP paketleri olarak değerlendirmektedir. Kullanıcının bu paketlerin RTP olduğunu programa anlatması gerekmektedir. Görüldüğü gibi telefon görüşmelerini otomatik olarak yakalayan görüşme sonlandığında kayıt işlemini durduran kaynaklarını bir sonraki görüşme için harcayabilen bir yapıya sahip değildir.

Paket yakalama programlarının telefon görüşmelerini kaydetmek için otomatik bir yapıya sahip olmamasından dolayı, bu işlemi yapabilen akıllı programlar ihtiyaç duyulmaktadır. Sonraki kısımlarda bu ihtiyaçlara karşılık verebilecek otomatik arama yakalama, otomatik kod çözme arşivleme özelliklerine sahip bir ses kayıt programının geliştirilmesinden bahsedilecektir.

5.3 Ağ Üzerinden Ses Kayıt Sisteminin Çalışma Prensibi

Ağ üzerinden paket dinleme yapılabilmesi için kısıtlamaları ve gereklilikleri bir önceki kısımda ele aldık. Bu kısımda ağ dinleme yapılabilmesi için gerekliliklerin sağlandığını kabul ederek sistemin çalışma prensibi incelenecektir. Ağ gerekli şekilde konfigüre edildiğinde ağda bulunan bütün paketler sistemimize ulaşmaktadır. Normal çalışma modunda çalışan bir ağ bağdaştırıcısı kendisine ulaşan ama kendisi ile alakalı olmayan IP paketlerini reddedecektir. Dinleme yapabilmek için ağ bağdaştırıcının kendisi ile ilgili olmayan paketleri de alacak şekilde konfigüre edilmesi gerekmektedir. Dinleme yazılımı bunu otomatik olarak yapacak

şekilde tasarlanmaktadır.

Sistemimiz daha sonra kendisi ile alakalı olmayan bu paketleri bir ses görüşmesine ait olup olmadığına karar vermeli, eğer ses taşıyan bir paket ise ses kanalını belirlemeli ve her bir paketi ilgili ses kanalına ait dosyalara işleyerek kayıt etmelidir.

Ses paketlerini işlemek ise şu adımları içermektedir.

- Ağ bağdaştırıcısını dinleme konumunda çalışmak için ayarlamak
- Paketleri kendi içlerinde sıralamak,
- Sesi kodlamak için kullanılan yöntemi belirlemek
- Sesi paketten geri kodlamak
- Geri kodlanmış ses bilgisini bir dosyaya kayıt etmek
- Uplink ve downlink ses dosyalarını birleştirmek ve dinlenebilir saklanabilir bir dosya formatına çevirmek.

5.4 Voip Görüşmelerini Dinleyen Programın Mimarisi

Bu çalışmanın uygulama kısmını oluşturan internet protokolü üzerinden ses görüşmelerini kayıt edebilme yeteneğine sahip Voicerec programının yapısı ve çalışma prensibi anlatılacaktır.

Voicerec de diğer paket yakalama programları gibi PCAP paket yakalama kütüphanesi üzerine inşa edilmiş bir yazılımdır. PCAP kütüphanesi , paket yakalamak için gerekli ayarlamaları yapmaya yarayan birtakım fonksiyonları içermektedir. Bu kütüphane programa ekledikten sonra paket yakalama özelliklerini kullanabilir hale gelmektedir. Voicerec ses kayıt ve arşivleme programı iki ana kısımdan oluşmaktadır, Bunlardan birincisi paket yakalama API'lerini sağlayan VoicerecDLL , ikincisi ise kullanıcı arayüzü ve giriş çıkış birimi olan VoicereAPP dir.

5.4.1 VoicerecDLL

VoicerecDLL VoicereAPP uygulama programının kullanacağı paket yakalama alt programlarını içeren bir dinamik bağlantı kütüphanesidir. Bu kütüphane ileride geliştirilebilecek daha gelişmiş ses kayıt sistemlerinin tarafından program geliştirme sırasında eklenip kolayca kullanılabilecek bir yapıya sahiptir. VoicerecDLL in sunduğu fonksiyonlar:

5.4.1.1 Opencapdev

kullanımı ; int opencapdev (char *dev ,char *filter_exp);

Bu alt rutin dinleme yapılacak ağ ara yüzünü dinleme moduna sokma ve dinleme yi başlatmak için kullanılmaktadır. Girdi olarak iki adet parametresi bulunmaktadır. Bu iki parametre dll i kullanan uygulama programı tarafından bildirilmek zorundadır Birinci parametre "*dev" , dinleme yapılacak ağ ara yüzünün hangisi olduğunu tutan karakter türünde bir yer tutucudur (pointer). İkinci parametre de birinci parametre gibi karakter türünde bir yer tutucu olup, dinleme yapılacak ağ ara yüzünde uygulanacak filtreyi barındırmaktadır. Bu filtre sözcük dizisinin yapısı libpcap paket yakalama kütüphanesi tarafından belirtilen formatta olmalıdır;

Filtre formatlarına birkaç örnek;

host 192.168.100.1 ;

sadece 192.168.100.1 ip adresine gelen giden trafiğe izin verir

host 192.168.100.1 and port 32450 ;

sadece 192.168.100.1 adresi port 32450 ye gelen giden paketleri yakalar.

host 192.168.100.1 and src port 32450 ;

sadece 192.168.100.1 adresin ve port 32450 den gelen paketleri yakalar

host 192.168.100.1 and dst port 32450 ;

sadece 192.168.100.1 adresine ve port 32450 ye giden paketleri yakalar.

Host 192.168.100.1 and dst port 32450 proto UDP;

Sadece 192.168.100.1 adresine ve port 32450 ye giden UDP paketlerine izin verir.

Detaylı bilgi için libpcap yasal sitesini inceleyebilirsiniz. http://www.tcpdump.org/

Opencapdev alt rutini yakalama aygıtı ve filtre sözcüğünü aldıktan sonra filtreyi ara yüze uygular ve paket yakalama işlemini başlatır. Yakaladığı her bir paket için got_packet alt rutinini çağırır.

5.4.1.2 Got_packet

Kullanımı; got_packet(u_char *args, const struct pcap_pkthdr *header, const u_char *packet)

Libpcap kütüphanesi pcap_loop fonksiyonu tarafından opencapdev alt rutini içerisinde çağrılan bu fonksiyonun görevi yakalanan paketi işlemektir. Pcap_loop fonksiyonu her seferinde *header ve *packet yer göstericileri ile yakalanan paketin hafızadaki yerini got_packet alt programına bildirir. Anlaşılacağı gibi paket hafızada başlık kısmı ve beden kısmı olarak iki farklı konuma yerleştirilmiştir. Got_packet ilk olarak paketin başlık kısmını değerlendirir. Paketin nereden gelip nereye gittiğini hangi portları kullandığına bakar. Paketin bir RTP paketi olup olmadığını değerlendirir ve kullanılan kodlayıcı bilgisini elde eder. Got_channel_num alt programını çağırarak başlık bilgisinden daha önce buna benzer bir paket gelmişse hangi kanalda olduğunu, eğer gelmemişse boş bir kanal numarasını söylemesini ister. Sistem on altı adet kanalı desteklemektedir. Bu da on altı adet konuşmayı aynı anda kayıt etme özelliğine sahip olduğu anlamına gelmektedir. Got_packet kanal numarasını aldıktan sonra paketin ses bilgisini içeren kısmını ayıklayarak write2channel fonksiyonu çağırırı ve bilginin ilgili kanal tampon belleğine yazılmasını sağlar.

