

**İNTERNET PROTOKOLÜ (IP)  
ÜZERİNDEN SES HABERLEŞMESİNDE  
SERVİS KALİTESİNE ETKİ EDEN  
PARAMETRELERİN ANALİZİ**

**Esin YAVUZ**

**Yüksek Lisans Tezi  
ELEKTRONİK VE HABERLEŞME  
MÜHENDİSLİĞİ ANABİLİM DALI**

**ISPARTA 2004**

**T.C.  
SÜLEYMAN DEMİREL ÜNİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ**

**İNTERNET PROTOKOLÜ (IP) ÜZERİNDEN  
SES HABERLEŞMESİNDE SERVİS KALİTESİNE ETKİ EDEN  
PARAMETRELERİN ANALİZİ**

**ESİN YAVUZ**

**YÜKSEK LİSANS TEZİ**

**ELEKTRONİK VE HABERLEŞME MÜHENDİSLİĞİ ANABİLİM DALI**

**ISPARTA – 2004**

## İÇİNDEKİLER

	Sayfa
İÇİNDEKİLER .....	i
ÖZET .....	iv
ABSTRACT .....	v
ÖNSÖZ .....	vi
ŞEKİLLER DİZİNİ .....	vii
ÇİZELGELER DİZİNİ .....	ix
1. GİRİŞ.....	1
2. İNTERNET .....	4
2.1. TCP – İletim Denetim Protokolü (Transmission Control Protocol) .....	7
2.2. UDP – Kullanıcı Datagram Protokolü (User Datagram Protocol) .....	8
2.3. IP – İnternet Protokolü .....	9
2.4. Fiziksel Katman .....	11
3. VoIP MİMARİLERİ .....	12
3.1 H.323 Mimarisi .....	13
3.1.1 H.32x Ailesi .....	13
3.1.2 H.323 .....	14
3.1.3 H.323 Bileşenleri .....	16
3.1.3.1 Geçit Denetim Sistemi (Gatekeeper) .....	16
3.1.3.2 Ağgeçidi (Gateway) .....	17
3.1.3.3 Çok Noktalı Kontrol Birimi (MCU – Multi-point Control Unit) .....	17
3.1.3.4 Terminaller .....	18
3.1.4 H.323'ün Yararları .....	18
3.2 SIP (Session Initiation Protocol – Oturum Başlatma Protokolü) .....	20
3.2.1 SIP Bileşenleri .....	20
3.2.2 SIP'in Sağladığı Hizmetler .....	21
4. H.323 PROTOKOLLERİ .....	22
4.1. Kodlama Teknikleri .....	22
4.1.1. Kodlama Standartları .....	23
4.1.2. Temel Sıkıştırma Tipleri .....	24
4.1.2.1. G.723.1 .....	24
4.2. Video Standardı .....	25

4.3. H.225 Kayıt, Kabul ve Durum Protokolü (Registration, Admission and Status - RAS) .....	25
4.4. H.225 Çağırma İşaretleşme Protokolü .....	26
4.5. H.245 Kontrol İşaretleşme Protokolü .....	27
4.6. T.12x Veri Haberleşme Protokolleri .....	27
4.7. H.235 Güvenlik Protokolü .....	28
4.8. Gerçek-Zamanlı Taşıma Protokolü (Real-Time Transport Protocol-RTP)...	28
4.9. Gerçek-Zaman Kontrol Protokolü (RTP Control Protocol-RTCP) .....	29
4.10. RTSP (Real-Time Streaming Protocol) .....	29
5. İNTERNET ÜZERİNDEN SESİN (VoIP) KALİTESİ .....	30
5.1. Servis Kalitesinin Önemi .....	31
5.2. Sistem ve QoS Kontrol .....	32
5.3. Servis Kalitesi Uygulamaları .....	32
5.3.1. Etkileşimli uygulamalar .....	33
5.3.2. Duyarlı uygulamalar .....	33
5.3.3. Zamanlı uygulamalar .....	34
6. SERVİS KALİTESİNE ETKİ EDEN PARAMETRELER VE ANALİZLERİ .....	35
6.1. Bandgenişliği .....	35
6.2. Gecikmeler .....	35
6.2.1. Paket Gecikmesi .....	35
6.2.2. İşlem Gecikmesi .....	37
6.2.3. Network Gecikmesi .....	37
6.3. Gecikme Değişiklikleri (Jitter) .....	38
6.4. Network Sıkışması .....	39
6.4.1. Eko (Echo) .....	39
6.4.2. Konuşmaların Üst Üste Binmesi (Talker Overlap) .....	40
6.4.3. TCP Sıkışma Kontrolü .....	40
6.5. Kayıplar .....	41
6.5.1. Kayıp Paket Telafisi .....	41
6.6. İletim Öncelikleri .....	42
6.6.1. IP Önceliği .....	42

