1. GİRİŞ

Tarih boyunca insanoğlunun gelişimine baktığımızda, özellikle son yüzyıl içerisinde sanayi devrimini takip eden zaman diliminde, tarih boyunca görülmemiş baş döndürücü bir gelişmenin yaşandığı her insanoğlunun kabul ettiği bir gerçektir. Bu gelişmenin bu denli hızlı olmasının sebepleri irdelendiğinde en göze çarpan unsurlardan birinin birbirinden kopuk insan toplulukları arasında mesafeleri ortadan kaldıran haberleşme teknolojilerinin olduğunu görürüz.

Çağlar boyunca birbirinden kopuk yaşayan insan toplulukları haberleşme ortamlarının gelişmesiyle fiziksel olarak olmasa bile düşünsel olarak bir araya gelme olanağı bulmuşlar ve sonuçta ortaya çıkan etkileşim, başta düşünce, medeniyet ve değişik teknoloji alanlarında alışverişe imkan sağlamış, doğal haliyle on yıllar belki yüzyıllarca çözüm bulunamayacak sıkıntılar aşılmış, bilim ve teknolojide gelişmeler hızlanmıştır.

Elbette haberleşme ortamlarının sağladığı bu hızlı teknolojik gelişme, yine haberleşme alanındaki teknolojilerin çeşit ve güçlerini artırmaktadır. Şu an en hızlı teknolojik gelişmelerin yaşandığı alanlardan biri de haberleşme teknolojileridir. Hatta haberleşme teknolojileri alanında faaliyet gösteren kurum ve kişiler dahi kimi zaman bu hıza ve değişime ayak uydurmakta zorlanmaktadırlar. Her geçen gün bilgi dağarcıklarına katmaları ve projelerinde uygulamak zorunda oldukları yeni teknolojilerle yüz yüze kalmaktadırlar.

1.1. Seminerin Amacı

Telekomünikasyon alanındaki hızlı gelişim ile, geleneksel ses iletişimin yerini; dinamik, interaktif, geliri yüksek, katma değerli servisler almaktadır. Henüz,12 yıllık bir geçmişi olan GSM haberleşmesinin altyapısında bile radikal değişiklikler olmaktadır. Gerek ISDN, PSTN gerekse GSM alt yapısında kullanılan sinyalleşme sistemi olan SS7 nin, yerini IP altyapısına bırakacağı görülmektedir. Bununla birlikte hem kablolu hem de kablosuz iletişim teknolojilerinde bant genişlikleri de artacaktır.

Türkiye ‘de IP üzerinden ses, görüntü, data v.s. iletiminin 1.Ocak.2004 tarihinden itibaren resmen yasallaşması ve Telekom altyapısının serbestleşmesi ile birlikte, bu hizmetleri verecek VoIP servis sağlayıcıları için abonelerine katma değerli, cazip servisler verebilmek kritik bir önem taşıyacaktır. Özellikle hem aboneler için mobil olmanın taşıdığı önem, hem de yeni nesil mobil el terminallerinde ki hızlı gelişim göz önüne alınırsa; kablosuz ağ teknolojileri üzerinde geliştirilecek servislerin kullanıcı sayısı da bir o kadar yüksek olacaktır.

Bilgisayar ağları ve ağ bileşenlerindeki teknolojik gelişim son yıllarda noktalar arası veri haberleşme hızları ile paralel bir gelişim süreci içerisine girmiştir. Bu gelişmelere paralel olarak mevcut ağ altyapıları üzerine eklenen yeni teknolojiler, geliştirilen yeni protokoller ve

teknikler ile birlikte bilgisayar ağları sadece bilgisayarlar için veri haberleşmesi alanında değil, başka alanlarda da hizmet vermeye başlamışlardır.

Bunlardan en etkileyici olanı ise VoIP olarak karşımıza çıkmaktadır. Aslında VoIP genel olarak mevcut telefon şebekesi ağ mimarisi üzerinde yapılan geliştirme çalışmaları sonucunda ortaya çıkan bir teknolojidir. Önceki zamanlarda anahtar devreli telefon sistemleri üzerinde ses haberleşmesi sağlarken günümüzde artık telekominikasyon şirketleri paket devreli sistemler üzerine geçerek IP tabanlı altyapılara dönmeye başlamışlardır.

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

VoIP telekom alanında gerçekleşen gelişmeleri takiben bilgisayar ağları üzerine geliştirilen sıkıştırma protokolleri ve ekipmanlar ile hayatımıza girmeye başlamıştır.

Kısa bir tanım yapmak gerekirse VoIP internet veya data hatları üzerinden ses aktarımı olarak açıklanabilir.

1.2. Seminerin İçeriği

2. INTERNET PROTOKOLÜ ÜZERİNDEN SESİN AKTARILMASI (VOIP)

2.1. VoIP'in Tanımı ve Avantajları

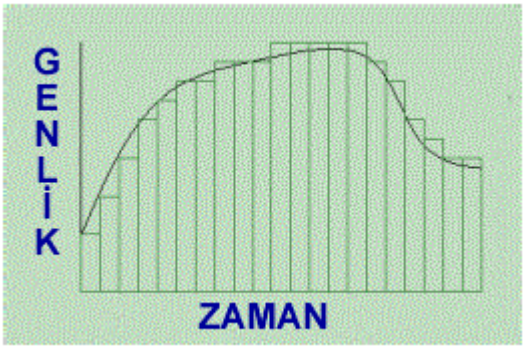
VoIP, Voice over Internet Protokol (Internet üzerinden ses) açılımına karşılık gelmektedir. VoIP, ses'i IP paketleri halinde internet üzerinden taşımaktır. Gelecekte PSTN (Genel Anahtarlamalı Telefon Ağı) şebekelerinin yerini alacağına kesin gözüyle bakılmaktadır. İletişim yatırım maliyetlerini çok büyük oranda düşürmesi, bakım onarım giderlerini düşürmesi, mobiliteyi arttırması ve dünyanın her yerinden erişebilirlik sağlaması, kurulum maliyetlerini düşürmesi, operasyonel maliyetleri düşürmesi [1], yüksek güvenirlilik [2], gelişme ve yeniliklere açık olması [3], var olan internet alt yapısı üzerine kurulabilmesi, ses ve veri hizmetlerinin bir arada verilebilmesi, paket bağlaşmalı birleşik şebeke hizmetlerinin devre bağlaşmalı ISDN'den çok daha verimli olarak sağlaması yeni bir teknoloji olarak sayılabilecek olan VoIP'in en önemli avantajları olarak sayılabilmektedir.

Voice Over IP'nin bir çok avantajı olmasına rağmen karşılaşılabilecek bir çok sorunu da bünyesinde barındırmaktadır. Bu sorunlar, servis kalitesinin hep aynı seviyede tutulamaması, ses paketlere ayrılıp iletim ortamına yollandıktan sonra paket iletiminde yaşanacak hataların seste kesilmelere yol açması, ses kalitesini klasik PSTN sistemlerdeki seviyeye çekilmesi için gerekli olan bant genişliğinin sağlanmasındaki zorluklar, VoIP'in güvenliği hakkındaki soru işaretleri sayılabilmektedir. Özellikle IP üzerinden ses iletirken kullanılacak olan UDP portları sistemde büyük açıklar oluşmasına sebep olabilmektedir. Bu açıklar sayesinde kötü niyetli bilgisayar korsanlarının gerçekleştirecekleri DoS (Denial of Service) saldırıları ile sistemi aşırı yüklemeleri söz konusu olabilmektedir. Bunun sonucunda, VoIP için gerekli olan QoS değerleri şebekedeki aşırı yük yüzünden sağlanamayabilir.[2] Ayrıca, ses iletiminin IP tabanlı sistemler üzerinden gerçekleştirilmesinde verinin analog bilgiden dijital bilgiye dönüştürülmesi sonucunda ses verisinin kötü niyetli kişiler tarafından dinlenmesi de söz konusu olabilmektedir. Bu sorunlara rağmen kaliteli ve güvenli bir VoIP oluşturulabilirse avantajları sayesinde vazgeçilemez bir sistem olacaktır.

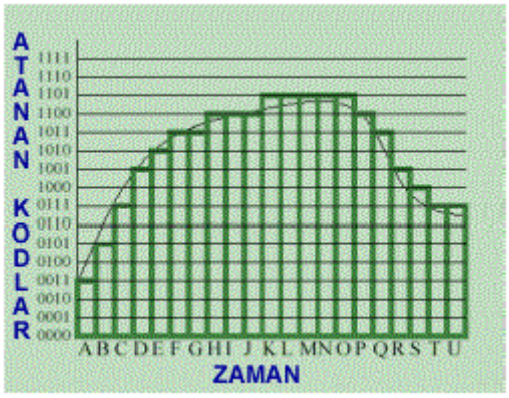
2.2. VoIP sisteminin çalışma prensibi

Dijital forma bilginin dönüştürülmesi uzak noktalara bilginin gönderilmesi noktasında büyük bir devrim niteliğindedir. IP üzerinden sesin iletiminde de bu prensip kullanılmaktadır. Öncelikle ses sinyali ADC'ler (analog digital converter) sayesinde anaolog bilgiden dijital bilgiye dönüştürülmektedir. Bunun için kullanılacak en basit donanım ses kartlarıdır. Analog bilginin dijitale dönüştürülmesi işlemi PCM (darbe kod modülasyonu) ile yapılabilmektedir. Analog bilginin dijital bilgiye dönüştürülmesi üç aşamadan oluşmaktadır. Birinci aşama örnekleme aşamasıdır ve analog veriden belirli aralıklarla örnekler alınması işlemidir. İkinci

aşamada alınan darbe şeklindeki veri örneklerinin belirli değerlere yuvarlanması işlemidir. Bu aşamaya kuantalama da denmektedir. Üçüncü ve son aşamada daha önceden belirlenmiş genlik değerlerine ötelenmiş sayısal ses işaretinin her genlik seviyesi için ikili kodlama (binary) şeklinde kodlanması işlemidir. Böylece PCM işaret elde edilmiş olur. VoIP sistemlerinde çoğu zaman 4 bitlik kod kelimeleri kullanılmaktadır.[4] Şekil 1 ve 2'de bilginin öncelikle darbe genlik modulayonu kullanılarak sesin örneklenmesi işlemi ve örneklenmiş verinin, kuantalanması ve kodlanması işlemleri gösterilmektedir.



Şekil 1 Sesin Örneklenmesi: PAM (Darbe Genlik Modulasyonu) kullanılarak örneklerin alınması



Şekil 2 Örneklenmiş ses işaretinin kuantalanması ve kodlanması işlemi

Elde edilen PCM sinyal ITU-T'nin G.764 tavsiyesine uygun olarak paketlenmekte ve karşı bilgisayara iletilmektedir. Oluşturulan paketlerin minimum band genişliği ile hedef bilgisayara gönderilmesi için ABD ve Japonya'da μ-Kuralı, Avrupa da ise A-kuralının kuantalama şemaları kullanılmaktadır. Tablo 1'de belirli giriş genlik değerlerine karşılık μ-kuralı ile kodlanan işaret için çıkış genlik değerleri ve bu değerler için gerekli olan kod çözücü genlik değerleri verilmiştir.

GİRİŞ GENLİK ARALIĞI	BASAMAK BOYUTU	SEGMENT KODU	KUANT. KODU	KOD DEĞERİ	KOD ÇÖZÜCÜ GENLİĞİ
0-1	1		0000	0	0
1-3			0001	1	2
3-5	2	000	0010	2	4
....			...	...	...
29-31			1111	15	30
31-35			0000	16	33
...	4	001	...	...	...
91-95			1111	31	98
95-103			0000	32	99
...	8	010	...	...	...
215-223			1111	47	219
223-239			0000	48	231
...	16	011	...	...	...
463-479			1111	63	471
479-511			0000	64	495
...	32	100	...	...	...
959-991			1111	79	975
991-1055			0000	80	1023
...	64	101	...	...	...
1951-2015			1111	95	1983
2015-2143			0000	96	2079
...	128	110	...	...	...
3935-4063			1111	111	3999
4063-4319			0000	112	4191
...	256	111	...	...	...
7903-8159			1111	127	8031

Tablo 1 µ-Kuralı Sıkıştırma – Çözme Tablosu[13]

Ses tablo 1 değerlerine göre sıkıştırılmaktadır. Bir sonraki aşama sıkıştırılarak hedef bilgisayara gönderilmiş olan verinin tekrar çözülmesi işlemidir.G.711 haricinde Huffmann sıkıştırması, G.723 ve G.729 gibi çeşitli sıkıştırma teknikleri de band genişliğinden kazanmak amacıyla kullanılmaktadır. Tablo 2'de ise belirli giriş genlik değerlerine karşılık µ-kuralı ile kodlanan işaret için çıkış genlik değerleri ve bu değerler için gerekli olan kod çözücü genlik değerleri verilmektedir.

GİRİŞ GENLİK ARALIĞI	BASAMAK BOYUTU	SEGMENT KODU	KUANT. KODU	KOD DEĞERİ	KOD ÇÖZÜCÜ GENLİĞİ
0-2			0000	0	1
2-4		000	0001	1	3
...			...		...
30-32	2		1111	15	31
32-34			0000	16	33
...		001	...	...	...
62-64			1111	31	63
64-68			0000	32	66
...	4	010	...	...	...
124-128			1111	47	126
128-136			0000	48	132
...	8	011	...	...	...
248-256			1111	63	252
256-272			0000	64	264
...	16	100	...	...	...
496-512			1111	79	504
512-544			0000	80	528
...	32	101	...	...	...
992-1024			1111	95	1008
1024-1088			0000	96	1056
...	64	110	...	...	...
1088-2048			1111	111	2016
2048-2176			0000	112	2112
...	128	111	...	...	...
3968-4096			1111	127	4032

Tablo 2 A-Kuralı Sıkıştırma – Çözme Tablosu

2.3. Diğer Modulasyon Teknikleri

Ses iletilirken gürültü, band genişliği ve dış etkiler önem kazanmaktadır. Bu etkileri azaltmak için darbe genlik modulasyonu ve darbe kod modulasyonun haricinde çeşitli sıkıştırma teknikleri mevcuttur.

2.3.1. Genel Amaçlı Sıkıştırma Algoritmaları

Sistem performansını arttırmak ve gerçek sese en yakın sesi elde edebilmek ve band genişliğini en verimli bir şekilde kullanabilmek için çeşitli sıkıştırma algoritmaları geliştirilmiştir.Bu algoritmalar aşağıda listelenmektedir.