5.4.1.3 Got_channel_num

Kullanımı; got_channel_num(char * addr_src, char * addr_dst, unsigned short port_src, unsigned short port_dst,const u_char *ch)

Bu alt rutin got packet tarafından her bir paket yakalandığında çağırılır. Temel görevi paketleri kanallara göre sınıflandırmak ve gelen paketin hangi kanala yazılacağını belirlemektir. Eğer daha önce bir kanala atanmamış bir paket türü ile karşılaşırsa boş kanallardan birini bu paket türüne atar. Eğer boş kanal yoksa bu paket kayıt edilemeyecektir. Got_channel_num fonksiyonu çağıran got_packet fonksiyonu got_channel_num fonksiyonuna paketle ilgili bilgiler vermektedir. Karakter yer tutucusu addr_src kaynak IP adresi bilgisini addr_dst hedef IP adres bilgisini işaretsiz kısa türünde olan port_src değişkeni kaynak port bilgisini port_dst ise hedef port bilgisini içerir. Sabit işaretsiz karakter türündeki *ch yer tutucusu ise kodlayıcı türünün bilgisini içerir. Bu bilgiler channel_info tampon belleğinde tutulur. Bu özelliklere ait daha sonra başka bir paket geldiğinde tampon bellekten kanal numarasını okuyarak write2channel alt fonksiyonuna bildirilir.

5.4.1.4 Write2channel

Kullanımı; write2channel(got_channel_num(inet_ntoa(ip->ip_src),inet_ntoa(ip->ip_dst), ntohs(tcp->th_sport), ntohs(tcp->th_dport), ch), payload,size_payload)

Yukarıdaki kullanımda got_channel_num ve write2 channel fonksiyonlarını birlikte nasıl kullanıldığı görülmektedir. Write2channel aslında üç parametre almaktadır. Bunardan birincisi got_channel_num tarafından döndürülen sayı türündeki kanal numarasıdır. İkincisi ise kanala yazılacak ses verisinin hafızadaki başlangıç yeridir. Üçüncüsü ise bu başlangıç yerinden itibaren ne kadar uzunlukta bir bilginin yazılması gerektiğini ifade eder.

5.4.1.5 Listdevs

Kullanımı listdevs(void);

Amacı programın çalıştığı bilgisayar sistemini ağ ara yüzlerinin bir listesi çıkartarak kullanıcı arabirimine yansıtmaktır. Bu listeden seçilen ağ ara yüzü daha sonra paket yakalama işlemi için kullanılacaktır

5.4.1.6 Monitor_channles

Kullanımı ; hThread[0] = CreateThread(NULL, 0,(LPTHREAD_START_ROUTINE) monitor_channels ,NULL,0,&dwID[0])

Görüldüğü üzere monitor_channels alt rutini, bir thread yapısı ile beraber kullanılmaktadır. Therad'ler programın paralel işlem yapmasına olanak sağlayan yapılardır. Aslında tam anlamıyla paralel bir işlem yapılmamaktadır fakat işlemci programı işletirken ana programa bir süreliğine ara verip thread fonksiyonlarını işletir. Daha sonra programı işletmeye kaldığı yerden devam eder. Bu şekilde alt programlar paralel çalışıyormuş gibi algılanır.

Bu alt rutinin görevi kanal durumunu her iki saniyede bir raporlamaktır ve kullanılmayan kanalları kullanıma hazırlamaktır. Bunu VoicerecDLL içerisinde got_channell_num fonksiyonunun kullandığı channel_info tampon belleğindeki paket sayısı ve kanal durumu bölgelerini takip ederek yapar. Eğer kanal durumu aktif olup da , paket sayısı iki saniye boyunca artmamış bir kanal varsa artık bu kanaldaki konuşmanın sona erdiğine karar verir ve kanal durum alanındaki değeri "0"yapar. Böylelikle got_channel_num yeni kanal ihtiyacı hissettiğinde bu bölgesi "0" olan kanallardan en küçük numaralı olanı seçebilecektir.

5.4.2 VoicerecAPP

VoicerecAPP sistemin kullanıcı arayüzü ve girdi çıktı arabirimidir. Amacı kullanıcının istekleri doğrultusunda paket yakalama yapılacak ağ ara yüzünü seçmek, isteğe göre filtre tanımlamalarını almak , kanal durumunu takip ederek kullanılmayan kanalları tekrar kullanıma hazırlamak, VoicerecDLL tarafından kanal tampon belleklerine yazılan bilgileri kodlayıcı türüne göre geri kodlayıp dosyalara yazmaktır. Bunların yanı sıra konuşma zamanını konuşmanın yapıldığı IP adres çiftini ve ilgili konuşmanın kayıt edildiği dosyayı arşivlemektir. VoicerecAPP bu işlemleri aşağıdaki program parçalarını çalıştırarak başarmaktadır.