6.6.2. Öncelik Sıralaması – Tamponlama .....	42
6.7. Atılım Öncelikleri .....	43
6.8. Konuşma Kalitesinin Ölçümü .....	44
6.9. Rastgele Erken Sezme (Random Early Detection - RED) .....	45
6.9.1. Ağırlıklı Öncelik (Weighted Precedence) .....	46
6.9.1.1 Ağırlıklı RED (Weighted RED – WRED) .....	46
6.9.1.2. Ağırlıklı Adil Kuyruklama (Weighted Fair Queuing – WFQ) .....	46
6.10. Rezervasyon Protokolü (Reservation Protocol - RSVP) .....	46
6.10.1. RSVP Çalışması .....	47
6.10.2. RSVP Sınırlamaları .....	48
6.11. Çoklu Protokol Etiket Anahtarlama (Multiprotocol Label Switching – MPLS) .....	49
6.11.1. MPLS Çalışması .....	49
7. IP ÜZERİNDEN SES HABERLEŞMESİNDE SERVİS KALİTESİNE ETKİ EDEN PARAMETRELERİN ANALİZİ İÇİN KULLANILAN TEKNİKLER VE TEST SONUÇLARI .....	51
7.1. Kullanılan Test Programı .....	51
7.1.1. NetMRG .....	51
7.1.2. Programın Kullanıldığı Platform .....	53
7.1.3. Yardımcı Programlar .....	53
7.1.3.1. RRDtools (Round Robin Database) .....	53
7.1.3.2. SNMP – Simple Network Management Protocol (Basit Ağ Yönetim Protokolü) .....	54
7.1.4. NetMRG İle Grafiklenen Değerler .....	55
7.2. Uzak Noktadaki Test Sonuçları .....	56
7.3. Yakın Noktadaki Birinci Uygulamanın Test Sonuçları .....	58
7.4. Yakın Noktadaki İkinci Uygulamanın Test Sonuçları .....	60
7.5. Test Sonuç Değerlendirmesi .....	64
8. SONUÇ .....	65
9. KAYNAKLAR .....	69
EK .....	71
ÖZGEÇMİŞ .....	78

## ÖZET

İnternet ve intranetin gelişerek yaygınlaşmasıyla birlikte, ses iletişiminin IP ağları üzerinden iletimi gündeme gelmiştir. IP üzerinden ses haberleşmesinin ekonomik olması, varolan sistemin üzerine kolay adapte edilebilmesi gibi sebepler bu sistemin gün geçtikçe yaygınlaşmasında önemli rol almaktadır.

Ses iletimi, gerçek zamanlı olması gereken bir iletimdir, ama heterojen yapıya sahip internette gerçek zamanlı bir uygulamaya ait paketlerin hepsinin doğru sırada gitmesi beklenemez. Bunun en basit sebebi, iletimin birden çok router üzerinden yapılması ve ayrı iki routerdan gelen paketin aynı sürede iletilmemesidir. Bu gecikme sorunlarının, bazı protokoller sayesinde aşılmasına çalışılmaktadır. İnternetin yapısından dolayı, geciken ve sırası değişen paketler, alıcı tarafında yeniden doğru şekilde sıralanır ve dijital sinyal elde edilir, ama asla gönderilen sinyallerin aynı olmaz. Bu noktada servis kalitesi (QoS) sorunu gündeme gelir.

Bu tezin amacı, İnternet Protokolü (IP) üzerinden ses haberleşmesinde sesin kaliteli ve kesintisiz bir şekilde iletilmesi için gerekli olan parametrelerin analizidir. Çalışmada, servis kalitesine etki eden bandgenişliği, gecikme, paket kayıpları, network hataları gibi parametreler incelenerek, analiz edilmiştir.