– **Huffmann Sıkıştırması**

Değişik uzunluktaki sayısal kod kelimelerine mesajın atanması olayıdır. Kod kelimelerinin uzunluğu ilişkilendirilmiş mesajın ortaya çıkma olasılığıyla ters orantılıdır.

Böylece sık yollanan mesajlar seyrek yollanan mesajlara göre daha kısa bitlerle ifade edilmektedir [5]

– **LZ (Lempel Ziv) Sıkıştırma Algoritması**

Piyasada kullanılan birden çok LZ algoritması bulunmaktadır. Özellikle LZ78 algoritması bir sözlük kullanır. Bu sözlük string değişkenlerini ve bu değişkenlerin uzunluklarını tutmaya yarayan bir veri yapısına sahiptir. [4]

– **Diferansiyel PCM**

PCM kodlamada alınan örnekler belirli kuanta seviyelerine yuvarlatılarak kodlanmaktadır. Ancak alınan örnekler arasında çok küçük farklar olabilmektedir. Bu gibi durumlarda işaretleri ayrı ayrı göndermek yerine örnekler arasında ki farklar alıcıya gönderilir. Böylece band genişliği daha verimli şekilde kullanılır.

– **Doğrusal Delta Modulasyonu**

Bu modulasyon türünde modulatöre giren işaret ile modulatörden çıkan işaret arasındaki fark geri besleme yoluyla alınmaktadır. Daha sonra arasındaki farka bakılarak çıkış işaretine ±Δ şeklinde bir değer eklenerek çıkış, analog giriş işaretine yaklaştırılır. [6]

– **Adaptif Delta Modulasyonu**

Delta modulasyonunda olduğu gibi adaptif delta modulasyonunda da girişlerle çıkışlar arsında ±Δ gibi ekleme yapılmaktadır. Giriş ile çıkış arasındaki fark ne kadar büyükse eklenen farkta girişi yakalamak için o kadar büyük olacaktır.

2.3.2. Kullanılan Ses Kodlayıcı ve Kod Çözücüleri

Sesin sıkıştırılması ve tekrar çözülmesi işlemine codec (Coding-Decoding) denilmektedir. Aşağıda çeşitli ses codec örnekleri verilmektedir.

– **G.711 Sıkıştırması**

Örnekleme frekansı 8 KHz.'dir. Örnek başına 8 bit kullanılır. Toplam bit hızı gereksinimi 64 kbit/sn dir. Standart PCM sıkıştırmasıdır. MOS (Mean Opinion Score) değeri 4,3 tür.

– **G.723 Sıkıştırması**

Genel olarak düşük bit hızlarında iletim için kullanılmaktadır. Kalite olarak G.711 den kötüdür. Ancak band genişliği gereksinimi G.711 in onda biri kadardır. Cebirsel CELP yada MP-PLQ algoritmaları kullanır. MOS (Mean Opinion Score) değeri 4,1 dir.

– **G.726 Sıkıştırması**

16,24,32,40 kbit/sn bit hızlarında adaptif diferansiyel PCM kodlaması kullanır. MOS değeri 2 ila 4,3 arasında değişmektedir.[7]

– **G.728 Sıkıştırması**

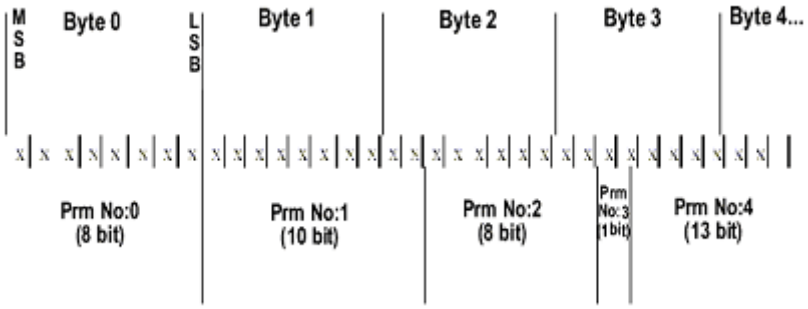
Düşük gecikmeli CELP kullanır.Bit hızı 16 kbit/sn, MOS değeri 4,1 dir. [8]

– **G.729 Sıkıştırması**

CS-ACELP algoritması kullanır. Bit hızı 8 kbit/sn 'dir. MOS değeri 4,1 dir. Kodlayıcı ses işaretlerini 10 ms'lik çerçeveler halinde kodlar. Ayrıca 5 ms lik aktarım gecikmesi oluşur.

Parametre	Açıklama	Kullanılan Bitler
Prm#0	Birinci Kod Kitabı	8 bit
Prm#1	İkinci Kod Kitabı	10 bit
Prm#2	Pitch peryodu	İlk alt çerçeve 8 bit
Prm#3	Parity (denklik) kontrolü ilk peryotta	1 bit
Prm#4	Kod kitabı birinci indeksi (Pozisyonlar)	13 bit
Prm#5	Kod kitabı ikinci indeksi (İşaretler)	4 bit
Prm#6	Pitch ve kod kitabı kazançları	7 bit
Prm#7	Göreceli pitch peryodu	İkinci alt çerçeve 5 bit
Prm#8	Kod kitabı birinci indeksi (Pozisyonlar)	13 bit
Prm#9	Kod kitabı ikinci indeksi (İşaretler)	4 bit
Prm#10	Pitch ve kod kitabı kazançları	7 bit

Tablo 3 G.729 Bit Paketlemesi



Şekil 3 G.729 Bit Dizilişi

2.3.3. Çeşitli Kodlamalar İçin Ses Kalitesi

Uzun yıllar süren araştırmalar sonucunda insanların sesleri algılayış biçimleri değerlendirilmiş ve bir notlandırma sistemi oluşturulmuştur. MOS derecelendirmesi denen bu sistem ITU'nun P.800 tavsiyesinde bulunabilir. Kısaca MOS derecesi 5 ile 1 arasında değişirken, müşterilerin bu işten tatmin olma yüzdeleri de MOS sayısıyla orantılı olarak

değişir. Tablo 4'de codecler için derecelendirme katsayıları ve paket gecikmesi gibi unsurlar bulunmaktadır.

Codec	Veri Hızı	Paket Süresi	Paket Gecikmesi	Jitter Buffer Süresi	MOS
G.711u	64 kbps	20 ms	1.5 ms	2 datagram (40 ms)	4.4
G.711a	64 kbps	20 ms	1.5 ms	2 datagram (40 ms)	4.4
G.729	8 kbps	20 ms	15.0 ms	2 datagram (40 ms)	4.07
G.723.1 MPMLQ	6.3 kbps	30 ms	37.5 ms	2 datagram (60 ms)	3.87
G.723.1 ACELP	5.3 kbps	30 ms	37.5 ms	2 datagram (60 ms)	3.69

Tablo 4 Codec Özellikleri

2.3.4. DSP ve Sesin Paketlenmesi

Ses işleme uygulamalarında bu iş için özelleşmiş DSP (Sayısal İşaret İşleme) işlemcileri kullanılmaktadır. Bu işlemciler, sahip oldukları güçlü yongalar sayesinde birçok karmaşık işlemi rahatlıkla yapabilmektedirler. DSP'lerin yerine getirdikleri en önemli görev ise; analog telefon işaretlerini IP şebekesinin algılayabileceği sayısal formasyona dönüştürmek ve bunları telefon hatlarına vermektir. Bir DSP'de aranan başka bir özellik ise; insan tarafından oluşturulmuş sesleri rasgele dağılıma sahip olan gürültüden ayırmaktır.[9]

Tablo 5'den çıkarılabilecek bir önemli sonuç, sessizlik bastırması yapıldığında gerekli olan band genişliği ihtiyacının yarı yarıya azalmasıdır. Bu durum, sistem kaynaklarının daha ekonomik olarak kullanılmasını sağlar. Yalnız burada dikkat edilmesi gereken bir nokta vardır. Sessizlik bastırması olduğu takdirde konuşan tarafın dinleyen tarafın hala hatta olduğunu anlaması için arkaya yazılım yardımıyla biraz gürültü verilmesi gereklidir. Aksi takdirde iki taraf arasında çeşitli iletişim problemleri çıkacaktır. Tablo 5'den çıkan diğer bir sonuç ise G.729 ses codecinin en düşük paket büyüklüğüne sahip olmasıdır. Bu durum düşük hızlı şebekelerde gerçek zamanlı iletimi mümkün kılarken, codecin içindeki başlık/yük oranı yüksek olduğundan şebeke verimi biraz düşebilir. Son olarak, G.723 gibi yüksek sıkıştırma yapan codecler kullanılırken codec gecikmesinin de sistem performansını olumsuz etkileyeceği göz ardı edilmemelidir. Bu durumda band genişliğinden kazanılsa bile işlemci gücünden kaybedilmiş olacaktır.[10]

Codec	Ses Band Genişliği (kbps)	MOS	Codec Gecikmesi	Paket Büyüklüğü (byte)	IP\UDP\RTP Başlığı (byte)	cRTP	L2 Başlığı (byte)	Toplam Band Genişliği	Sessizlik Bastırmalı BG.
Ethernet									
G.711	64	4.1	1.5	160	40		14	85.6	42.8
G.711	64	4.1	1.5	160		2	14	70.4	35.2
G.729	8	3.9	15	20	40		14	29.6	14.8
G.729	8	3.9	15	20		2	14	14.4	7.2
PPP									
G.711	64	4.1	1.5	160	40		6	82.4	41.2
G.711	64	4.1	1.5	160		2	6	67.2	33.6
G.729	8	3.9	15	20	40		6	26.4	13.2
G.729	8	3.9	15	20		2	6	11.2	5.6
G.723	6.3	3.9	37.5	30	40		6	16	8
G.723	6.3	3.9	37.5	30		2	6	8	4
Çerçeve Aktarma									
G.711	64	4.1	1.5	160	40		4	81.6	40.8
G.711	64	4.1	1.5	160		2	4	66.4	33.2
G.729	8	3.9	15	20	40		4	19.7	9.9
G.729	8	3.9	15	20		2	4	9.6	4.8
G.723	6.3	3.9	37.5	30	40		4	15.5	7.8
G.723	6.3	3.9	37.5	30		2	4	7.6	3.8
ATM									
G.711	64	4.1	1.5	160	40		5 hücre	106	53
G.711	64	4.1	1.5	160		2	4 hücre	4	42.4
G.729	8	3.9	15	20	40		2 hücre	2.3	14.1
G.729	8	3.9	15	20		2	1 hücre	14.1	7.1
G.723	6.3	3.9	37.5	30	40		4	22.3	11.1
G.723	6.3	3.9	37.5	30		2	4	11.1	5.6

Tablo 5 Band Genişliği Hesaplamaları [17]

2.3.5. Servis Kalitesi (QoS – Quality of Service)

Servis Kalitesi çok farklı yöntem ve teknolojileri kullanarak bir ağ üzerindeki trafik akışının istikrarlı bir şekilde düzenlenmesini sağlayan teknikler bütünüdür. Bir ağ sahip olduğu bant genişliğinin kullanımını aktif bir biçimde monitör eder ve herhangi bir zamanda kalabalık oluşup oluşmadığının izini tutar. Bilgisayar ağı aktif bir biçimde kullanım modellerini üretir ve bant genişliği istatistiklerini tutar. Bunun yanında hizmet sağlama, kullanım ve mevcut bant genişliğinin dağıtımına bağlı olarak hali hazırdaki kurallara uyulmasını zorlar.

Servis kalitesi bir aktarım sisteminin performans ölçüsüdür. Bu bakımdan aktarım sisteminin kalitesini ve ayakta kalma gücünü yansıtır. Hizmetin ayakta kalması ve istenen her zamanda ona erişilebilmesi Servis Kalitesinin temel elemanıdır. Herhangi bir Servis Kalitesi gerçekleştirimi uygulamaya alınmadan önce yapılması gereken en yararlı iş altyapının daima ayakta kalacak şekilde düzenlenmesidir. Aktarım kalitesinin karar verilmesinde etkili üç faktör bulunur bunlar: kayıp, gecikme ve gecikme miktarıdır.

VoIP konusu göz önüne alındığında servis kalitesi (quality of service), önceden tanımlanmış uçtan uca hizmet gereksinimlerinin IP şebekesi gerçekleştirilebilme yeteneği olarak tanımlanabilir. Özel olarak, IP şebekesinde QoS sadece şebeke tarafından güvenilirlik gereksinimlerini sağlamak değildir. Belirli gecikme gereksinimlerinin de sağlaması lazımdır. Örneğin, IP QoS teknikleri, sistemin ihtiyaç duyduğu yeterli band genişliğini sağlamalı ve belirli gecikme ve jitter değerlerinin gerçeklenmesini öngören ses ve görüntü aktarım uygulamalarında bu teknikler sistem önceliklerini de dikkate alacak şekilde gerekli manipulasyonlarda bulunmalıdır.

2.3.6. Servis Kalitesini Etkileyen Unsurlar

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

– **Gecikme (Delay):** Ses paketinin kaynaktan yollanması ile alıcı tarafından alınması arasında geçen süre olarak tanımlanır. Başlıca gecikmeler beş adettir.[8,11]

• Örnekleme Gecikmesi: Darbe kodlama modulasyonu yapılmadan önce ses işareti örneklenir. İşte bu örnekleme esnasında belirli bir süre geçer. Bu geçen süreye örnekleme gecikmesi denir. Bu değer işaretin örnekleme aralığı ile doğru orantılıdır. Çoğu zaman 125- 150 ms kadardır.

•**Sıkıştırma Gecikmesi:** Sesin belirli bir codec ile kodlanması sırasında geçen süredir. Bu süre kodlama algoritmasının karışıklığına ve kodlama yapan işlemcinin işlem yapma hızına bağlıdır.

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

•**Transmisyon Gecikmesi:** Paketin iletimi esnasında iletim yollarında geçen süredir. Bu süreyi azaltmanın en iyi yolu, iletim hattının enformasyon hızını arttırmaktır. Örneğin,

16kb'lik bir veri paketi 4kb/s hızındaki bir hattan iletildiğinde iletim 4 saniye alırken, 48kb/s'lik bir hattan (ISDN-D kanalı)yollandığında iletim 0,33 saniye alır.