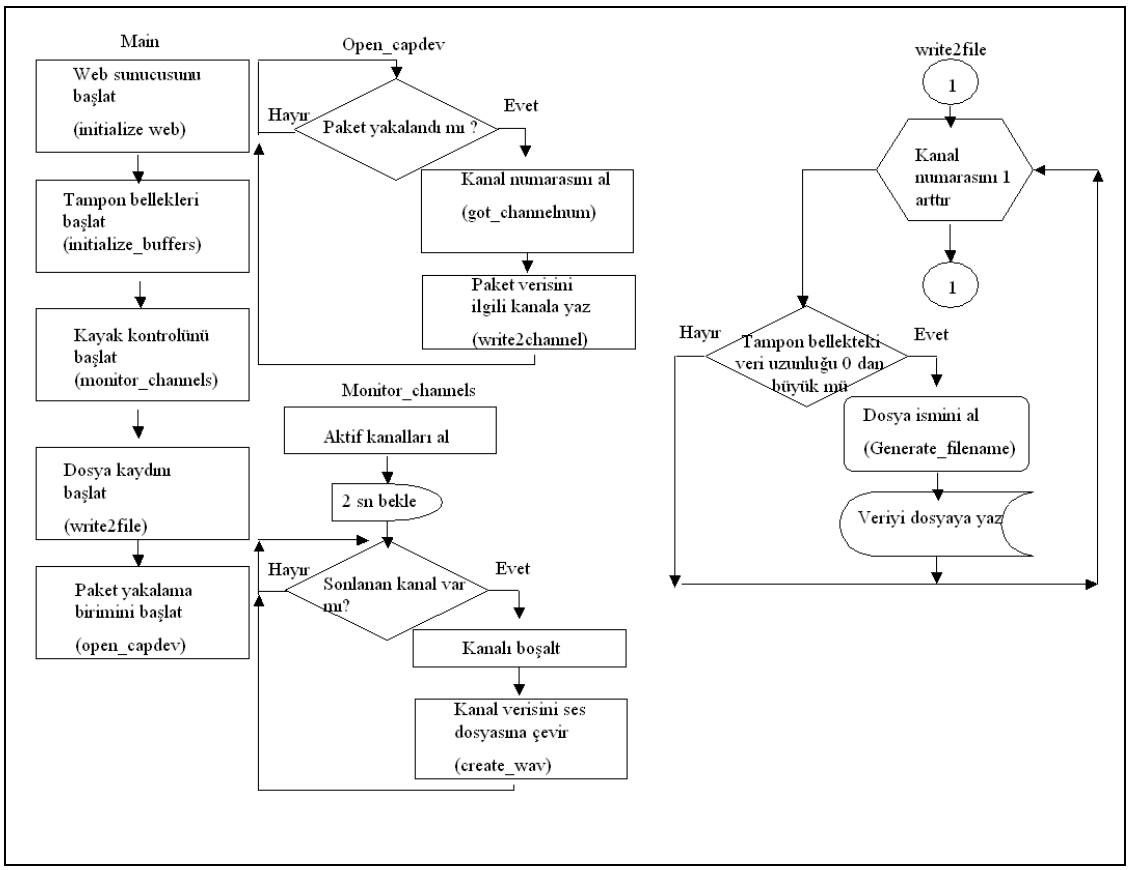
5.4.2.1 Write2file

int write2file(void);

Bu alt program programın çıkış arabirimini oluşturmaktadır. Aktif olan kanaları takip ederek bu kanallara ait halkasal tampon bellekleri boşaltmakla görevlidir. Programın en hassas kısmını oluşturmaktadır. Bu fonksiyondaki bir gecikme kanal tampon belleklerinde taşmaya neden olacak ve veri kaybı kaçınılmaz olacaktır. Temel görevi kanal tampon belleklerinin taşmasına izin vermeden belleklerdeki verileri okuyarak kod çözme işlemine tabi tutuktan sonra ilgi dosyaya kayıt etmektir. Dosya kaydı bittikten sonra HTML formatındaki arşiv soyasına bu kayıtla ilgili bilgileri girmek ve ilgili dosyaya bir bağlantı kurmaktır.

6. UYGULAMA ve SONUÇLAR

Geliştirilen uygulama programı Şekil 6-1 Voicerec uygulamasının blok diyagramından da anlaşılacağı gibi uygulama çoklu thread yapısına sahiptir. Treadler birbirinden bağımsız çalışan ama birbirleri ile veri alışverişinde bulunan alt programlar olarak düşünülebilir. Programın ana döngüsü treadleri başlatmak ile yükümlüdür.



Şekil 6-1 Voicerec uygulamasının blok diyagramı

6.1 Program Altyapısı

Web uygulamasını başlatıldıktan sonra diğer threadlerin ortak kullandıkları tampon bellekler başlatılmaktadır. Tampon bellekler başarılı bir şekilde oluşturulduktan sonra ise kanalları takip eden, boş kanalları yakalayıp o kanalları boş olarak işaretleyen monitor_channles threadi başlatılır. Bu aşamadan sonra kanal tampon belleklerini takip eden ve dosyalar yazan write2file threadi başlatılmaktadır. Son olarak da dinleme işlemini başlatan ve kendi içinde bir sonsuz döngü yapısı olan open_capdev altprogramcığı başlatılmaktadır. Open_capdev, her

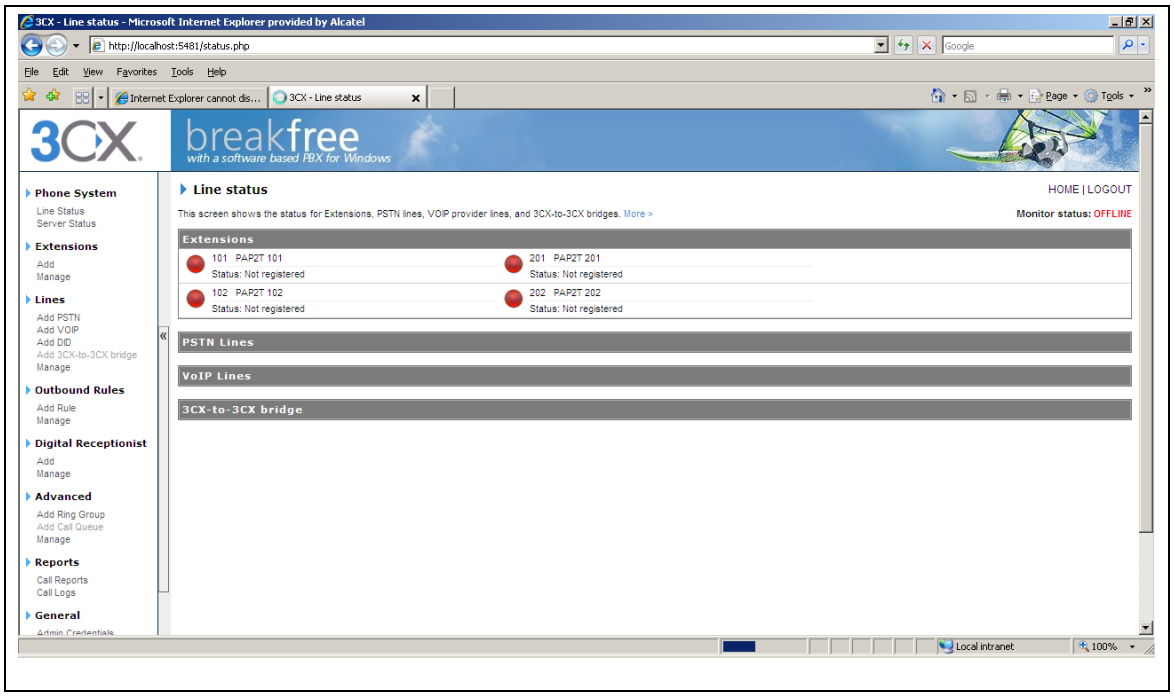
yakaladığı paket için paket işleme alt programı olan got_packet'i çağırmaktadır. Got_packet içinde çağırılan got_channelnum alt programı ile gelen pakete benzer paketlerin kayıt edildiği kanal numarası alınarak write2channel rutini ile paket kanala yazılmaktadır.

6.2 Uygulama Düzeneği

Uygulama düzeneği Şekil 6-2 Test düzeneğinde görüldüğü üzere iki adet analog telefon adaptörü bir adet hub türü anahtarlayıcı, ve uygulamanın çalıştığı bir adet bilgisayar ile basitçe gerçekleştirilebilmektedir. Kullanılan analog telefon adaptörleri Linksys firması tarafından üretilmekte olup birçok VoIP uygulamasında yaygın olarak kullanılmaktadır. Aynı anda iki kanaldan VoIP görüşesi yapabilme yeteneğine sahip bu cihazların bir çifti ile iki adet arama aynı anda gerçekleştirilebilmektedir. G711, G729, G723 ve GSM kodlayıcılarını destekleyen bu cihaz yardımı ile çeşitli türlerdeki RTP akışı gerçekleştirilebilmektedir. Bu cihazların çalışabilmesi için bir adet VoIP PBX uygulamasına gerek duyulmaktadır. Test ortamında 3CX VoIP yazılımının ücretsiz versiyonu kullanılmaktadır. Söz konusu uygulama