Bu tez çalışmasında, VoIP teknolojisi her yönü ile incelenmiştir. İkinci bölümde İnternet kavramı öncelikli olarak ele alınmış ve gerekli giriş bilgileri verilmiştir. Çalışmanın üçüncü bölümünde, VoIP teknolojisinde kullanılan mimariler incelenmiştir. Bu mimarilerden şimdilik en yaygın olarak kullanılanı H.323 mimarisidir. Bu sebeple, dördüncü bölümde H.323 mimarisinde kullanılan protokoller, standartlar ve kodlama teknikleri üzerinde ayrıntılı olarak durulmuştur. Beşinci ve altıncı bölümlerde, servis kalitesi ve buna etki eden parametrelerin analizine yer verilmiştir. Yedinci bölüm, analiz için kullanılan teknikleri ve test sonuçlarını içermektedir. Çalışmanın EK bölümünde, çalışmada kullanılan kısaltmaların ve terimlerin daha ayrıntılı anlatıldığı indeks yer almaktadır.

**ANAHTAR KELİMELEER:** IP üzerinden ses haberleşmesi (VoIP), Servis Kalitesi (QoS), İnternet Telefonu, H.323

## ABSTRACT

With the growing expansion of internet and intranet voice transmission over IP networks has been seriously considered lately. Such reasons as economical value and its adaptability to the present system have played an important role in the wide spread of this system.

Voice transmission must be a real-time transmission. It can not be expected for the packets of an application to be transmitted in the right order over internet which has a heterogeneous structure. This is because transmission can be conducted over a multiple router and the packets from two different routers can not be transmitted at the same period. The problems of delay are being tried to get over by some protocols. Considering the structure of internet, the packets delayed or disordered are put into correct order by the receiver and a digital signal is obtained, but these signals are never the same as they were before. At this point, the quality of service problem becomes significant.

The aim of this thesis is the analysis of parameters necessary for the quality and continuous transmission of the voice over Internet Protocol (IP). In this study, parameters such as bandwidth, delay, packet loss, network errors that effect quality of service are analyzed.

In this thesis, the Voice over IP technology was examined with all respects. In the second chapter, first the internet concepts were discussed and required introductory knowledge was presented. In the third chapter, the Voice over IP structure was analyzed. Of all the most commonly used structure is H.323 for the nonce. Therefore, in the fourth chapter, the protocols, standards and coding techniques used in H.323 structure were studied in detail. In fifth and sixth chapters, the quality of service and parameters were investigated. The seventh chapter includes the techniques and test results used for the analyses. In the appendix of the study, abbreviations and terms used were given at the index.

**KEY WORDS:** Voice over IP (VoIP), Quality of Service (QoS), Internet Telephony, H.323

## ÖNSÖZ

Bu çalışmanın gerçekleşmesindeki katkılarından dolayı Danışman Hocam Prof. Dr. Mustafa Merdan'a, çeşitli öneri ve fikirleriyle tez çalışmama yön vermemde yardımcı olan Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanı Ziya Öncü'ye, uygulama aşamasındaki desteklerinden dolayı Sertaç Selim Sarıca'ya ve desteklerini daima arkamda hissettiğim aileme teşekkürü bir borç bilirim.

Bu tez çalışmasında Süleyman Demirel Üniversitesi Enformatik Bölümü bünyesinde yer alan Akıllı Sınıf'ın sağladığı imkanlardan faydalanılmıştır.