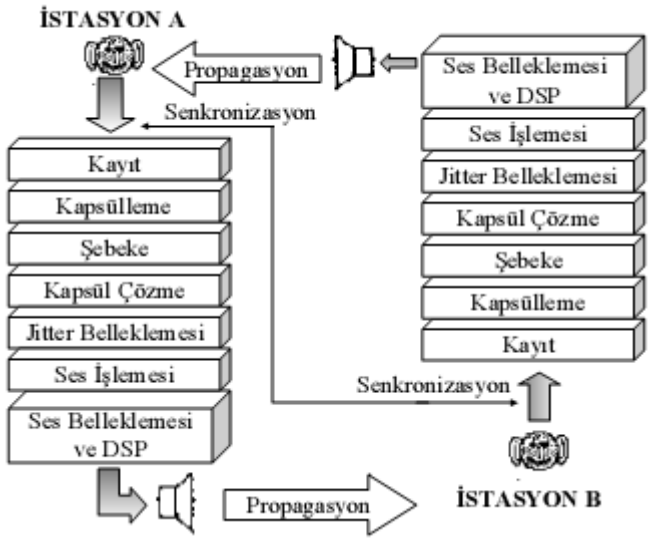
•**Bellekleme Gecikmesi:** Tüm paket gecikmelerinin aynı yapılması amacıyla verilerin belirli bir süre belleklerde (buffer) tutulmasından kaynaklanan gecikmedir. Ayrıca bu gecikme sadece karasal transmisyonda görülmez. Bunun yanı sıra uydu haberleşmesinde de uydunun Dünya ile olan konumunun devamlı değiştiği orta (MEO) ve kısa yörünge (LEO) uydularının veri aktarımı esnasında da görülür.

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

•**Yankı (Echo):** İletim hatlarındaki ek noktalarında veya hattın uygun empedans ile sonlandırılmaması nedeniyle oluşur. Empedans uyuşmazlığı olan noktalarda işaretlerin bir bölümü hatta yoluna devam ederken elektriksel işaretin diğer bir bölümü ise yansır. Benzer etki PSTN'deki iletim hatlarında kullanılan 2 tel – 4tel dönüşümü yapan hibrit trafolarda da ortaya çıkar.[12]

•**Net Çıkış Hızı (Throughput):** Alıcı tarafından alınan verilerin ortalama hızıdır. Bu ortalama hesaplanırken tıkanma durumu da göz önünde tutulmalıdır.

•**Paket Kayıp Oranı:** Hedefe ulaşmayan veri paketlerinin o hedefe yollanan veri paketlerine oranıdır.



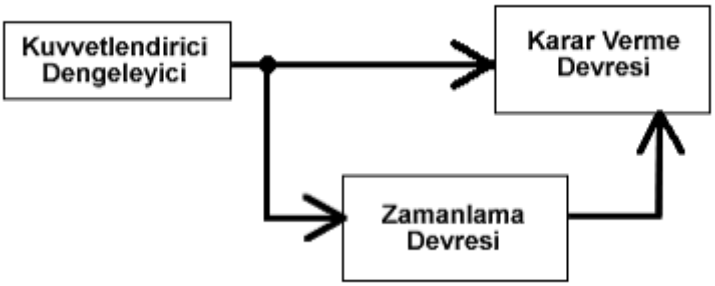
Şekil 4 Sistemdeki Tüm Gecikmeler

•**Gürültü:** Hattın enformasyon hızını dolayısıyla servis kalitesini etkileyen bir başka unsur da gürültüdür. Shannon denklemi gereğince, aşağıdaki formüle başvurulursa, kanal kapasitesini (C) band genişliğinin (B) ve işaret-gürültü oranının (S/N) ne şekilde etkilediği daha rahat anlaşılabilir.

$$C = B \cdot \log_2(1 + \frac{S}{N})$$

Hatta bulunan gürültü arttıkça kanal kapasitesi düşecek; dolayısıyla iletim süresi artacak ve servis kalitesi olumsuz etkilenecektir. Gürültünün azaltılması için DSL sistemlerinde ayırıcı (splitter) denen bir cihaz kullanılırken, radyo link sistemlerinde eliptik dalga kılavuzları, GSM gibi hücresel kablosuz mobil sistemlerde verici işaret gücünün arttırılması gibi yöntemler kullanılır. Ayrıca gürültü bazen o kadar kritik bir noktaya gelir ki; sistemdeki bit – hata oranı (BER) değerlerinin normal sınırlara çekilmesi için ek maliyetli rejeneratif repetörler (repeater, access point) kullanılır. [13] Şekil 5'te rejeneratif repetörün blok diyagramı verilmektedir.

İkinci bir gürültü kaynağı ise; sesin kaydedildiği ortamın gürültüsü ya da arka fon gürültüsüdür. Bu gürültünün engellenmesi, hat gürültüsüne nispeten daha kolaydır. Mikrofon tarafından alınan ses işaretinin genliği, özel bir eşik sezici aracılığıyla belirli bir genlik değeriyle karşılaştırılır ve bu genliğin altında kalan değerler karşı tarafa iletilmezler, çünkü bu bileşenler çoğunlukla gürültüden kaynaklanan işaretlerdir. Buna ek olarak, verici tarafta konuşma olmadığı zaman karşı tarafa sessizlik olduğunun anlatılması için özel bir işaret yollanır. Böylece kısıtlı band genişliği daha verimli kullanılmış olur ve hatta gereksiz veri paketleri yollanmaz.



Şekil 5 Rejeneratif repetörün blok diyagram

2.4. VoIP Mimarisi

VoIP mimarisi denince ilk akla gelen cihazlar uç birim cihazlarıdır. Bunlar telefon ve bilgisayarları kapsayan geniş bir ailedir.

2.4.1. Standart Şebeke Elemanları

VoIP şebekelerinde sık kullanılan elemanlar aşağıda verilmektedir. Bu elemanların bir kısmı SIP (Session Initiation Protocol)'de bir kısmı da H.323 mimarisinde kullanılmaktadır.

•**Kullanıcı Ajanı (UA):** Bu kategoriye giren cihazları "Hardphone" denen telefon cihazları ve "Softphone" denen bilgisayar üzerinde çalışan programlar (Ör: MSN Messenger

veya Netmeeting gibi) diye ikiye ayırmak mümkündür. Kullanılan hardphonelar bildiğimiz ahizeli telefon cihazlarıdır. Normal telefon postalarından tek farkları ise bağlantı ara bağdaşımı olarak telefon hattı yerine ethernet ara bağdaşımını kullanırlar. Bunun yanı sıra, H.323 ve SIP gibi işaretleşme protokollerini desteklerler. Bu sisteme bağlanan bir hardphone'un en önemli özelliği, sabit (statik) bir IP adresine sahip olmasıdır. Örneğin aynı telefon İstanbul yerine Hakkâri'deki bilgisayara da bağlansa telefon numarası değişmez. Kişiler hardphoneların yaptıkları bütün işleri kendi modemlerine ve ara bağdaşım programlarına yaptırmaktadırlar. VoIP mimarisinde etkin rol oynayan bir başka cihaz da ağ geçitleridir. Gateway (GW) olarak da adlandırılan bu cihazların en büyük özellikleri protokol dönüşümü yapmalarıdır. Başka bir değişle PSTN ile IP şebekesi arasındaki ara bağlaşımı sağlarlar.[14] İki çeşit ağ geçidinden söz edilebilir.

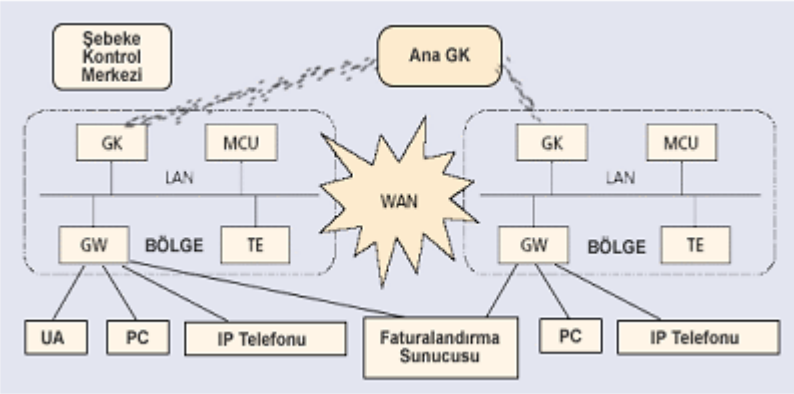
•**İşaretleşme Ağ Geçidi (Signalling Gateway):** İşaretleşme enformasyonunun IP şebekesi ile CSN (Devre Bağlaşmalı Şebeke) arasında aktarılmasını sağlar. Bu tür GW'ler hem SS7 hem de SIP ve H.323 desteklerler.

•**Medya Ağ Geçidi (Media Gateway):** PSTN ile IP şebekeleri arasında aktarılan verinin hedef şebeke tarafından anlaşılabilir hale getirilmesi için gerekli değişiklikleri yapmaktan sorumludur. [15]

•**Terminal (TE):** Şebekenin sonlanma noktalarıdır. Bunlar özellikle H.323 işaretleşmesinde çift yönlü transfere izin veren ve hem GW'ler hem de MCU (Multi Point Control Unit)'larla haberleşme yeteneğine sahip olan cihazlardır. Bir terminal diğer bir terminali arama yeteneğine sahip olduğu gibi bu arama işlemi bir gatekeeper (GK) üzerinden de yapılabilir.

•**Çok Noktalı Kontrol Ünitesi (MCU):** Şebekedeki üç ve daha fazla terminalin veya GW'in çok noktalı konferans görüşmesine katılmasını sağlar. MCU'lar da şebekenin sonlanma noktalarından biri olabilirler.

•**Geçit Sorumlusu (Gatekeeper):** Şebekedeki adres tercüme işlemlerini gerçekleştiren cihazlardır. Ayrıca terminallerin, ağ geçitlerinin ve MCU'ların birbirlerine erişimlerini kontrol eden cihazlardır. Zaman zaman, GW'ler diğer GW'lere ulaşmak istediklerinde eğer hedef ağ geçidinin fiziksel konumu veya MAC adresi belli değilse bunu geçit sorumlusuna sorarak öğrenirler. Bu bakımdan şebeke üzerinde büyük bir hâkimiyetleri vardır. [16]



Şekil 6 VoIP şebekesinin genel yapısı

2.4.2. Seçime Bağlı Şebeke Elemanları

Seçime bağlı şebeke elemanları denince, akla ilk gelen düşünce bu elemanların bulunmaması durumunda sistem işleyişinin etkilenmeyeceğidir. Aslında bu elemanların birçoğu ticari uygulamalarda kullanılmaktadır ve şebekeye hem yapay zekâ hem de ek özellikler kazandırmaktadır. Ayrıca şebeke yönetimi bu cihazlar sayesinde çok kolaylaşmıştır. Bu elemanlar aşağıda verilmektedir.

•**Faturalandırma Sunucusu:** Şebekedeki GW'lerin genelde bağlandıkları noktalardır. Bu birimler GW'lerden aldıkları süre ya da konuşma esnasında iletilen veri bilgisini işleyerek, kullanıcılara servis sağlayıcıların tarifeleri doğrultusunda fatura çıkarırlar. Faturalandırma işlemi bazen GW'ların da bir fonksiyonu olarak kullanılabilir ama çoğu operatör bu işlemin kendi sunucuları üzerinde yapılmasından yanadır.

•**Şebeke Yönetim Merkezi (NMC):** Bu aygıt sistem yöneticisiyle şebekenin etkileşimini sağlar. NMC şebekedeki her cihaza kullanıcı ajanları, IP telefonları ve kişisel bilgisayarlar hariç bağlıdır. Örneğin bir ağ geçidinin herhangi bir ağ arayüz kartında oluşacak problemi sistem yöneticisi NMC aracılığıyla fark eder. Bu sezme işlemi, NMC'nin belirli aralıklarla bağlı olduğu tüm cihazlara belirli veri paketleri gönderip onların çalışıp çalışmadıklarını belirlemesiyle olur. Şebeke elemanlarından herhangi birinde bir problem çıktığı takdirde NMC önceden tanımlanmış olan program kodlarını çalıştırır veya sistem yöneticisine e-posta yollayabilir. Hatta servis sağlayıcı şirketin bir GSM operatörüyle anlaşması varsa, GSM operatörünün mesaj sunucuları üzerinden sistem yöneticisine SMS yollayabilir.

•**Servis Yönetim Merkezi (SMC):** Bu cihaz, AAA (üç A) işlemlerinden sorumludur. Bu üç A harfi İngilizce'deki Authorization (yetkilendirme), Authentication (doğrulama), Accounting (hesap tutma) kelimelerinin baş harfleridir. Özellikle kullanıcının sisteme kaydolması esnasında sahip olduğu kullanıcı adı ve parolanın kontrolü için bu cihaza

başvurulur. Genel olarak kullanıcı bilgileri bu sunucularda tutulur. SMC'ler diğer medya ağ geçitleri ile de RADIUS güvenli iletişim protokolüyle haberleşebilirler.

•**Proxy Sunucusu (PX):**Bazı firmalar tarafından genişletilmiş proxy sunucusu olarak da adlandırılan bu eleman, hem bir uç birim hem de yeri geldiğinde bir sunucu olarak görev yaparak, diğer uç birimlerden gelen istekleri işler. Bazı durumlarda bir LAN üzerindeki IP telefonlarının çağrı isteklerini kendi üzerinden çıkışını sağlayarak bir konsantratör görevi görür. Dış ağlardan gelen istekleri ise kendi ağına aktaran bir köprü görevi görmektedir. Böylece yayma işlemleri de bu cihaz üzerinden yapılabilmektedir.[9]

•**Yönlendirme (Redirect) Sunucusu:** Bu sunucu, arayan tarafa aranan taraf hakkındaki lokasyon bilgilerini iletirler. Proxy sunucularının aksine yönlendirme sunucuları kendi SIP isteklerini başlatamazlar. Eğer yönlendirme sunucuları hizmet verebilir durumdalar ise çağrı isteğini işleyebilirler; ancak hizmet veremiyorlarsa bunu başka bir sunucuya yönlendirirler.

•**Lokasyon Sunucuları:** Bu sunucular özellikle SIP bazlı sistemlerde kullanılırlar. Bunlar, uç birimlerin fiziksel adreslerini tutarlar ve bir virtüel devre kurulması esnasında SIP sunucuları tarafından konum bilgisinin elde edilmesi amacıyla başvurulan bir cihazdır.