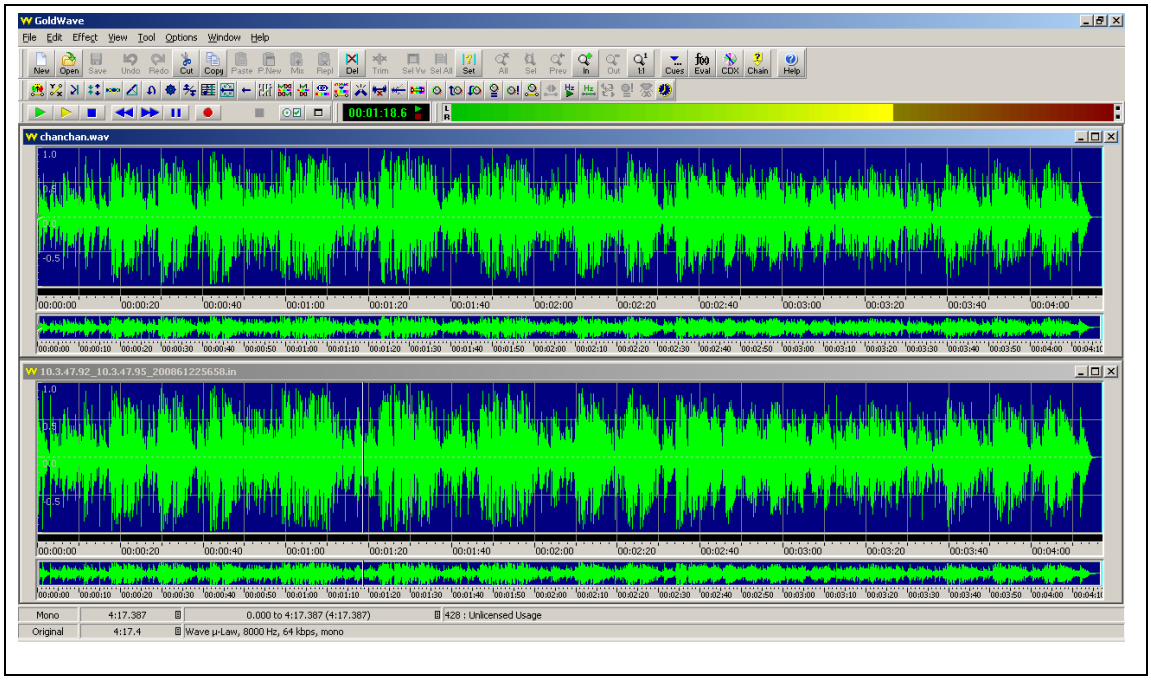
Şekil 6-2 Test düzeneği

Düzenekte görülen bilgisayar üzerinde çalışmaktadır. Şekil 6-3 3CX VoIP PBX uygulamasının ara yüzünde sisteme kayıt edilmiş kullanıcıların durumu gözlemlenmektedir.



Şekil 6-3 3CX VoIP PBX uygulamasının ara yüzü

Şekil 6-4 Gerçek ve kayıt edilen dosyaların karşılaştırılmasında gerçek ses doyası ile bu ses dosyasını kullanılarak yaratılan bir RTP akımının Voicerec uygulaması tarafından yakalanıp kayıt edilmiş halinin Golwave ses işleme programı ile açılarak karşılaştırılması görülmektedir. Ses kalitesinde hissedilir bir değişme olmamakla beraber modülasyon kayıplarından doğan küçük farklılıklar gözlemlenmektedir.



Şekil 6-4 Gerçek ve kayıt edilen dosyaların karşılaştırılması

6.3 Donanım Gereksinimleri

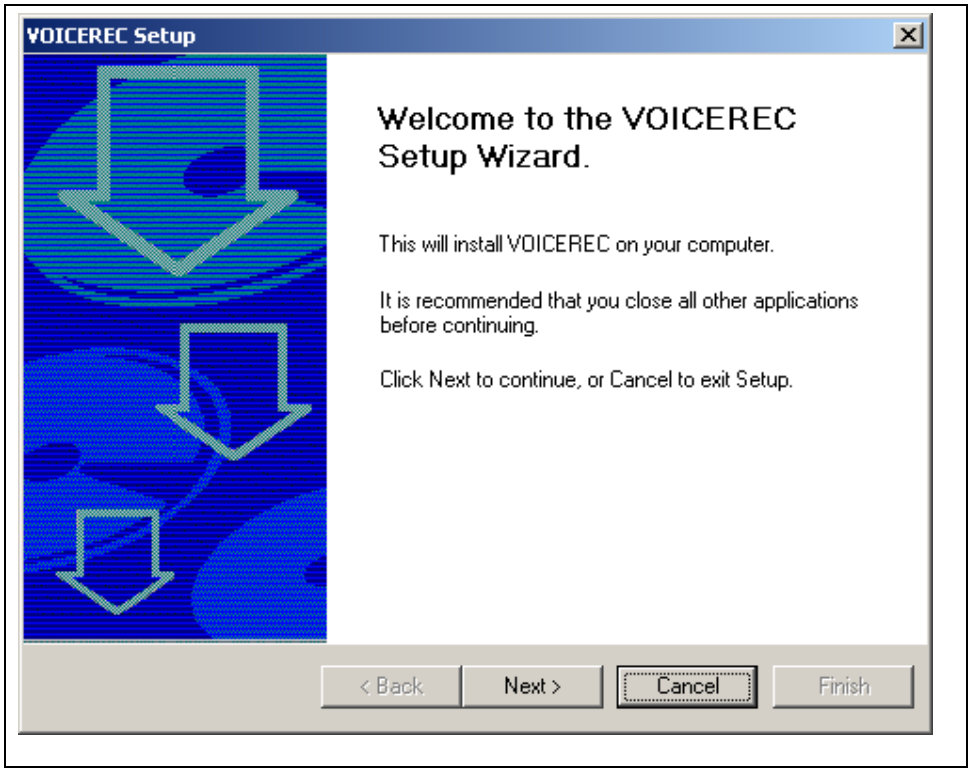
Voicerec uygulaması aynı anda 16 kanal kaydını yapabilmesi için Windows işletim sitemi tabanlı Pentium 4 işlemci ailesinden işlemciye sahip bir donanım yeterli olmaktadır. Donanımda "gigabit" veri iletim hızlarını destekleyen bir ağ ara yüzüne sahip olması performansı arttıracaktır.

6.4 Yazılım fonksiyonları ve uygulama

Voicerec uygulaması g711 g729 kodlayıcıları ile kodlanmış ses akışını kayıt edip .wav dosya formatında saklama yetisine ip bir programdır. Aynı anda on altı adet konuşmayı kayıt edebilmektedir. Kayıt edilen konuşmaların kayıt tarihi ve hangi ağ adresleri arasında yapıldığı saklanabilmektedir. Görüşmelerin kayıt edildiği .wav dosyaları iki kanallı (stereo) olup ses kalitesi oldukça yüksektir. Kayıt sırasında filtre kriteri uygulama durdurulmadan değiştirilebilmekte, yeni kritere uyan süregelen kayıtlar devam etmektedir. Uygulama şifre korumalı bir web ara yüzü ile yönetilmekte ve gözlemlenebilmektedir. Bir konfigürasyon dosyası ile son konfigürasyonunu tutmakta, yeniden başlatıldığında son konfigürasyonunu hatırlamaktadır.