## ŞEKİLLER DİZİNİ

	Sayfa
Şekil 1.1. Ses, veri ve video'nun aynı hat üzerinden iletimi .....	1
Şekil 2.1. TCP/IP katmanları .....	5
Şekil 2.2. TCP Segmenti .....	8
Şekil 2.3. IP Datagram .....	10
Şekil 2.4. Ethernet Paketi .....	11
Şekil 3.1. H.323 Bileşenleri .....	16
Şekil 4.1. H.323 protokoller topluluğu.....	22
Şekil 4.2. RAS Çalışması .....	26
Şekil 4.3. H.225 Çağırma İşaretleşme Protokolü .....	27
Şekil 4.4. H.245 Kontrol Protokolü .....	27
Şekil 6.1. Gecikme Kaynakları (1) .....	36
Şekil 6.2. Gecikme Kaynakları (2) .....	37
Şekil 6.3. Jitter .....	38
Şekil 6.4. VoIP konfigürasyonunda eko ve gecikme .....	39
Şekil 6.5. Öncelik Sıralaması .....	43
Şekil 6.6. Networkün giriş ve çıkışında bulunan LSR'ler (Etiket Anahtarlama Router'ları) .....	50
Şekil 7.1. Data Alınacak Cihaz/ların Seçildiği Menü .....	51
Şekil 7.2. Veri Alınacak Cihazın Interface'i .....	52
Şekil 7.3. Interface Üzerinden Alınan Tüm Değerler .....	52
Şekil 7.4. Alınan Değerin Saatlik, Haftalık ve Aylık Detaylı Gösterimi ....	53
Şekil 7.5. Bytes In Grafiği-1 .....	56
Şekil 7.6. Bytes Out Grafiği-1 .....	56
Şekil 7.7. Bytes In ve Bytes Out Grafiği-1 .....	57
Şekil 7.8. Errors In Grafiği-1 .....	57
Şekil 7.9. Errors Out Grafiği-1 .....	58
Şekil 7.10. Bytes In Grafiği-2 .....	58
Şekil 7.11. Bytes Out Grafiği-2 .....	58
Şekil 7.12. Bytes In ve Bytes Out Grafiği-2 .....	59

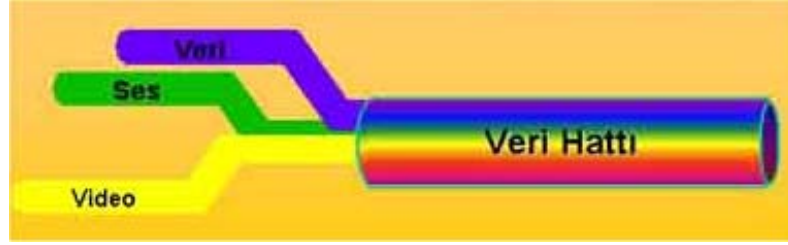
Şekil 7.13. Errors In Grafiği-2 .....	59
Şekil 7.14. Errors Out Grafiği-2 .....	59
Şekil 7.15. Akıllı Sınıf ve NetMRG Makinesinin Seçildiği Menü .....	60
Şekil 7.16. NetMRG Makinesinden alınan tüm değerler .....	60
Şekil 7.17. Bytes In Grafiği-3 .....	61
Şekil 7.18. Bytes Out Grafiği-3 .....	61
Şekil 7.19. Bytes In ve Bytes Out Grafiği-3 .....	61
Şekil 7.20. Errors In Grafiği-3 .....	62
Şekil 7.21. Errors In Grafiği-3 .....	62
Şekil 7.22. 1 dakikalık ortalama yük grafiği .....	63
Şekil 7.23. 5 dakikalık ortalama yük grafiği .....	63
Şekil 7.24. 15 dakikalık ortalama yük grafiği .....	63
Şekil 7.25. Ortalama Yük Grafiği .....	63

**ÇİZELGELER DİZİNİ**

	Sayfa
Çizelge 3.1. H.323 Protokol Yapısı .....	15
Çizelge 6.1. Kodlama/Sıkıştırma yöntemlerinin karşılaştırılması .....	45

## 1. GİRİŞ

Gelişen teknoloji ile birlikte networkler üzerinde kullanıcı sayılarının artması ve buna bağlı olarak uygulamalardaki çeşitlilik network trafiğinin ve kullanıcı isteklerinin artmasına neden olmuştur. Tümüleşik sistemler diye tabir edilen data, ses ve video'nun aynı hat üzerinden iletilmesini sağlayan yapılar kullanılmaya başlanmıştır. Dünyadaki tüm organizasyonlar, artan haberleşme maliyetlerini azaltmak istemektedirler. Mevcut durumda ayrı olan ses ve veri şebekelerinin birleştirilmesi, önemli tasarruf fırsatları sunmaktadır. Bu aşamanın ilk adımı olarak karşımıza VoIP (Voice over Internet Protocol) teknolojisi çıkmaktadır.