•**NAT Sunucusu:** NAT (Şebeke Adres Tercümesi) sunucusu IP v.4'deki adres kısıntısının önüne geçilmek geliştirilmiş bir şebeke elemanıdır. Böylece çok sayıda IP adresine ihtiyacı olan büyük firmalar tek bir uluslararası legal IP alarak bütün sistemlerini bu IP adresi üzerinden dış ağlara açabilmektedirler.[17] Tabii ki; bu firmaların kendi iç ağlarında çalıştırdıkları cihazlarda belirli IP adreslerini kullanmaları zorunluluğu vardır. Aksi takdirde bu cihazlar birbirleriyle bile haberleşemezler. Sonuç olarak, iç ağlarda kullanılan IP adreslerine illegal IP adresleri denmiştir ve bu adresler yalnız iç ağlarda kullanılmak için IETF tarafından ayrılmıştır. Aşağıda bu IP adres bölgeleri verilmiştir. [18]

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

NAT sunucusunun bir önemli özelliği de, sesli görüşme yapılan şebekedeki IP adreslerini gizlemesi nedeniyle şebekenin daha dışarıdan gelebilecek saldırılara karşı daha güvenli hale getirilebilmesidir. Ayrıca tek IP üzerinden giden ve gelen trafiğin gözlenmesi ve o adresteki cihaza yapılabilecek saldırılara karşı çeşitli yöntemlerle (güvenlik duvarı ve saldırı tespit sistemi gibi)önlem alınabilmesi çok daha kolaydır.

3. VoIP PROTOKOLLERİ

IP ağı üzerinden sinyalleri taşıyan protokollere Voice Over IP protokolleri denir. VoIP, Katman 3 protokolüdür ve Katman 2 deki pek çok point-to-point (noktadan noktaya) ve link katman protokollerini (PPP, Frame Relay, ATM gibi) veri transferi için kullanır.

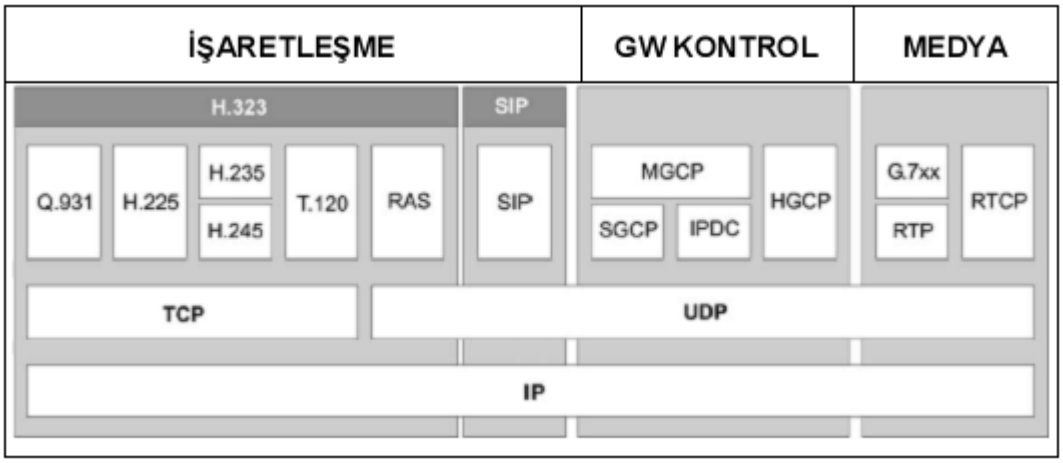
VoIP protokollerinin en önemlisi RTP (real-time transport protocol –gerçek zamanlı iletim protokolü)'dir. RTP, ses ve video verisini Internet üzerinden taşımak için paket biçimi standartları tanımlamıştır. RTP bir multicast (çoklu yayın) protokolü olarak tasarlanmıştır. Ancak sonradan pek çok unicast (tekli yayın) uygulamaya uygulanmıştır. Daha çok video konferans gibi real-time stream media (gerçek zamanlı kesintisiz ortam) uygulamalarında kullanılmaktadır. Protokol, RFC 3550 ile tanımlanmıştır.

RTP dışında, SIP (Session Initiation Protocol), H.323 gibi alternatif protokoller de mevcuttur. H.323 ve SIP ağ üzerinde dağıtık bir yapıda çalışır ve bir çağrı başlatılırken uç nokta ekipmanları dışında başka ağ elemanlarının desteğine ihtiyaç duymaz. SIP, IETF tarafından geliştirilen noktadan noktaya multimedya sinyalleşme protokolüdür. ASCII tabanlı HTTP benzeri bir yapıdadır. H.323, ITU-T 'ye ait H.320 standardının video konferans için geliştirilmiş şeklidir. Tablo 6'te VoIP Protokolu ve Fonksiyonlarının OSI Katmanları gösterilmektedir.

OSI Katmanı	VoIP Protokolu ve Fonksiyonları
7. Application	NetMeeting benzeri uygulamalar
6. Presentation	Codec'ler
5. Session	H.323/MGCP/SIP
4. Transport	RTP/TCP/UDP
3. Network	IP
2. Data Link	Frame Relay, ATM, Ethernet, PPP, MLP vs...

Tablo 6 VoIP Protokolu ve Fonksiyonları

İnternet üzerinden ses taşınırken iki önemli faz vardır. Bunlar işaretleşme ve veri aktarım fazıdır. İşaretleşme esnasında güncel olarak iki önemli protokolden söz etmek mümkündür. Bunlar ITU'nun bir standardı olan H.323 ve IETF'nin bir standardı olan SIP (Session Initiation Protocol)'dir. Veri aktarım fazı ise; işaretleşmeyle anlaşmaya varan ve senkronize olan iki uç birim cihazının birbirleriyle gerçek zamanlı haberleşmeye başlamasıyla gerçekleşir. Tablo 7'te veri aktarımı esnasında hangi protokol ailesinin kullanıldığı belirtilmiştir.



Tablo 7 Çoklu Ortam Şebeke Protokolleri [19]

3.1. İşaretleşme Protokolleri

3.1.1. SAP ve SDP

Özellikle multicast (bütün kullanıcıların birbirleriyle direkt mesaj alışverişinde bulundukları) ortamlarda oturum yönetiminde kullanılan protokollerdir. Böyle ortamlarda kullanıcı sunucu (client - server) kavramı önemini yitirir. SAP, oturum enformasyonunun dağıtılması için multicast grupların kullanım ilkelerini tanımlar. Oturumu açan taraf periyodik olarak oturum enformasyonunun yeniden duyurulmasından sorumludur ki böylece "özel duyuru grubu" (special announcements group) içinde yer alan kullanıcıların yeni bir oturumun açıldığından haberleri olsun. Oturumu tanımlayan enformasyonun formatı SDP tarafından belirlenir. [20] Bu enformasyonlar arasında uç birimlerin RTP ve RTCP protokolleri yardımıyla gerçek zamanlı veri transferi için hangi portları kullanacakları bilgisi de yer alır. [21]

a) SAP Paket Formatı

SAP paketleri aşağıdaki formata sahip UDP paketleridir. Tablo 8'de SAP paket formatı gösterilmiştir.

SAP Başlığı
Metin Bölümü

Tablo 8 SAP Paket Formatı

SAP mesajları multicast ortamlardaki duyuru işlemlerini yaparlar. Bu iş için SAP başlığı bölümü kullanılır. Bunun yanında kullanılan metin bölümünde SDP oturum açıklaması bulunur

ve bu bölüm 1 kbyte'tan büyük olamaz. Bir pakette sadece bir adet oturum duyuru mesajına yer verilir.

b) SDP'nin Görevleri

SDP özellikle iki önemli amaca hizmet eder. Bunlar, varolan bir oturumla haberleşmeyi sağlamak ve oturuma katılmak isteyen taraflara gerekli enformasyonu sağlamaktır. Unicast (sadece karşılıklı iki kullanıcının varolduğu) bir ortamda ise SDP sadece oturuma katılmak isteyen tarafa bu oturumun başlatılması için gerekli enformasyonu sağlamakla yükümlüdür. Böylece SDP aşağıdaki enformasyonu içerir: [9]

• Oturum adı ve amacı,

• Oturumun aktif kalacağı süre,

• Oturumu oluşturan medyanın türü,

• Bu medyayı (adresler, port numaraları, formatlar, gibi) almak için" gerekli olan enformasyon

Eğer kaynaklar bir oturuma katılmak için sınırlıysa, bu durumda SDP aşağıdaki enformasyonu da içerebilir:

- Konferansta kullanılacak band genişliği enformasyonu
- Oturumdan sorumlu kişinin kontak enformasyonu

c) SDP Medya İçeriği

SDP aşağıdaki bölümleri kapsar:[22]

- Medyanın türü (görüntü aktarımı, ses aktarımı, vs.)
- Taşıma protokolü (RTP/UDP/IP, H.320 gibi)
- Medyanın formatı (H.261 Video, MPEG video, vs.)

Multicast (bütün kullanıcıların birbirleriyle direkt mesaj alışverişinde bulunduğu ve ikiden çok kullanıcının tek bir oturumda haberleştiği) ortamlar için gerekenler:

- Taşınacak medya için multicast adresi
- Taşınacak medya için taşıma portu

Unicast ortamlar için gerekenler:

- Karşı tarafın adresi
- Karşı tarafla iletişim için gerekli olan port numarası

3.1.2. SIP

SIP, IETF'nin Multiparty Multimedia Session Control (MMUSIC) grubu tarafından geliştirilen multimedia uygulamaları için bir protokol grubudur. MMUSIC H.323'ün aksine küçük bir çekirdek protokol ile başlayıp bu protokolü ihtiyaçlara göre geliştirmeyi

amaçlamaktadır. Temel olarak HTTP protokolünü alan bu protokol, e-mail gibi diğer internet servisleri ile de benzerlik göstermektedir.

Bu protokole göre bir çağrı başlatıldığı zaman, gelen çağrı, çağrıyı başlatan tarafa servis veren bir sunucuya yönlendirilmektedir. Çağrının yönlendirildiği sunucu çağrıyı reddedebilir veya bir başka sunucuya yada terminale yönlendirebilir. Çağrı bu şekilde cevap verecek bir sunucu bulununcaya kadar ağda hiyerarşik olarak ilerletilir. SIP basit bir protokoldür ve basitliği nedeni ile karmaşık hizmetlerin verilmesi gerektiği durumlarda diğer protokollerden faydalanması gerekebilir.

SIP'in çağrı kontrol mesajlarının geçirilebileceği güvenilir bir kanal açmak için INVITE ve ACK mesajları bulunmaktadır. SIP bir alt seviye taşıyıcı protokol için minimum varsayımları yapar. Bu protokol güvenilirliğini kendisi sağlayıp TCP'nin güvenlik ile ilgili normlarını kullanmaya gerek duymaz. SIP kullanılacak codec uzlaşması (negotiation) için yani o oturumda hangi codec'in kullanılacağına karar vermek için Session Description Protocol (SDP)'yi kullanmaktadır.SIP'in sağladığı servisler ise;

· User location-Kullanıcı yeri: haberleşme için kullanılacak uç sistemin belirlenmesi

· Call setup: arayan ve aranan tarafların zil çaldırması ve çağrı parametrelerinin kurulması

· User availability: aranan tarafın haberleşmeye dahil olma isteğinin belirlenmesi

· User capabilities: kullanılacak media-ortam ve media parametrelerinin belirlenmesi

· Call handling: çağrının transferi ve sonlandırılması

SIP'in Parçaları

SIP Sistemi temel olarak iki parçadan oluşur.

- **User Agent - Kullanıcı birimi:**Kullanıcı birimi kullanıcı adına çalışan uç sistemdir. Bu birim iki parçadan oluşur, İstemci ve Sunucu. İstemci kısmı İstemci Kullanıcı Birimi (User Agent Client - UAC) diye bilinir. Sunucu kısmı ise Sunucu Kullanıcı Birimi (User Agent Server - UAS) şeklinde ifade edilir.
- **Network Servers - Ağ Sunucuları:**Bir ağda 3 tip sunucu vardır. Bir kayıt sunucusu, kullanıcıların mevcut lokasyonları ile ilgili bilgileri alır. Bir proxy sunucu ise aldığı istekleri, aranan tarafın lokasyonu hakkında daha fazla bilgiye sahip olan bir sonraki sunucuya iletir. Yönlendirme sunucusu ise, aldığı istek üzerine bir sonraki sunucunun adresini öğrenerek, çağrı isteğini göndermek yerine, bu adresi istemciye iletir. SIP protokolü, uç birimlere fazla fonksiyonellik yüklemesi sonucu ücretlendirme ve ağ yönetimi konularında problemlerle karşılaşabileceği yönünde eleştirilmiştir.

3.1.3. H.323

Genellikle bir işaretleşme standardı olarak görülen H.323 aslında bir çok protokolün birleşerek oluşturduğu bir protokoldür. H.323, ses, veri ve görüntünün birleşik bir şekilde IP bazlı şebekelerden nasıl iletilmesi gerektiğini açıklayan kuralları barındıran bir protokoldür. H.323, gecikmeye duyarlı ses ve veri trafiğinin IP telefonu uygulamalarında gerçekleştirebilme kurallarını tanımlar.[23]

– **H.323 Protokol Yığını**

H.323 protokol yığını aşağıdaki temel bileşenlerden oluşur.

- İşaretleşme ve kontrol: H.245, H.225, RTCP
- Ses codecleri: G.7xx
- Görüntü codecleri: H.26x
- Çoklu ortam haberleşmesi: T.12x
- Taşıma: RTP

Tablo 9'da H.323'de hangi protokollerin hangi katmanlarda kullanıldığı gösterilmiştir.

<table>
<tr><th rowspan="2">Veri</th><th colspan="2" rowspan="2">Kontrol ve İşaretleşme</th><th rowspan="2">Sistem Kontrolü</th><th>Ses Codecleri</th><th>Görüntü Codecleri</th><th rowspan="2">Ses ve Görüntüsel Kontrol</th></tr>
<tr><td>G.7xx</td><td>H.26x</td></tr>
<tr><td>T.12x</td><td>H.245</td><td>H.225.0</td><td>H.225.0 RAS</td><td colspan="2">RTP</td><td>RTCP</td></tr>
<tr><td colspan="3">UDP/TCP</td><td colspan="4">UDP</td></tr>
<tr><td colspan="7">IP</td></tr>
<tr><td colspan="7">Değişken Katman 2 Protokolleri</td></tr>
<tr><td colspan="7">Değişken Katman 1 Protokolleri</td></tr>
</table>

Tablo 9 H.323 Protokol Yığını [24]

3.1.4. H.323 v.2

Bu sürüm var olan H.323 protokolüne yeni özellikler eklemiştir. Bu özellikler aşağıda verilmiştir.