6.4.1 Uygulamanın Kurulumu

Uygulama bir "setup.exe" adındaki bir kurulum dosyası yardımı ile kolayca kurulmakta , bilgisayar başlatıldığında otomatik başlamak üzere konfigüre edilebilmekte ve uygulamaya kısa yollar oluşturulabilmektedir.



Şekil 6-5 Voicerec kurulum ara yüzü

Şekil 6-5 Voicerec kurulum ara yüzünde "Next" tuşuna basıldıktan sonra başlangıç seçenekleri seçilerek uygulama kolayca kurulmaktadır. Uygulamayı başlatmak için oluşturulan kısa yol kullanılabilir.

6.4.2 Uygulamaya Bağlanma

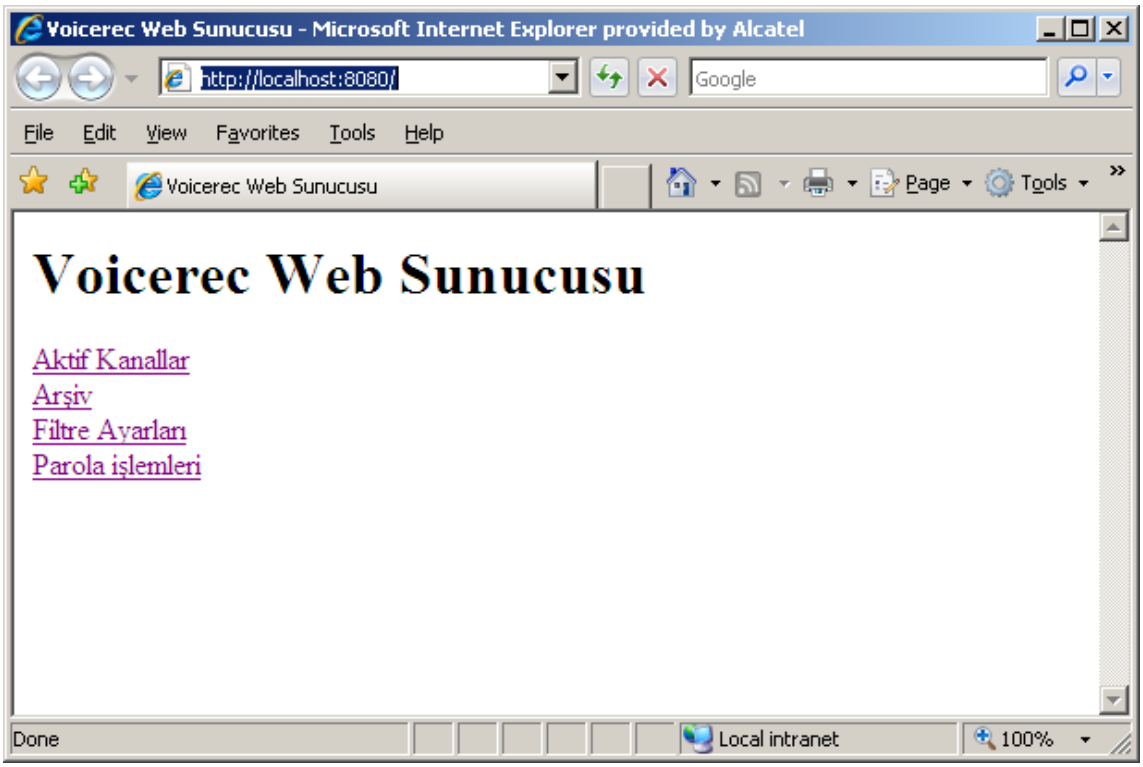
Voicerec uygulaması bir web sunucuya sahiptir. Uygulama ara yüzüne, uygulamanın bulunduğu bilgisayarın ağ adresi ve herhangi bir internet tarayıcısı arayıcılığıyla "8080" numaralı port kullanılarak ulaşılabilir. Kullanılacak port kurulumla gelen konfigürasyon dosyası yeniden düzenlenilerek değiştirilebilir.

Uygulamaya başarılı bir şekilde bağlanıldığında kullanıcı adı parola ara yüzü ekranda belirecektir. İlk kullanımda bu ara yüz henüz bir kullanıcı adı ve parola belirlenmediği için

"ok" tuşuna basılarak geçilmelidir.

6.4.3 Uygulama Ana Menüsü ve Fonksiyonları

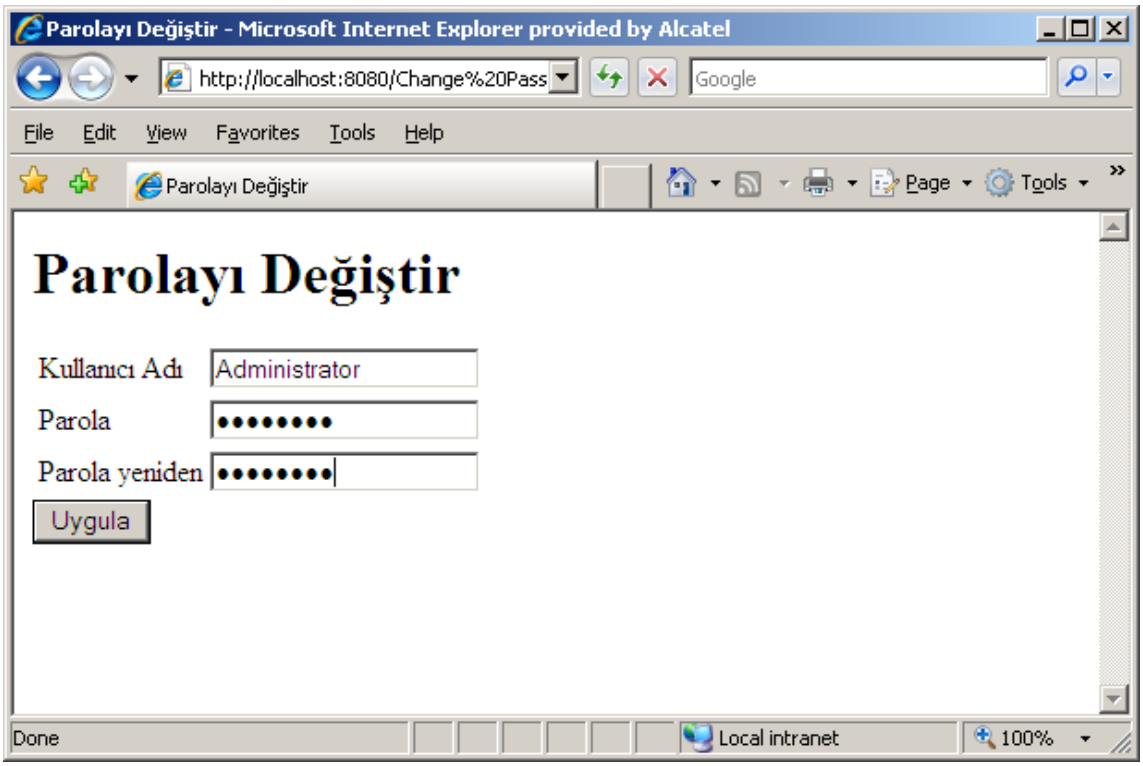
Kullanıcı adı parola adımı başarılı bir şekilde aşıldığında Şekil 6-6 Voicerec yazılımı ana menü ara yüzü karşımıza gelecektir. Uygulamaya ilk bağlanıldığında kullanıcı adı ve parola oluşturulmalıdır.