Şekil 1.1. Ses, veri ve video'nun aynı hat üzerinden iletimi

Bundan 20-30 yıl öncesine kadar, iletişim sadece PSTN (Public Switched Telephone Network/Kamusal Anahtarlamalı Telefon Ağı) hatlı telefonlarla yapılabiliyorken, veri iletimi özellikle uzun mesafeler için oldukça pahalıydı ve henüz kimse görüntülü iletişimi hayal bile edemiyordu. PSTN şebekeleri kullanıcılara, her çağrı için bir uçtan diğer uca bir devre bağlantısı sağlar. 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 yönlendirme ve çağrı sonlandırma işlemlerinden oluşmaktadır. PSTN hizmeti, yaklaşık yüz yıldan bu yana kullanılmaya devam etmektedir. Ancak buna paralel olarak veri trafiği için ayrı şebekeler oluşmuştur. Doğal olarak ayrı ses ve veri şebekeleri servis sağlayıcı için ilave yük aboneler için de ilave ücret anlamına gelmektedir. PSTN trafiği her geçen gün daha fazla veri

içerikli olamaya yüz tuttukça ses ve veri şebekelerinin birleşmesi yani tek bir platforma indirgenmesi ihtiyacı daha fazla belirgin hale gelmiştir.

Son yıllarda, internet ağının genişlemesi ve hızlanması, ses sıkıştırma ve işleme metotlarının gelişmesi, insanların PC'leri ve interneti kullanma oranının artışı gibi önemli gelişmeler, geleneksel ses iletimine alternatif olarak VoIP'in ortaya çıkışını ve yaygınlaşmasını sağlamıştır. İnternet Protokolü üzerinden ses (VoIP), telefon görüşmelerinin ve faksların IP tabanlı bir network üzerinden iletilmesine imkan veren teknolojidir. Aslında; analog bir sinyal olan sesin dijital bilgi haline getirilmesi ve bu bilgilerin internet üzerinden gönderilmesi, sistemin ana prensibidir. Dijital bir bilgi olarak ses, gideceği noktaya daha kolay iletilir.

1995'lerde modemlerin 14,4 kbps (kilo bit per second) hızına erişmesi, aynı anda 8 kbps'lik düşük hızlı codec'lerin (orjinalinde GSM-Global System for Mobile Communication haberleşmesi için geliştirilmiştir) kullanılabilir hale gelmesiyle IP ağları üzerinden ses transferi teknik olarak mümkün hale gelmiştir. 1995 yılında ilk küçük VoIP uygulaması (PC'den PC'ye) ortaya çıkmış, standartlaştırma çalışmaları da aynı yıl başlamıştır. 1996'da ilk VoIP standartları kabul edilmiş, düşük kapasiteli H.323 ağgeçitleri (gateway) gibi ilk öncü ürünler aynı yıl geliştirilmiştir. Ağgeçitlerinin ortaya çıkması ve kullanımı VoIP tarihinde anahtar bir rol oynamıştır. 1998'de bazı müteşebbislerin, ağgeçitlerini PC'den Telefona ve sonra da Telefondan Telefona bağlantı için konfigüre etmeleriyle VoIP belli bir güce ulaşmıştır. Daha sonra bazı müteşebbisler, nizami telefonları kullanarak müşterilerine ücretsiz görüşme olanağı sağlamaya başlamışlardır. Bu sistemle, uzun mesafe görüşmeleri ücretsiz sağlanabilmiştir.

Bugün VoIP için iki standart mevcuttur: H.323 ve SIP. Şu an çoğu anahtarlama ve yönlendirme ekipmanlarının (switchler ve routerlar) VoIP desteği bulunmaktadır. 2000 yılına gelindiğinde VoIP trafiği, tüm ses trafiğinin %3'ünü geçmiştir. 2005 yılında, VoIP trafiğinin tüm uluslararası ses için %25 ve %40 arasında hızla gelişmesi tahmin edilmektedir. (Intertangent Technology Directory, History of VOIP, 2004)

VoIP teknolojisindeki en önemli kriter, QoS olarak bilinen Servis Kalitesidir (Quality of Service). Servis Kalitesi, aynı hattı paylaşan verilerin sınıflandırılmasını ve bu şekilde kullanıcıya göre önem taşıyan verilerin öncelikli ve kayıpsız olarak iletilmesini sağlamak amacıyla kullanılan bir özelliktir. VoIP gerçekleştirilen bir network içerisinde sesi ileten cihazların (router) QoS desteğini sağlıyor olmaları gerekmektedir. Aksi takdirde hatlardan geçen dataların yoğunluk kazandığı esnada yapılan sesli görüşmeler, yeterli bandgenişliğine sahip olamayacakları için kesilebilmektedir. QoS ile ses dataları önceliklendirilip, sesin en iyi şekilde iletilmesi sağlanabilmektedir. Sesin, kesintisiz ve kaliteli iletimini etkileyen en önemli faktörlerden biri de gecikmedir. Kabul edilebilir değer, 200 ms'den az süren gecikmedir. Daha fazla olursa, kayıplar yaşanabilmektedir. Servis kalitesini etkileyen diğer bir etmen de jitter tabir edilen network üzerindeki trafiğin yoğunluğu sebebiyle oluşan kuyruklardır.