- Hızlı Bağlanma (Fast Connect):Çağrının kurulma hızını arttırır. Böylece çağrı kurulum süresi kısalır.
- Ek Hizmetler (Supplementary Services): H.450 serisi standartlar da sisteme entegre olmuştur. Bu standartlardan H.450.1 bu ek servislerin kontrolünü ve işaretleşmesini sağlar. H.450.2 (çağrı transferi) bir A kullanıcısının B kullanıcısıyla olan görüşmesini B ile C

kullanıcısı arasındaki görüşmeye dönüştüren ve bu transferin A kullanıcısı tarafından seçilmesine izin veren bir standarttır. H.450.3 ise; gelen çağrının başka bir hedefe yönlendirilmesini sağlar.

- H.235 güvenliğini destekleyen H serisi çoklu ortam terminalleri: Bu özellik doğrulama, güvenilirlik, gizlilik ve reddedilmeme gibi işlemleri tanımlar. Doğrulama sadece yetkili kullanıcıların haberleşebilmesini sağlayan bir mekanizmadır. Güvenilirlik, gelen paketle kaynaktan yollanan paketin içindeki veriyle birebir aynı olmasını sağlar. Gizlilik, paketin şifreleme yoluyla sadece hedeflenen alıcı tarafından alınmasını sağlar. Reddedilmeme ise, kullanıcının bir konferans görüşmeye katılmak istediğinde onun o görüşmeye katılma isteğinin reddedilmemesini garantiler.

•Üst üste bindirilmiş gönderim (Overlapped Sending): GK'nin hafızasında bir rota belirlenemezse kullanıcıdan ekstra adres enformasyonu ve yönlendirme enformasyonu istenir. Böylece bağlantı daha hızlı kurulmuş olur. Diğer bir değişle, arayan tarafın direkt olarak GK ile temas kurması sağlanır.

•Alternatif Uç Birim Noktası (Alternate Endpoint): Yedekleme amacıyla bir uç birim noktasına kendisine alternatif bir bitim noktası adresi veya ikincil şebeke arayüzü tanımlaması olanağı verir.

•Şebeke Sorumlusu Fazlalığı (GK redundancy): Birincil GK hizmet dışı kaldığında kullanıcının ikincil ve üçüncül GK'lar tanımlamasına olanak verir. Böylece verilen hizmetin sürekliliği artar.

•**Canlı Tutma(Keep Alive):** Bir uç birimin GK'ya kaydolmasına; böylece GK'nın onu belirli aralıklarla test ederek, uç birimin çalışıp çalışmadığına karar vermesini sağlar. Bu işlem GK'dan yollanan kontrol mesajlarıyla yapılır.

•**QoS:** Bitim noktalarının kendi QoS parametrelerini belirlemelerini sağlar. Bu şekilde şebeke performansının arttırılması sağlanır.

•**Yaşam Süresi (Time to Live):** GK'nın uç birim kaydını ne kadar süre aktif olarak tutacağını belirler. Böylece belirli bir süre aktif durumda olmayan uç birimlerin sistemden kayıtları silinir.

•**Kaynağın Müsait Olması (Resource Availability):** GW'nin kendi kapasite enformasyonunu GK'ya bildirmesini; böylece daha uygun rotaların GK tarafından çizilmesini ve sistem ükünün dağıtılmasını sağlar.

•**Bitim Noktası Yetenek Ayarı (Endpoint Capability Set):** GK'nın ek servisleri desteklemeyen uç birimlerden gelen çağrıların tekrardan yönlendirilmesine izin verir.

3.1.5. H.323 v.3

Bu sürüm daha önceki sürümlere ek olarak, hızlı bağlantı kurulması için TCP yerine UDP zerinden işaretleşmenin yapılmasını sağlar. Tabi ki bu teknik küçük şebekelerde işe

yarayan bir tekniktir. Binlerce çağrının üzerinden geçtiği şebekelerde UDP uzun çağrı kurulum süreleri oluşmasına neden olur. H.323 v.3, SS7 işaretleşmesinin olduğu PSTN şebekelerine de entegre olmuştur ve dört adet yeni ek servise destek vermeye başlamıştır. Bunlar H.450.4 ile o anda etkin olan çağrıyı belirli bir süre bekletip diğer gelen çağrıya bakılmasını, H.450.5 ile gelen bir çağrının belirli bir süre bekletilip; daha sonra önceden belirlenmiş farklı telefonlar tarafından karşılanabilmesini sağlar. Aynı şekilde bir çağrının farklı telefonlardan aynı şekilde çıkarılmasını sağlar. H.450.6 ile aranan tarafın meşgul olduğu durumlarda gelen çağrının bekletilmesi sağlanır. H.450.7 kullanıcıya kendisini bekleyen mesajların olduğu bildirilir. Ayrıca H.323 v.3, H.246C desteğidir. Bu destek ise ISUP ile H.226 konuşabilmesini sağlar.

3.1.6. H.323 v.4

H.323'ün dördüncü sürümü diğer sürümlere göre daha geniş şebekeler için geliştirilmiştir. İlk üç sürümde ağ geçitleri bütün işleri hallederlerdi. Yapılan bu işler, işaret dönüşümü, çağrı kontrolü ve çeşitli çoğul ortam codecleri (ses ve görüntü) arasında dönüşümleridir. Bütün bu görevlerin ağ geçitlerinin üzerine bindirilmesi ise şebeke büyüdüğü zaman ölçeklenebilirlik açısından sıkıntılarına yol açmaktadır.

H.323 v.4 geniş şebekelerdeki ölçeklenebilirlik problemini GW'leri üç ayrı şebeke elemanına ayırarak çözmüştür. Bu üç eleman aşağıda verilmiştir.

- Akılsız (Dumb) Medya Ağ Geçidi (MG)
- Medya Ağ Geçidi Kontrolörü (MGC)
- İşaretleşme Ağ Geçidi

MG'ler sadece PSTN ile veri şebekesi arasında akan sesin gideceği şebekenin formatına uygun şekle dönüştürülmesinden sorumludurlar. Böylece paket şebekesindeki RTP başlığını ve PSTN'deki taşıyıcı kanalları sonlandırma görevini üstlenmiş olurlar. MGC'ler MG'lerin çağrıları nasıl işlemesi gerektiğini bilen ve gerekli emirleri MG'lere veren yönetim cihazlarıdır. Eğer MG ve MGC'ler farklı cihazların içinde bulunuyorlarsa, yani tümleşik değillerse; bu durumda birbirleriyle iletişim kurabilmeleri amacıyla GCP (Ağ Geçidi Kontrol Protokolü) adlı protokolü kullanırlar. GCP'nin ITU-T tarafından H.323 v.4 için geliştirilmiş hali H.248'dir. H.248 ise IETF'nin MEGACO protokolüyle beraber çalışması için tasarlanmıştır.

SG'ler ise sistemdeki tüm işaretleşmeden sorumludurlar. Bunlar, SS7 işaretleşme mesajlarının IP şebekesi üzerinde de uygun formatta yol almalarını sağlayacak dönüşümleri yaparlar.

H.323 v.4, çoklu akış iletimine izin verir; ki bu iletim ses ile görüntü verilerinin birleştirilmiş bir şekilde aynı anda akmasını sağlar. Bu özelliğin sağladığı en büyük fayda ise;

ses ve görüntünün önceki sürümlere göre çok daha kolay bir şekilde senkronize olabilmesidir. Ayrıca dördüncü sürümde desteklenen ek servislerin sayısı arttırılmıştır. Bunlar:

•**H.450.8**: Kullanıcı bilgilerinin karşı taraftaki uç birim noktasına gönderilmesini sağlar. Bu hizmet PSTN şebekesinde sadece arayanın numarasını gösterme (caller id) şeklinde verilebilmektedir.

•**H.450.9**: Aranan taraf meşgul olduğunda veya cevap yoksa çağrının otomatik olarak kesilmesini sağlar.

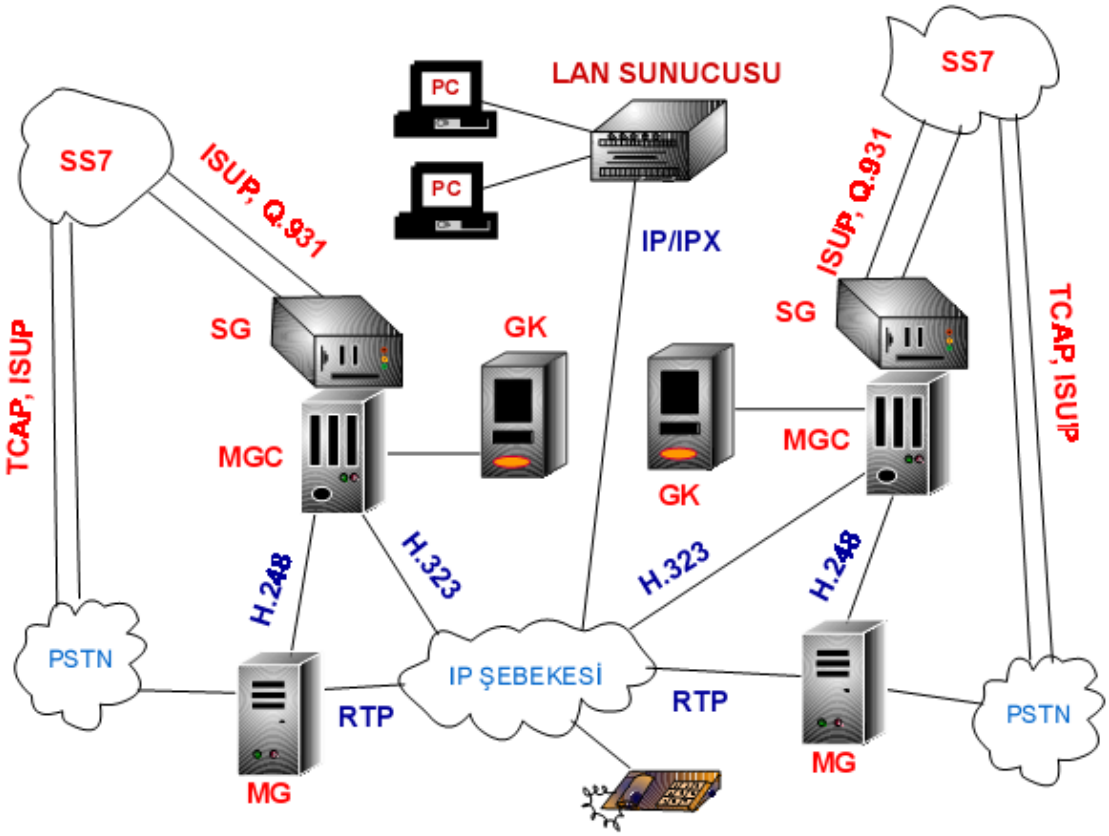
•**H.450.10:** Arayan tarafın isteğine bağlı olarak aranan taraf meşgulse, arayanın hatta tutulması ve meşgul durumun sona ermesiyle birlikte çağrının kurulmasını sağlar. Bu özellik, ülkemizde aranan tarafın devamlı meşgul olduğu, yarışma programları gibi yerlerde, kullanılmak için oldukça elverişlidir.

•**H.450.11:** Arayan A kullanıcısının, aranan B kullanıcısı C kullanıcısıyla görüşme halindeyse araya girmesini sağlar. Bu hizmet, A kullanıcısının isteğine göre verilebilir. Özellikle önceliği yüksek olan kullanıcılar (komutanlar, büyük patronlar) bu hizmetten yararlanmak isteyeceklerdir.

H.323 v.4, ayrıca H.323 cihazlarının HTTP tabanlı kontrolüne izin veren Annex K desteğine ve bir H.323 cihazının nitelik sunucusuna (feature server) bağlanıp şebekeye ek özellikler sağlayan Annex L desteğine sahiptir. Ayrıca, ek kayıt (additive registration) adı verilen bir özelliğe sahiptir. Bu özellik, uç birimlerin GK'ya çeşitli uzantılarla (alias) kayıt olmasını sağlar. Önceki sürümler uzantı desteğini vermezler. Buna ek olarak, alternatif GK'ları güvenilirliğin arttırılması amacıyla desteklerler. Son olarak, SIP benzeri arama formatı da desteklenir. [25]

Şekil 7'de H.323 elemanlarını içeren bir şebeke örneği verilmiştir.

Bu şekilde ayrıca hangi işaretleşme protokollerinin de kullanıldığı gösterilmiştir.



Şekil 7 H.323 v.4'ün desteklediği ekipmanlarla donatılmış bir şebeke örneği

3.1.7. SIP ile H.323'ün Karşılaştırılması

Tablo 10'da SIP ile H.323'ün karşılaştırılması verilmiştir.

Kategori	SIP	H.323
Uç Birimler	Akıllı	Akıllı
Akıllı Şebekeler ve Servisler	Sunucular tarafından sağlanır. (Proxy, Redirect, Registrar)	Geçit sorumlusu tarafından sağlanır.
Kullanılan Model	İnternet/WWW	Telefon/Q.SIG
İşaretleşme Protokolü	UDP ya da TCP	TCP (UDP Version 3'den itibaren opsiyonel)
Medya Protokolü	RTP	RTP
Kod Tabanı	ASCII	İkili (Binary) (ASN.1 kodlaması)
Kullanılan Diğer Protokoller	IETF/IP protokolleri: SDP, HTTP/1.1, IPmc ve MIME	ITU / ISDN protokolleri: H.225, H.245, ve H.450
Çeşitli Satıcıların Ürünleriyle Çalışabilme	Yaygın	Yaygın

Tablo 10 SIP H.323 Karşılaştırması[26]

Yukarıdaki tablodan çıkarılabilecek sonuçlar şunlardır. Her iki protokol de VoIP sistemindeki işaretleşme işlemlerinin yürütülmesi amacıyla geliştirilmiştir. H.323 daha eski bir protokol olup ve ITU-T'nin telekomunikasyon dünyasına kabul ettirmeye çalıştığı bir protokoldür. Diğer taraftan SIP ise IETF'nin geliştirdiği bir protokoldür. Burada da bir çok konuda olduğu gibi ABD ile Avrupa'nın çekişmesi görülmektedir. SIP'in yeni çıkan bir protokol olması nedeniyle çeşitli avantajları vardır. Bunlardan bazıları, metin bazlı olmak, kolay geliştirilebilir olmak ve UDP gibi bağlantısız bir aktarım protokolünü desteklemektir. SIP modüler bir yapıya sahiptir ve görevler akıllı sunucular arasında paylaştırılmıştır. Buna karşın H.323'de daha merkezi kontrol sistemi mantığı ile hareket edilmiş olup geçit sorumlusu olan cihazlar büyük yetkilerle donatılmışlardır. Son yıllarda birçok şirket ürettikleri cihazlarda hem SIP hem de H.323 desteği vermeye başlamışlardır. Ayrıca SMC, PX, GK, Lokasyon sunuculuğu gibi birçok işlem tek bir cihazda toplanmıştır. Çok fonksiyonel bu cihazlara "softswitch" denir ve bu cihazlar iki işaretleşme protokolünü de desteklerler.