Şekil 6-6 Voicerec yazılımı ana menü

6.4.3.1 Kullanıcı Adı ve Parola Girişi

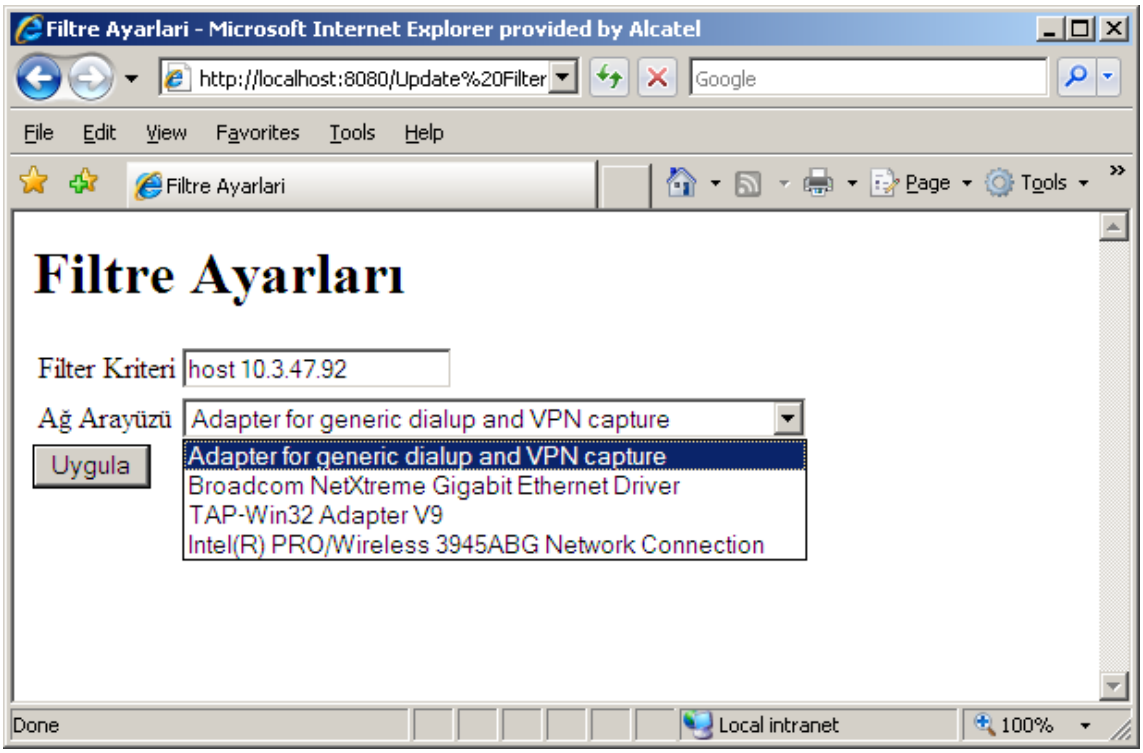
Uygulamanın kullanıcı adı ve parolası sistem üzerindeki "conf.xml" Dosyasında tutulmaktadır. Kullanıcı; kullanıcı adını ve parolasını "Parola işlemleri" Şekil 6-7 Parola değiştirme ara yüzünden değiştirebilmektedir:



Şekil 6-7 Parola değiştirme ara yüzü

6.4.3.2 Filtre Kriteri ve Ağ Ara Yüzü Ayarı

Programın kullanacağı ağ arayüzü ve kayıt edilecek ağ adreslerini tanımlayan filtre kriteri ana menüden ulaşılan "Filtre Ayarları" menüsünden gerçekleştirilebilmektedir. Şekil 6-8 Filtre ve Ağ ara yüzü değişimi menüsü bir önceki konfigürasyonu ekrana getirebilme yeteneğine sahiptir. Menünün birinci kısmında filtre kriteri yazı olarak girilmelidir. Filtre söz dizimi bir önceki bölümde örnekler verilerek açıklanan PCAP filtre formatında olmalıdır. Kullanılacak ağ ara yüzünü seçmeye yarayan çok seçenekli menüdeki değerler yazılım tarafından sistem taranarak oluşturulmaktadır. Eğer konfigürasyon dosyasında bu değerlerden biri mevcutsa bu değer en varsayılan değer olarak görünmektedir:

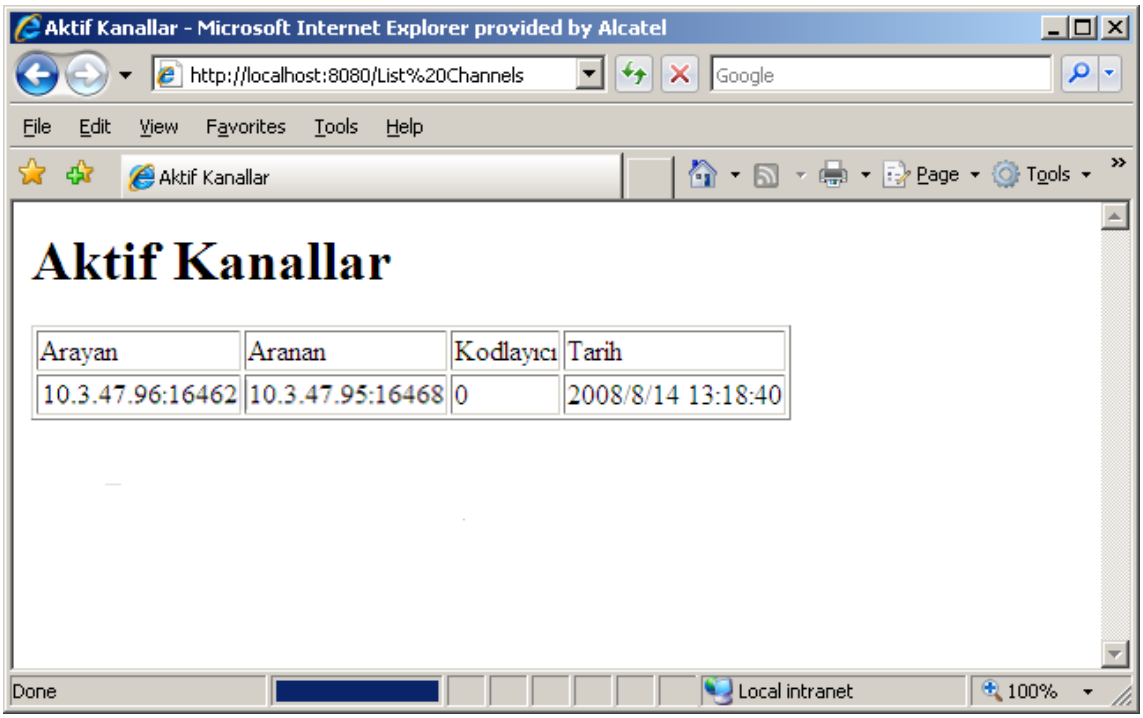


Şekil 6-8 Filtre ve Ağ ara yüzü değişimi

Filtre kriteri değiştirildikten sonra süre gelen ve yeni filtre tarafında engellenemeyen kayıtlar devam edecektir. Filtrenin değiştirilmesi sırasında anlık olarak kayıt işlemi durmakta fakat , ses kalitesi üzerinde hissedilebilir bir değişiklik görülmemektedir.