3.2. Veri Aktarım Protokolleri

Veri aktarım fazında başlıca üç protokol kullanılır. Bunlar; kaynak ayırmak için kullanılan SVP (Kaynak Ayırma Protokolü), gerçek zamanlı veri akışı için kullanılan RTP (Gerçek Zaman Protokolü) ve bu protokolün kontrolünü sağlayan RTCP (Gerçek Zaman Kontrol Protokolü) olarak adlandırılır.

Sistemde veri aktarılmaya başlanmadan önce SIP veya H.323 ile işaretleşme yapılır. Daha sonra RSVP ile sistem kaynaklarının bir bölümü VoIP görüşmesi için ayrılır. Sonra SDP ile uç birimler RTP ve RTCP kullanılması için hangi UDP portlarının kullanılacağından haberdar olurlar.[21]

3.2.1. RSVP

RSVP internet üzerinden oturum açmak için gerekli olan ayrılması için kullanılır. IP bağlantısız bir protokol olduğu için yol kurulması gibi bir durum oluşmaz. Dolayısıyla bu yollar için belirli bir band genişliği ayrılmaz. Kurulan yollardaki trafik akışı için gerekli olan band genişliğini sağlamak için RSVP tasarlanmıştır. RSVP yönlendirme faaliyetlerinde bulunmasa da ICMP ve IGMP'de olduğu gibi taşıma olarak IP'nin çeşitli sürümlerini kullanır. IP'de olduğu gibi kendi mesajları için lokal yönlendirme tablolarına bakarak yol çizer. RSVP bir multicast gruba ilk katılımda kullanmak için IGMP'yi kullanır ve multicast grubu için kaynak ayırma protokollerini çalıştırır. [24]

– **RSVP'nin Çalışma Modları**

RSVP'nin iki çalışma modu bulınmaktadır. Bu modlar yol kurma modu ve yer ayırma modudur.

•**Yol Kurma Modu:** Bu modda RSVP unicast ve multicast çalışma prosedürlerinden birini işletir. Yukarıda da anlatıldığı gibi, IGMP multicast gruba ilk katılım anında kullanılır. Daha sonra kaynak ayırma prosedürleri çalıştırılır. RSVP trafiği alan tarafların akış için servis kalitesi isteklerine ihtiyaç duyar. Alıcı tarafta çalışan uygulama hangi QoS profilinin geçirileceğine karar verir. İstek mesajının alınmasından sonra RSVP veri akışının gerçekleşeceği tüm düğümlere istek (request) mesajları yollar. Ayrıca yönlendiriciler tarafından dağıtılan QoS istek mesajlarının düğümlere ulaşmasını ve her düğümde bu istek mesajları için gerekli kaynağın ayrılması için kullanılır. [27]

•**Yer Ayırma Modu:** Bu modda alıcı taraf yollayıcı tarafa ve ara elemanlara (yönlendiriciler gibi) kendi QoS gereksinimlerini haber verir. Rezervasyon modu olarak da geçer.

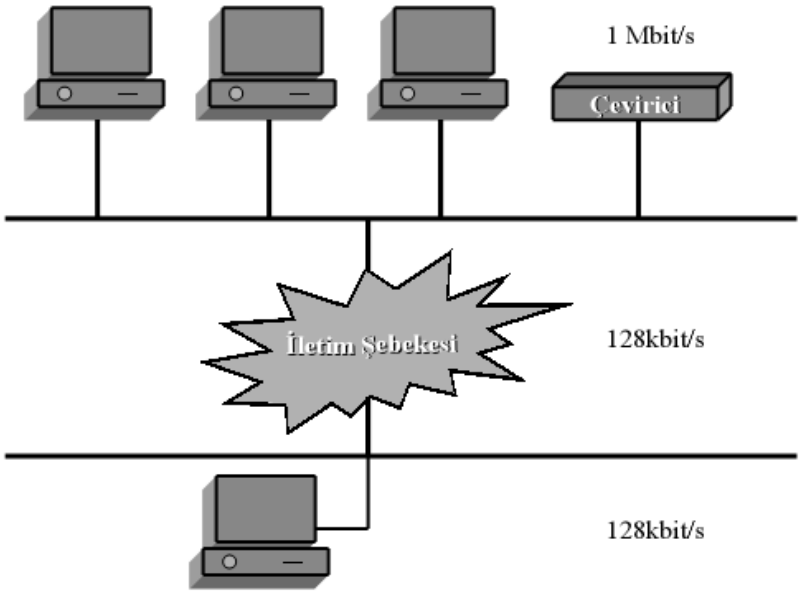
3.2.2. RTP

RTP (Gerçek Zaman Taşıma Protokolü) uçtan uca gerçek zamanlı ses ve görüntü verisinin taşınması gibi şebeke taşıma fonksiyonlarını icra edebilmek için geliştirilmiş bir protokoldür. RTP, UDP üzerinde çalışır. UDP'nin çoğullama ve başlık kontrol mekanizmalarını kullanır. Buna rağmen RTP başka alt seviye protokolleriyle de çalışabilir. RTP'nin bir diğer önemli özelliği ise multicast ortamlarda birden çok kullanıcının veri transfer işlemini gerçekleştirebilmesidir. Bu şekilde sesli ve görüntülü konferans uygulamaları gerçeklenebilir duruma gelmiştir. [28]

RTP sahip olduğu dizi numaraları sayesinde veriyi alan tarafta ses veya görüntünün tekrar birleştirme işini kolaylaştırmaktadır. Bunun yanı sıra RTP'nin içerdiği zaman damgası (etiketi) ile de sistemdeki senkronizasyon işlemleri kolayca yapılabilmektedir.

– **RTP Elemanları**

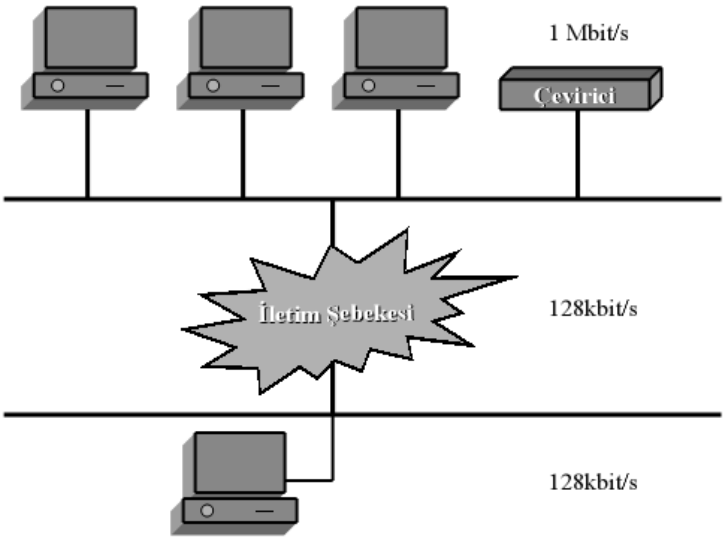
RTP yapı olarak çeşitli çeviricilerin (translator) ve karıştırıcıların (mixer) kullanılmasına olanak sağlar. Çeviriciler iletilen verinin ya da yükün (payload) sentaksının başka bir sentaksa dönüştürülmesi ve kodlanması işlemini yaparlar. Örneğin 1 Mbit/sn'lik görüntü üreten bir sistem olsun. Bu sistemde üretilen veri gerçek zamanlı olarak 128kbit/sn'lik veri yolu üzerinden RTP çeviricisi yardımıyla uygun şekilde taşınabilir. Çeviriciler Şekil 'de gösterildiği gibi veriyi üreten tarafın veri yolundan daha hızlı bir çıkışa sahip olduğu durumlarda kullanılır.



Şekil 8 RTP Çeviricisi [24]

RTP çeviricisi yukarıda görünen 3 istasyonun da birbirleriyle etkileşim içinde bulunmasını sağlar. Ayrıca bu istasyonlardan gelen veriler sistemin band genişlemesi sınırlamalarına uygun olarak paketlenirler.

RTP karıştırıcıları ise birden çok kaynaktan gelen veriyi tek bir veri akışı şekline dönüştürmeye yararlar. Özellikle ses operasyonlarına katılan karıştırıcılar alıcıya gelen işaret kalitesini düşürmezler. Sadece birden çok işareti tek bir işaret içinde belirli bir formata uygun olarak kombine ederler. Unutulmaması gereken bir durum ise; karıştırıcıların yük çevirme işlemini yapmamalarıdır. Şekil 9'da RTP karıştırıcısı gösterilmektedir.



Şekil 9 RTP Karıştırıcısı

3.2.3. RTCP

RSVP ile yer ayırma işleminin ardından, veri paketleri RTP yardımıyla uç birimler arasında akmaya başlar. Daha sonra RTCP devreye girer ve uç birimlerin sağlayabilecekleri ve alabilecekleri hizmet kalitesi seviyesinden haberdar olmalarını sağlar. Aslında bir sunucu da bağlı olduğu düğümlerden aldığı geri bildirim yoluyla servis kalitesi ayarlamaları yapabilir. Ama bu hareket biçimi RTCP tarafından tanımlanmamıştır.[9]

– **RTCP Paket Türleri**

RTCP ile taşınan raporlar sistemdeki uç birimler hakkında bilgi ve istatistikler verir. Bu raporların tipini değiştiren ise RTCP paket numarasıdır. RTCP paket türleri Tablo 11'de gösterilmiştir.

Numara	Paket Türü	Kullanım Amacı
200	Gönderici Raporu	Aktif paket göndericilerinin gönderme ve alma istatistiklerini gösterir.
201	Alıcı Raporu	Alan taraflar için sadece alma istatistiklerini gösterir.
202	Kaynak Açıklaması	Kaynak açıklama bölümlerini içerir.
203	Sonlandırma Mesajı (Bye)	Katılımın sonunu belirtir.
204	Uygulamaya Özel	---

Tablo 11 RTCP Paket Türleri

4. VOIP GÜVENLİĞİ

IP, kablosuz ağ ve ses birleşmesi birçok esneklik sağlamakla birlikte bunların yanında bir de karanlık tarafı yanında taşımaktadır. Bu hizmeti veren taşıyıcılar ve firmaların karşı karşıya oldukları tehditlerin yanı sıra son kullanıcıya yönelik tehditlerde içermektedir. Bu saldırıların amacı finans sağlamak, bedava konuşmak, kimlik ve bilgi çalmak, kötü şöhret edinmek veya kullanıcıları rahatsız etmektir.

VoIP teknolojisinde analog ses sinyalleri dijital ses paketlerine dönüştürülerek internet üzerinden telefon görüşmesi yapılması sağlanmaktadır. Bunu yaparken de eski sistemlere göre düşük maliyetli telefon görüşmesi, daha fazla özellik taşıması, gelişmeye açık olması, kolay yönetim gibi avantajlarda sağlamaktadır. Ancak hızla gelişen VoIP teknolojisi beraberinde de güvenlik problemlerini de getirmektedir. VoIP trafiği de aynı diğer veri akışlarında olduğu gibi bir router (yönlendirici)dan diğer bir routere giden trafik olarak değerlendirmek mümkündür. Bu durumda VoIP trafiği kötü niyetli biri tarafından kesilebilir, engellenebilir, kopyalanabilir, yavaşlatılabilir veya değiştirilebilmektedir.

Günümüzde VoIP güvenliği için çeşitli bant genişliği güvenliği sağlanmaktadır. Bu trafik sınırlama, rate sınırı koyma veya servis kalitesini arttırma (QoS) gibi özelliklerdir. Ancak VoIP'te güvenliği sağlamak için trafiğin başladığı noktadan bittiği noktaya kadar güvenliğin sağlanması gerekmektedir. Bu yüzden bant genişliği üzerinden çözüm politikaları VoIP güvenliği noktasında yetersiz kalmaktadır.

İdeal VoIP güvenliği için bütün internet tehditlerine karşı önlem alınması gerekmektedir. Yani sadece VoIP aygıtlarını değil VoIP protokolünü de güvenli hale getirmek gerekmektedir. Bu yüzden öncelikle uzaktan geliştirilen hafıza taşması, açıklarına sahip olan Windows, Unix , Linux gibi sistemlerin korunması, DDoS, worm, ve diğer saldırılara karşı ağ katmanında önlem alınması, VoIP bant genişliğinin korunması gibi noktalarda çok dikkatli bir şekilde önlemlerin alınması gerekmektedir.

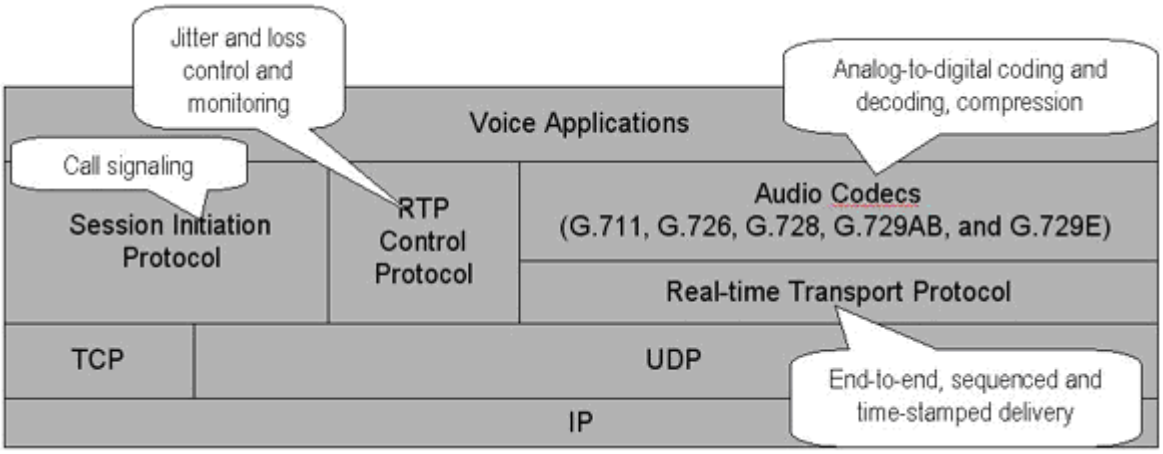
4.1. Güvenlik Tehditleri

VoIP ses akışına kelimeler sokmak en çok karşılaşılabilen güvenlik tehditleri arasındadır. Bu saldırıda saldırgan hali hazırda konuşmakta olan iki kişinin akmakta olan VoIP trafiğine müdahale ederek araya kelimeler sıkıştırmaktadır. Bunu taraflardan sadece birisi duyabilir. Yani karşı taraf araya konan kelimelerinde sizin tarafınızdan söylendiğini sanmaktadır.

Diğer bir güvenlik tehdit de SPAM'lardır. Ses posta kutunuza binlerce istenmeyen ses kaydıyla karşı karşıya kalabilirsiniz. Yada yapılacak olan bir DoS saldırısı ile ses kalitesinde ciddi kayıplar veya kesilmeler yaşamak mümkündür.

Bu tarz tehditlere karşı ses paketlerini şifrelemek veya IP telefonlarda dijital sertifikalar kullanılması kısa vadeli çözümler içinde görülmektedir. Çünkü ses paketlerini şifrelemek araya giren saldırganları engellese de sistemin performansını aşırı derecede etkilemektedir. Firewall kullanmakta çok etkileyici bir çözüm olarak görülmemektedir. Ateş duvarı ses sistemi ile tam bütünleşik çalışmadığı sürece konuşmayı kapatacağı zamanı kestirememesi önemli bir sorun olarak görülmektedir. Ateş duvarı konuşma biter bitmez konuşmanın olduğu UDP portunu kapatabilmelidir.

Bir çok saldırı IPT protokollerindeki açıkları kullanmaktadır.



Tablo 12 IPT protokolleri ve açıklar

Bu diyagramda görüldüğü gibi; arama sinyalleşmesi (SIP), ses mesajının iletilmesi (RTP), ve kontrol protokolü (RTCP) elverişli bir kullanıcı tanımlama, uçtan uca bütünlülük ve gizlilik sağlayamamaktadır. Bunları sağlayamadığımız sürece saldırganlar birçok açık bularak sistemlere müdahale etmeye devam edeceklerdir.

4.1.1. Kullanıcıya Yönelik Saldırı Türleri

Eavesdropping (başkalarının gizli konuşmalarını gizlice dinleme), SIP sunucu ile SIP telefon arasındaki arama sinyalleşmesi esnasında saldırgan kullanıcının IPT kullanıcı adını, PIN numarasını ve SIP telefon numarasını çalabilir. Bunu başarabilen bir saldırgan, her türlü kullanıcı bilgisini değiştirebilir. Mesela, bütün sesli mesajlarını silebilir, kullanıcının arama planını değiştirebilir, arama yönlendirme ayarlarını değiştirebilir veya en önemlisi konuşmayı tamamen kaydedip daha sonra dinleyebilir ve önemli bilgilere ulaşabilir. Veya kullanıcının bilgilerini kendisine özel kullanarak bedava konuşma yapabilir.

IPT aramalarındaki bütünlülük, eğer mesaj veya paketlerde kimlik tanımlaması kullanılmaz ise sağlanamayabilir. Örneğin, saldırgan kendini arayan ve aranan arasına yerleştirerek (man-in-the-middle) gelen RTP paketlerini yollamayıp yerine kendi hazırladığı ses

paketlerini yollayabilir. Özellikle kablosuz ağlarda buna araya kelimeler eklemek, gürültü yaratmak ve geciktirmek gibi saldırılarda eklenebilir.

DoS saldırısı yine SIP sinyalleşme protokolüne uygulanabilmektedir. TCP'deki gibi kontrol paketleri (SYN, RST) bazlı bir saldırıdır. Saldırgan SIP sunucuya arama talebi veya kimlik tanımla paketleri yollayarak SIP sunucunun kaynaklarını tüketmek ve aktif aramaları düşürmek veya yeni aramalara meşgul cevabı aldırmak gibi sonuçlara kadar götürebilmektedir.

RTP flooding, UDP flooding gibidir. RTP dijital ses taşıyan ses paketleridir. Çok büyük RTP paketleri yollayarak IPT cihazlarını bombardımana tutabilmektedirler.

IPT uygulamaları aynı zamanda TCP, UDP ve ICMP DoS saldırılarına da açıktır. Saldırgan kontrol paketlerini kullanarak kullanıcıların PIN numaralarını değiştirebilir ve hesabı kullanılmaz hale getirebilirler.
Bunlar SIP tabanlı telefonlaşmada bazı saldırı türleridir. Bunlar direkt kullanıcıya yönelik olup bazı noktalarda bu servisi veren taşıyıcıyı da kapsamaktadır.

4.1.2. Taşıyıcıya Yönelik Saldırı Türleri

IP yanında güvenlik avantajları getirdiği gibi aynı zamanda dezavantajları da bulunmaktadır. IP ağlarında olduğu gibi, VoIP'de de güvenlik IP ağlarındaki servislerde olduğu kadardır. Örneğin e-mail, web ne kadar güvenli ise VoIP de o kadar güvenlidir. Bu kritik servis saldırılara açıktır ve güvenlik açıkları içermektedir.

Mesela, ses servisi solucan, virüs ve DoS saldırılarına açıktır ama eski tip anahtarlamalı sistemlerde (circuit-switched) bu tehlike söz konusu değildir. Ek olarak IP sistemlerine saldırabilecek birey sayısı çok fazla iken anahtarlamalı sistemlerde bu sayı düşüktür.

VoIP servisi paylaşımlı bir IP ağı üzerindedir. Örneğin LAN kullanıcıları tarafından erişilebilir veya internet üzerinden bu kullanıcılar kullanılarak direkt veya endirekt olarak erişilebilir. VLAN ve benzeri korumalar bu ağları ayırmaya yarayabilir ama tam bir güvenlik çözümü getirmemektedir.

VoIP, geleneksel anahtarlamalı sistemlere göre daha fazla cihaz ve uygulama gerektirmektedir. IP PBX, destek sunucuları, medya sunucuları, anahtarlar, yönlendiriciler, ateş duvarları, kablolama, IP telefonlar ve yazılım telefonlar gibi. Daha fazla cihaz ve uygulama kullanılması daha fazla güvenlik açığı getirmektedir. Kullanılan bu cihaz ve uygulamalar genelde özel amaçlı işletim sistemleri yerine genel amaçlı işletim sistemlerinde çalışmaktadır. Bu gereklilikte ayrıca güvenlik açıklarını yanında getirmektedir.

Uygulamadaki açıklar programlama hatalarıdır. Örneğin, protokol isteklerinin tam olarak kontrol edilmemesi, nasıl, ne zaman saldırılacağı, aşağıdaki konuları yanında getirebilmektedir.

•**Remote Access(Uzaktan Erişim):** Saldırgan sistem sorumlusunun hesabı ile sisteme giriş yapabilmektedir.

•**Kötü biçimlendirilmiş paket ile DoS:** Bu sayede sistem ya tamamen etkisiz hale gelebilmektedir yada yapması gereken bazı şeyleri yapamayacak hale gelmektedir.

•**Yük tabanlı Dos:** Flood olarak bilinmektedir. Zayıf dizayn edilmiş sistemlerde görülmektedir. IP PBX sistemleri genelde saldırganların hedefi olarak görülmektedir.

•**İşletim sistemi saldırıları:** İşletim sisteminin sahip olduğu açıkların kullanılmasıdır. Direkt olarak VoIP sistemine yönelik olmasa da etkileri içine alacaktır.

•**Destek yazılımı saldırısı:** Veritabanı veya web sunuculara yönelik saldırılardır.

•**Protokol saldırıları:** Protokollerin uygulanış biçimi ile alakalı açıklardır. SIP ve H.323 gibi. Örneğin, Microsoft ISA sunucudaki H.323 açığı gibi.

•**Uygulama saldırıları:** Ses uygulamalarının sahip oldukları açıklar olarak adlandırılabilir. Protokolün uygulanışı esnasında filtrelenmemesi sonucunda ortaya çıkmaktadır.

•**Uygulama manipülasyonu:** Zayıf konfigürasyon veya kimlik tanımlamasından kaynaklanmaktadır.

• **DoS:** Uygulama açıkları sonucunda yetenek kaybı veya flood olarak görülmektedir. Örneğin SIP protokolüne karşı DoS atağının yapılması gibi.

Aynı tipte saldırılar ve açıklar VoIP'deki diğer bileşenler için de geçerlidir. Sinyalleşmedeki DoS saldırısı ise en popüler olanıdır. Aygıtlara DoS saldırısı yapmak çok etkili bir yöntemdir. DoS saldırısına maruz kalan VoIP aygıtı, paketleri proses etmede oldukça güçlük çekecek ve VoIP gibi gecikmeye son derece hassas bir serviste oldukça güç problemler ortaya çıkaracaktır. VoIP aygıtı normalde RTP ile ses paketlerini taşımaktadır. Saldırgan çok yüksek sayıda RTP ve QoS paketleri yollayarak normal RTP paketlerinin de sekteye uğramasına ve Delay veya Jitter oluşmasına sebebiyet verecektir.

Kullanıcılar e-mail ve mesajlaşmada olduğu gibi değil, telefon konuşmalarında gizliliğin tam olduğu beklentisi içinde olacaktır. Bazı VoIP konuşmaları şifrelenmiş olsa da birçoğu şifresiz olarak gerçekleşmektedir. Eğer saldırgan şifresiz meydaya ulaşmayı başarırsa VOMIT tarzı uygulamalar ile konuşmaları dinleyebilmektedir.

4.2. Güvenlik Tehditlerine Karşı Alınabilecek Tedbirler

•Form veya kullanıcı tabanlı IDS'ler kullanarak saldırıları tespit etmek

• Ses uygulamaları için özel olarak optimize edilmiş ateş duvarları kullanarak IP PBX'leri LAN ve Internet kullanıcılarından uzak tutmak

•VLAN kullanmak

•Tüm ağ bileşenlerini güvenli hale getirmek

•Sadece kampüs tipi dizayn edilmiş VoIP ağlarında dışarıdan içeriye ve içeriden dışarıya bu trafiği tamamen kapatmak yada gerektiği gibi kısıtlamak.

•DoS saldırılarına karşı WAN üzerinden gelen arama sayısını sistemin desteklediği rakama göre sınırlamak

•Ağı monitör edebilecek yazılımlar kullanmak

VoIP için optimize edilmiş ateş duvarı ve güvenlik çıkışı (security gateway) kullanmak oldukça önemli olup aşağıdaki özellikleri de yanında getirmelidir:

•Uygulama katmanı seviyesinde monitör edebilme ile sinyalleşmeye karşı gerçekleşebilecek saldırılara karşı korunma desteği

•Protokol tabanlı NAT ve medya oturumu monitör edebilme desteği

•QoS için işaretleme

•Circuit-switched ateş duvarları ile birlikte çalışabilmek ve VoIP entegrasyonu sırasında çoklu (hybrid) güvenlik desteği

IP telefonları ve yazılım tabanlı IP telefonları güvenlik altına almayı da unutmamak gerekir. Telefonlar VoIP ağının en çok kullanılan arabirimleri olup, saldırganlar tarafından en kolay geçilen birimdir. Telefonları güvenli yapabilmek için:

• Medya ve sinyalleşme için güçlü kimlik tanımlaması, şifreleme ve güvenlik sağlayan telefonlar satın alınmalı

• Sistem sorumlusunun şifresi güçlü olmalıdır

• Uzaktan erişimi kapatabilmeli

• Web tabanlı ise güçlü bir şifre kullanılmalı

• Telefonun üretici güncelleme servisini güvenli şekilde yapmak

• Lokal yönetimi etkisiz hale getirmek

• Eğer mümkün ise Log yapmasını sağlamak

5. VOIP SÖZLÜĞÜ

AHT:(Average Hold Time): Ortalama bekleme süresi arayanın numarayı çevirdikten sonra, karşının açma veya kapama anına kadar geçen süredir.

ANI:(Automatic Number Identification): Telefonun arayan numarayı aranan tarafa iletmesi.

ASP(Application Service Provider)**:** Uygulama Desteği Servisi Yazılım tabanlı uygulamalarda 3.kuşak destek tipi. Uygulama WAN üzerinden kullanılarak belli kriterlere göre ödeme yapılmaktadır.

ASR(Answer-Seizure Ratio): Normal Gerçekleşen Arama-Toplam Arama Oranı Başarı ile gerçekleşen arama sayısının toplam arama girişimi sayısına oranıdır.

A-Z Rate – A'dan Z'ye Ücretler Bir operatörün elindeki, servis verebileceği tüm hedef noktaların (ülke, şehir veya özel bir nokta) ücret tarifesi.

Billing Increment: Faturalama kriteri Toplam arama süresini faturalandırırken, ilk arama ve kontur atış değerleri, sn olarak.

Buyer: Satın alan Telefon sonlandırma hizmetini satın alan şahıs yada şirket.

Buyer Tariff: Satın Alma Tarifesi Satın alınana sonlandırma hizmetinin lokasyonlara gore fiyatlandırması. Genelde AtoZ rate diye geçer. A dan Z ye verilebilen sonlandırma hizmetinin fiyatlarını içerir.

Call: Arama 2 uç nokta arasında gerçekleşmiş yada gerçekleşmesi için girişimde bulunulmuş ses bağlantısı.

Call deflection: Çağrı Yönlendirme H450.3 olarak tanımlanan, bir uç noktadaki cevaplanmayan bir H323 aramasının başka bir H323 uç noktasına aktarılması.

Call Detail Record (CDR): Arama Detayı Tek, tek bütün aramaların detaylarını içeren, otomatik olarak yaratılmış, zaman dilimlerine göre sıralanan, indirilebilen rapor dosyası.

Codec - Compression-decompression: Sıkıştırma Arama esnasında ses paketlerinin sıkıştırılması için kullanılan protocol.

Congestion: Tıkanıklık Gerçekleşmek isteyen trafiğin sahip olunan bant genişliğini aşması sonucu ortaya çıkan sıkışma.