6.4.3.3 Aktif Kayıtları Görüntüleme

Ana menüdeki "Aktif Kanallar" alt menüsü Şekil 6.9 da gösterilmiştir.Bu menü kullanılarak aktif kayıtlar görüntülenebilmektedir. Bu alt menü kendi kendini her iki saniyede bir tazeleme yeteneğine sahip olup , kanallardaki değişimlerin anlık olarak görüntülenmesine olanak sağlamaktadır. Sistem aynı anda 16 kayıt yapabilme yeteneğine sahip olduğu için bu ekranda en fazla on altı adet satır gözlemlenebilecektir. Her bir satırda o kanalda konuşan kullanıcıların ağ adresleri, portları, konuşmaya başlama zamanları ve kullandıkları kodlayıcı türü görüntülenmektedir.

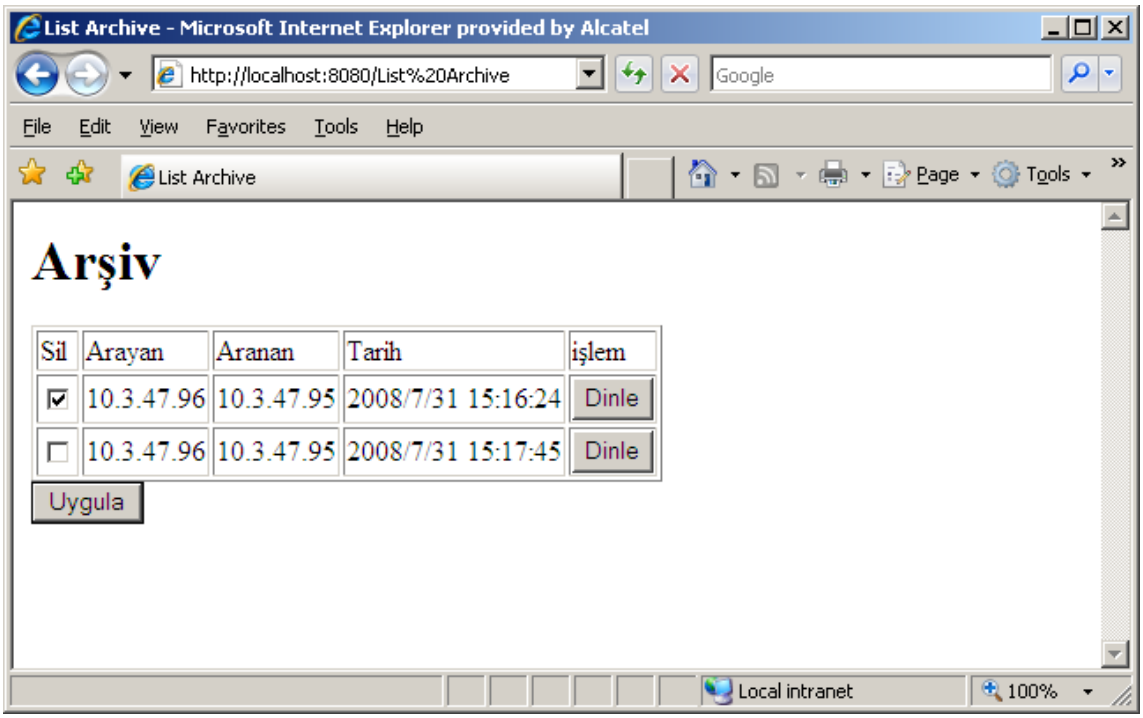


Şekil 6-9 Aktif Kayıtları Görüntüleme Ara Yüzü

Arama sonladığında "temp" klasörüne kayıt edilen aramanın iki yönün oluşturan geçici dosyalar birleştirilerek "archive" klasörü altında .wav dosyası olarak saklanmaktadır. Birleşme tamamlandığında geçici dosyalar silinmektedir. Dosya isimleri kimin kimle ne zaman konuştuğu bilgisini içermektedir.

6.4.3.4 Arşiv Görüntüleme ve Düzenleme

Kayıt edilen ve dinlenebilir formata çevrilen dosyalara, şekil 6-10 da gösterilen "Arşiv" alt menüsünden ulaşılabilmektedir. Bu menü yardımıyla arşivlenmiş kayıtlar her birin yanındaki "Dinle" tuşu vasıtası ile internet üzerinden dinlenebilmekte, silinmek istenen kayıtlar yanlarına birer işaret konulup silinebilmektedir. Bu silme işlemi arşiv klasöründen ilgili dosya yada dosyaları kaldıracaktır. Aynı anda birden fazla silme işlemi yapılabilmektedir.



Şekil 6-10 Arşiv Görüntüleme Arayüzü

7. SONUÇ

Bu çalışma sonucunda IP ağları üzerinden yapılan telefon görüşmelerinin şuandaki yapıda kolayca kayıt edilip arşivlenebileceği gözlemlenmiştir. Fiziksel kısıtlamalar nedeni ile dinleme işlemi geliştirilen yazılım sayesinde sadece yerel ağ içerisinde, yada yerel ağ ile başka bir ağ arasındaki telefon haberleşmesini kaydedebilmektedir.

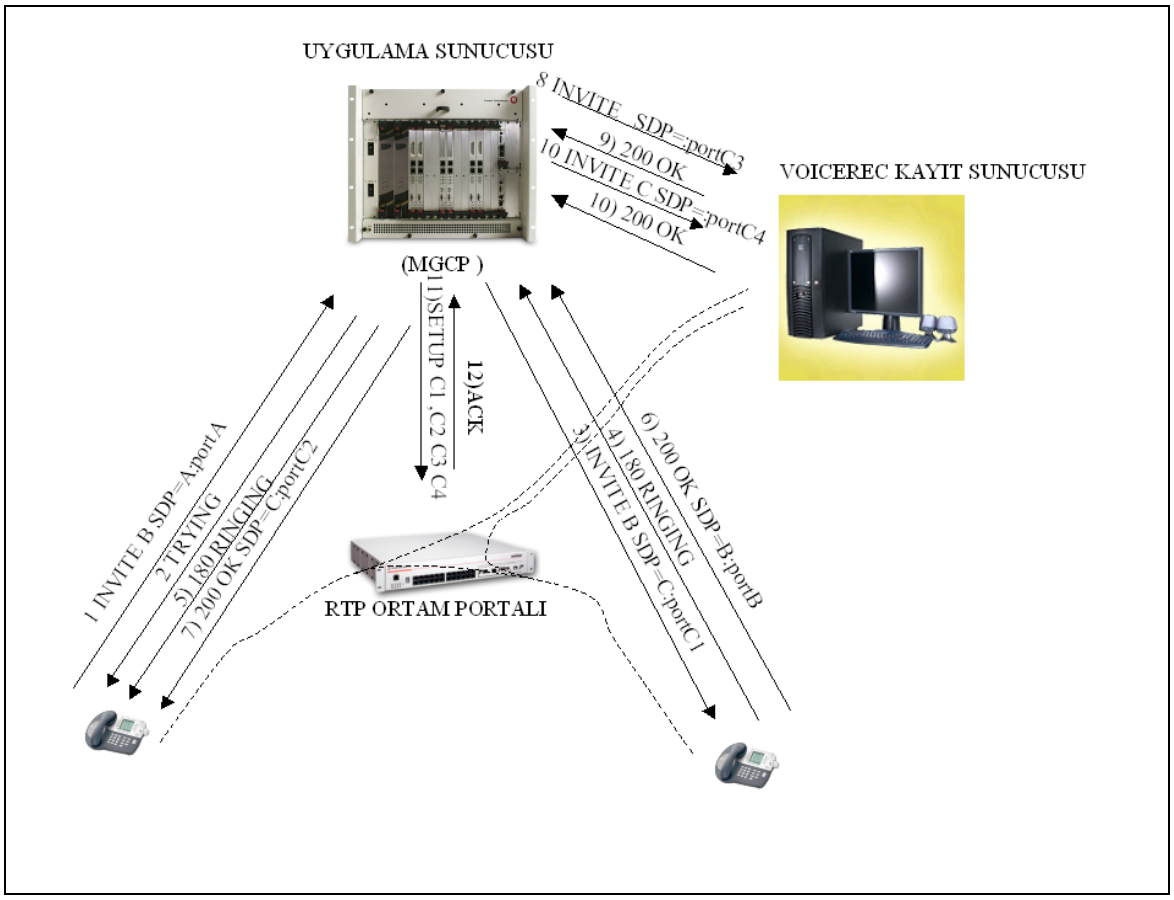
Program geliştirme sırasında :