Contract: Kontrat Arama sonlandırması satın almak veya satmak için 2 veya daha fazla taşıyıcı (Carrier) arasında yapılan anlaşma. Kontrat, önerilen dakika fiyatı (Tarif), ödeme periyodu, istenen veya taahhüt edilen dakika miktarı, arama faturalama kriteri, en az bir tane kayıtlı gateway veya gatekeeper gibi bilgileri içerir**.**

Deposit: Depozit Taşıyıcılardan satın alanın satana yaptığı bir ön ödemedir. Bu ödeme kredi olarak kullanılır.

Dial-peer Adreslenebilir arama uç noktası. Aranan taraf. Aranan uç noktanın gitmesi gereken adresi ve hangi aygıtın hangi ses portunda gideceğini söyleyen tanım.

Dial-peer hunting Aranan uç noktanın meşgul olması, yanlış numara hatası alma veya dial-peer tanımlanmamış numara aranması gibi durumlada aranabilecek diğer numara.

DiffServ (Differentiated Services): Ayrıcalık Tanıma Servisi Eğer ban genişliğini zorlayan başka bir protocol var ise ses paketlerine öncelik tanıyarak sesin kalitesini arttıran servis.

DNIS (Dialed Number Identification Service): Arayan Numara Tanımlama Servisi Arayan numaranın cevaplayan karşı tarafa yollanması özelliği.

DTMF (Dual-Tone Multifrequency) Telefonun tuşlarına bastıkça üretilen ses sinyali çeşitleri.

E&M (Ear and Mouth) Analog PBX bağlantısını karşılayan portlara verilen ad.

E.164 Uluslar arası telekomünikasyon sayısal planı. E164 numarası, eşsiz olup, genel ağ sonlandırma noktasını temsil eder. 3 alan içerir. CC (Country Code) Ükle Kodu, NDC (National Destination Code) Ulusal Hedef Kodu ve SN (Subscriber Number) Kullanıcı Numarası. En fazla 15 dijit olabilir.

E1 Geniş Ağ dijital transmisyon şeması. Avrupa için : 2,048 Mbits/s; 31 kanal, her biri 64 Kbps. **EndPoint:** Uç Nokta Bütün arama topolojisi göz önüne alınırsa, aramanın başladığı veya aramanın karşılandığı noktalar uç noktalardır. Aramanın gerçekleşmesi için arada rol gateway ve gatekeeper lar ise her biri karşılıklı kendi içinde uç nokta olarak anılabilir.

Failed Call: Gerçekleşemeyen Arama Arama gerçekleşti mesajını alamayan her arama denemesi, gerçekleşemeyen aramadır. Genelde ücretlendirilmez. Ama faturalandırma tarifelerine göre bir kısmı ücretlendirilmiş olabilir.

FXO (Foreign Exchange Office) Analog PBX bağlantısını karşılayan ses aygıtı. Dial-Tone vermez. Santralin dahili tarafına bağlanan tek kanal analog ses portudur.

FXS (Foreign Exchange Station) Telefon, Fax gibi cihazların direk takılabildiği ses aygıtı. Santralin harici (PSTN) tarafına bağlanır ve Dial-Tone verir.

G.711 64 kbps, yüksek kalite, düşük işlemci yükü.

G.723.1 6.4/5.3 kbps, orta kalite, yüksek işlemci yükü.

G.726 16/24/32/40 kbps, iyi kalite, düşük işlemci yükü.

G.728 16 kbps, orta kalite, çok yüksek işlemci yükü.

G.729 8 kbps, orta kalite, yüksek işlemci yükü.

G.7xx Ses sıkıştırmada ITU standartları.

Gatekeeper IP ağlarında ses, fax ve multimedia uygulamalar için yönetim görevi gören merkezi kontrol aygıtı. Gatekeeperlar çalışmakta olduğun ağın bilgi kaynağıdır. Adres çözümleme, kimlik tanımlama ve yetkilendirme, CDR kaydı ve ağ yönetim sistemleri ile iletişim sağlar. Gatekeeper lar bant genişliğini kotrol edebilme, eski sisteme ara bağlantı sağlamak, gerçek zamanlı ağ yönetimi ve yük dengeleme ile ağı izleme yeteneklerine de sahip olabilir.

Gateway

IP telefon sisteminde, ses ve fax aramalarını, gerçek zamanlı olarak PSTN (Public Switched Telephone Network) ve IP ağı arasında çevirmeye yarar. Ses ve fax sıkıştırma ve açma, paketleme, arama yönlendirme ve control sinyalleşmesi başlıca görevleridir. Ek olarak, dışarıdan bağlantı için arabirim sağlar, mesela Gatekeeper veya softswitch, faturalandırma sistemi ve ağ yönetim sistemleri. **Grace Period:** Müsade Süresi Aramanın başladığı zaman aralığı. Sn olarak anılır.

H.225 RAS, RTP/RTCP, Q.931 arama sinyalleşmesi protokolleri ve H323 mesaj formatı için kullanılır.

H.245 Karşılıklı uygunluk iletişimini, medya akışı için açık ve kapalı kanalların mesajlarını ve benzeri iletişimi sağlayan protokoldur. (örneğin; medya sinyalleşmesi)

H.323 Paket tabanlı, çoklu media iletişim sistemlerini tanımlayan ITU-T 'Şemsiye' standardıdır. Bu standart değişik çoklu media uç noktalarını bir nevi çoklu media sistemine (uç noktalar, Gateway ler, MCU(Multipoint Conferencing Units – Çok noktalı konferans cihazı) ve Gatekeeper lar) çevirmeye ve iletişim kurmalarına yarar. BU standart birçok IP üzerinden ses taşıyan uygulamada kullanılır. Ve diğer standartlara (H.225, H.245) göre özellikle gereklidir.

Hairpin Teekom terimidir. Anlamı; Aramanın geldiği yol üzerinden geri arama yollamaktır. Örneğin; eğer arama, aramanın başladığı en yakın gateway'e IP üzerinden taşınamıyor ise geldiği yoldan local gateway'e aynen geri yollanır.

Hop off Genellikle gateway'lerde görülen H.323 ile arama yapmak isterken karşıda H.323 olmayan bir karşılama söz konusu olmasıdır. Lokalde hopoff olmuş demek haippin olmuş demektir. Örneğin; Aranılan numara için verilen tanımlamalar dial-peer tanımlarında yok ise gatekeeper en yakın local gateway'e aramayı geldiği yoldan yollar.

IP Centrex Arama bekletme, arama transfer etme, aranan son numara, tekrar arama, arama yönlendirme, 3 yollu arama gibi servisleri sunar. Fakat sadece paket tabanlı ağlarda olabilir.

IP Telephony – IP üzerinden telefonculuk Ses ve fax aramalarının veri ağları üzerinden IP (Internet Protokolü) ile aktarılmasıdır. IP telephony, devre-anahtarlama (circuit-switched) telefon ağlarının, paket tabanlı telefon ağlarına dönüşümünün bir sonucudur. Ve ses sıkıştırma teknikleri, esnek ve sofistike transmisyon teknikleri, zengin servis kullanımı gibi getirileri olmuştur.

ITSP Internet Telephony Service Provider. IP üzerinden telefonculuk hizmeti veren şirket.

ITU-T Telekomunikasyon sektörü için ITU standartları.

Jitter Butun paketlerin iletilmesinde yaşanan toplam gecikme miktarı.

Latency - Gecikme Paketin kaynaktan hedefe ulaşıncaya kadar harcadığı zaman. Gecikme ve bant genişliği, hız ve ağın kapasitesini tanımlar.

Media Gateway – Medya Geçidi Ses gibi medyaların başladığı ve bittiği noktalarda kullanılan cihazlar. Bu iletişim esnasında geçilen her Gateway ve Gatekeeper'larda aslında karşılıklı olarak birer Media Gateway'dir.

MGCP (Media Gateway Control Protocol) – Media Gateway Kontrol Protokolü H.323 ve SIP protokollerinin tamamlayan protokol. Gateway gibi control elemanlarının Media Gateway'leri control etmesi için dizayn edilmiştir. Gateway Location Protocol (GLP – Gateway Lokasyon Protokolü) ile birlikte çalışır. PSTN tarafından gelen aramayı, gerekli noktaya ulaşması için ara iletişim kanalını açar. MGCP, yeni paket üzerinden ses taşıma standartları getirerek sistemi kolaylaştırmış, complex ihtiyaçları elimine etmiş, kaynak kullanımını azaltmış ve uçlardaki terminallerin fiyatlarını azaltmıştır. **Minimum Duration** – En az süre Aramanın, ne kadar kısa sürerse sürsün yuvarlanacağı arama süresi. Örneğin hizmet aldığınız operator 30 sn ile belirlemişse bu süreyi, siz 20 sn de görüşmüş olsanız 30 sn olarak ücretlendirilir. Genellikle bu süre 30 veya 60 sn dir. (Editör Notu : Eğer kötü niyetli değillerse tabii. Şahsen bunu 120 hatta 240 sn olarak ücretlendirenlerini bile gördüm. Düşünsenize, telefon ettiniz arkadaşınıza ve 'geciktim ama yoldayım' dediniz ve kapattınız. Mesaj yazacak durum da yok. Gitti 10 sn için 4 dakika.)

PBX (Private Branch eXchange) Ev veya ofis içinde telefonların haberleşmesini sağlayan şebeke. Aynı tüm bunları birleştiren genel şebeke gibi.

PRI (Primary Rate Interface) 30 B kanalı 1 D kanalı olan ISDN servisi. PRI 30 adet ses kanalı içeren dijital ses arayüzüdür.

PSTN (Public Switched Telephone Network): Genel Anahtarlamalı Telefon Ağı Telefon aramalarını bakır teller üzerinden bir uçtan diğer uca kadar taşıyan şebeke.

Q.931 ISDN bağlantı control protokolü. Akış kontrolü ve tekrar yollama desteği yoktur. Bağlantının kurulması ve sonlandırılması ile sorumludur. H.323 senaryosunda; bu protocol TCP'de paketlenir ve 1720 numaralı TCP portuna yollanır.

QSIG Q sinyalleşmesi. SİnyalleşmeStandardı. ISDN Q.931 standardına dayanan, bilinen kanal sinyalleşmesi. Birçok PBX'de kullanılır.

RAS (Registration, Admission, Status): Kayıt, Girme izni, Durum Terminaller ve Gateway'ler arası yönetim protokolü.

RSVP (Resource Reservation Protocol): Kaynak Rezervasyon Protokolü BU protocol IP ağlarında kaynak rezervasyonu yapar. IP üzerinde çalışan uygulamalar bağlanılan uç noktadaki transfer edilmek istenen paket akışı doğasını (bant genişliği, trafiğin çıkabileceği en uç nokta, jitter ve benzeri) görmek için RSVP protokolü kullanabilirler. RSVP IPv6 ya bağımlıdır.

RTP (Real-Time Transport Protocol): Gerçek Zamanlı Transport Protokolü Genellikle IP ağlarında kullanılır. RTP uçtan uça ağda, uygulamaların gerçek zamanlı veri transferi

yapabilmeleri için tasarlanmıştır. Örneğin; ses, görüntü veya simülasyon verisi. Multicast veya Unicast olabilir.

SS7 (Signalling System 7): Sinyalleşme Sistemi 7 PSTN'de SS7, aramanın başlatıldığı bölgeden başka bir hakim bölgeye doğru giden aramaların başlatılması ve yönetilmesi için kullanılır. Buradan da anlaşılacağı gibi, SS7 ancak operatörler arasında kullanılır. Bu protokol aslında IP tabanlı ağlarda BGP protokolüne benzetilebilir. SS7 :

• Aramanın başlatılması, kurulması ve yönetilmesini
• Arama bittiği zaman sonlandırılmasını
• Ücretlendirilmesini
• Arama yönlendirme,
• Arayan numaranın gösterilmesi
• 800 ve 900'lü numara,
• Kullanıcı tanımlama, kişisel dolaşım

Gibi servisleride destekler.

SIP (Session Initiation Protocol): Oturum Başlatma Protokolü Uygulama katmanı protokolüdür. Internet Telefonculuğunda sinyalleşme için kullanılır. SIP, ses/görüntü konferansı veya etkileşimli oyunlar için oturum açar. IP ağlarında arama aktarma özelliği getirerek, IP telefonculuk yapan servis sağlayıcıların web, elektronik posta veya chat servisleri ile bu özelliği birleştirmesini sağlar. Ek olarak, kullanıcı tanımlama, yönlendirme ve kayıt olma servisleri sağlar. SIP geleneksel telefonculuk özelliklerini de desteklemektedir, örneğin; kişisel dolaşım, günün saatine göre arama yönlendirme, coğrafi duruma göre arama yönlendirme.

Softswitch (Proxy çalışan Gatekeeper, Arama Sunucusu, Arama Ajanı, Media Gateway denetleyicisi, veya Anahtar Denetleyici olarak da bilinir) PSTN ile IP Telefon arasında köprü görevi görür. Media Gateway'den gelen telefon aramasının control edilmesi işini görür. Protokol dönüştürme, kimlik tanımlama, yetkilendirme ve yönetim görevleride vardır.

Trunk İki nokta arasında iletişim kanalı. Tipik olarak, birçok aramayı kaldırabilecek anahtarlama merkezleri ile veri sinyalleşmesi arasındaki yüksek bant genişliklerine sahip telefon kanalları olarak adlandırılır.

VoIP (Voice over IP): IP üzerinden Ses Normal telefon sistemindeki sesi IP tabanlı Internet üzerinden aynı ses kalitesinde, güveninirliliğinde ve özelleiklerinde taşımaktır. Telefon ve fax konuşmalarının router (yönlendirici) üzerinden taşınmasıdır. VoIP'de, DSP (Digital Signal Processing – Dijital sinyal prosesi) segmantleri ile ses sinyali frame'lere çevrilir ve belli bir gurup oluşturduklarında ses paketlerine çevrilir. Bu paketler ITU-T'nin tanımladığı H.323 protokolü ile IP üzerinden transfer edilir.

VoIP Termination Service – VoIP Sonlandırma Servisi IP üzerinden taşınan ses trafiğinin sonlandırılabilmesi servisidir. Örneğin; bu hizmeti veren bir operötörün belli noktalarda VoIP'i PSTN yani lokal servise sunmasıdır. Yani, her eve giden bakır tellerin oluşturduğu PSTN şebekesi ile IP tabanlı system arasında geçiş sağlamaktır.

VoIP Origination Service – VoIP Başlatma Servisi Sonlandırma servisinin tam tersidir. Yani ses trafiğinin PSTN şebekeden alınıp IP tabanlı sisteme yollanmasıdır.