- C++ program geliştirme ortamı daha yakından tanınmıştır
- DLL geliştirme ve modüler program geliştirme becerileri kazanılmıştır
- Dairesel tampon belleklerin uygulama becerileri kazanılmıştır
- WINPCAP ve WINSOCK kütüphanelerini ile program derleme becerisi kazanılmıştır.
- G711 ve G729 kodlayıcı-kod çözücülerinin çalıştırılması becerileri kazanılmıştır.
- Çoklu thread program geliştirme becerisi kazanılmıştır.

Yazılım hafızada yük harici durumda 9.968 Kbyte'lık bir yer tutmakta ve %0 işlemci kullanımı göstermektedir. Tek kanallı kayıt durumda ise : 9.968Kbyte'lık bir yer tutmakta ve yer yer %1 işlemci kullanımı göstermektedir. Kanal yük durumundan hafızada kullanılan bellek görüldüğü gibi artmamaktadır. Bunu sebebi programın çalışmaya başlaması ile kanal dairesel tampon belleklerini kendi kullanımı için ayırmasıdır. Kanal kayıt edilen kanal sayısının artması sadece işlemci üzerinde yük yaratmaktadır. Dosyalara yazım sırasında dinamik bellekler kullanılmaktadır. Bu beller dosyaya yazılacak verini hazırlanması sırasında tutulmakta veri yazıldıktan sonra bırakılmaktadır. Bu anlık değişimler Windows işlem yöneticisi tarafından yansıtılmamaktadır.

Voicerec uygulaması sadece bağlı bulunduğu ağdan geçen paketleri yakalayabilmekte ve kayıt etmektedir. Uzak iki ağ arasında yapılan sesli görüşmeler bu yapı ile kayıt edilmektedir. Bu problem Voicerec uygulaması ve çağrı yönetme sisteminin beraber çalışması ile aşılabilmektedir. Çağrı yönetme sistemi dinlenilecek aramaya karar vermeli SIP H323 gibi protokoller yardımı ile oluşturulan RTP akışının bir kopyasını Voicerec uygulamasına yönlendirebilecek yeteneğe sahip is Voicerec uzak ağlardaki konuşmaları da kayıt edebilme yeteneğine sahip olacaktır. Çağrı yönetme sistemi örnek olarak SIP protokollüyle Voicerec uygulamasına dinlenilecek ağ adresi ve port numarasını bildirebilir. Bu durumda Voicerec uygulaması için bir SIP protokol arayüzü geliştirilmesi gerekmektedir. . Böyle bir

uygulamada içinde bulunulan ağ devamlı ses görüşmeleri için devamlı taranmayabilir. Buda başarım üzerinde olumlu etki yaratacaktır. Sekil 7-1 de bu şekil kurulmuş bir ağ ve olası SIP mesajlaşmasına ait bir örnek bulunmaktadır.



Şekil 7-1 Arama yönletici ile beraber çalışma referans modeli

KAYNAKLAR

Arango, M., Dugan, A., Elliott, I., Huitema, C. and S. Pickett, "Media Gateway Control Protocol (MGCP) Version 1.0", RFC 2705,October 1999.

Cisco, “Guide to Cisco Systems VoIP Infrastructure Solution for SIP” Cisco Systems, Inc. 2003.

Cuervo, F., Greene, N., Rayhan, A., Huitema, C., Rosen, B. and J. Segers, "Megaco Protocol Version 1.0", RFC 3015, November 2000.

Donovan, S., "The SIP INFO Method", RFC 2976, October 2000.

Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

Handley, M., Schulzrinne, H., Schooler, E. and J. Rosenberg, "SIP: Session Initiation Protocol", RFC 2543, March 1999.

Harte, L., "Introduction to Public Switched Telephone Networks (PSTN), Local Loop, Switching, DSL, ATM, SS7, and AIN", August 2003.

Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.

ITU-T Recommendation H.323, Packet-Based Multimedia Communications Systems, 1998.

Johnston, A., Donovan, S., Sparks, R., Cunningham, C., Willis, D., Rosenberg, J., Summers, K. and H. Schulzrinne, "SIP Call Flow Examples", Work in Progress.

M., Zhang, L. and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

McCann, J., Mogul, J. and S. Deering, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.

Monson H. Hayes "Schaum's Outline of Digital Signal Processing (Schaum's)", August 1998.

Postel, J. (ed.), "Internet Protocol - DARPA Internet Program Protocol Specification", RFC 791, USC/Information Sciences Institute, September 1981.

Postel, J., "DoD Standard Transmission Control Protocol", RFC 761, January 1980a.

Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980b.

Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with SDP", RFC 3264, June 2002a.

Rosenberg, J. and H. Schulzrinne, "SIP: Locating SIP Servers", RFC 3263, June 2002b.

Schulzrinne, H., Casner, S., Frederick, R. and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 1889, January 1996.

Schulzrinne, H., Rao, R. and R. Lanphier, "Real Time Streaming Protocol (RTSP)", RFC 2326, April 1998.

EKLER

Ek 1 Voicerec Uygulaması Kaynak kodu

ÖZGEÇMİŞ

Doğum tarihi	21.02.1981	
Doğum yeri	Sinop	
Lise	1992-1999	Sinop Anadolu Lisesi
Lisans	1999-2005	Yıldız Üniversitesi Elektrik Elektronik fakültesi Elektronik ve Haberleşme Mühendisliği Bölümü

Çalıştığı kurum(lar)

2004-2007	Nortel Netaş Telekomünikasyon AŞ
2007-Devam ediyor	Alcatel Lucent Telekomünikaston AŞ