Bu tez çalışmasında, servis kalitesine etki eden tüm bu parametreler detaylı olarak analiz edilmiş ve konuyla ilgili uygulama çalışmaları yapılmıştır.

## 2. İNTERNET

İnternet'in temeli, 1960'lı yıllarda Amerika Birleşik Devletleri Savunma Bakanlığı'nın, askeri personel ve sivil arařtırmacıların savunma ile ilgili projelerde haberleřmelerini saęlamak amacıyla bilgisayar aęlarının kullanılması dūřuncesine dayanır. 1970'li yıllarda ARPANET adlı bir geniř alan aęı ortaya çıkmıřtır. ARPANET ile birlikte yerel alan aęlarının, geniř alan aęlarına baęlanması kavramı ortaya çıkmıř ve birbirine baęlı aęlararası iletiřim (internetwork) gündeme gelmiřtir. (Baykal, 2001)

Aę üzerinde iki bilgisayarın karřılıklı veri aktarabilmesi ve ortak sūreçler yūrūtebilmesi iin bilgisayarların birlikte alıřabilme yeteneęinin olması gerekir. Birlikte alıřabilme, verici ve alıcı arasında kullanılacak iřaretler, veri formatları ve verinin deęerlendirme yūntemleri üzerinde anlařmayla mūmkūn olur. Bunu saęlayan kurallar dizisi, protokol olarak adlandırılır. Protokol, aęın farklı paralarının birbiriyle nasıl etkileřimde ve iletiřimde bulunacaęını belirler. Standartlar ise, her ūreticinin uyduęu ortak tanımlamalardır.

Bir aę ierisinde aynı anda birden ok protokol kullanılıyor olabilir; ūnkū iřletim sistemleri, protokol kūmesi farklı olan birok bilgisayar, aynı anda aęda bulunabilir ve hepsinin birbirleriyle iletiřimde bulunması gerekebilir. Bu aęlar arasındaki uyumsuzluk sorununun giderilmesi amacıyla da TCP/IP (Transmission Control Protocol/Internet Protocol – İletim Kontrol Protokolū/İnternet Protokolū) geliřtirilmiřtir. TCP/IP, farklı topoloji ve protokollere sahip bilgisayar aęlarını birbirine baęlamak iin kullanılan bir protokoller dizisidir.

İnternet birbirine geiř yolları (gateway) ile baęlanmış ok sayıdaki baęımsız bilgisayar aęlarından oluřur. Kullanıcı bu aęlar üzerinde yer alan herhangi bir bilgisayara ulařmak isteyebilir. Bu iřlem esnasında kullanıcı farkına varmadan bilgiler, dūzinelerce aę ūzerinden geiř yapıp, varıř yerine ulařırlar. Bu kadar iřlem esnasında kullanıcının bilmesi gereken tek ūey ulařmak istedięi noktadaki bilgisayarın 'İnternet adresi'dir. Bu adres toplam 32 bit uzunluęunda bir sayıdır. Fakat bu sayı 8 bitlik 4 ayrı ondalık sayı ūeklinde kullanılır (193.140.181.18 gibi). Bu

8 bitlik gruplara ‘oktet’ ismi verilir. Bu adres yapısı genelde karşıdaki sistem hakkında bilgi de verir.

IP, bağlantısız (connectionless) ağ teknolojisini kullanmaktadır ve bilgi “datagramlar” (TCP/IP temel bilgi birim miktarı) dizisi halinde bir noktadan diğerine iletilir. Büyük bir bilgi grubunun (büyük bir dosya veya e-posta gibi) parçaları olan “datagram” ağ üzerinde tek başına yol alır. Mesela 15000 oktetlik bir bilgi pek çok ağ tarafından bir kerede iletilemeyecek kadar büyük olduğu için protokoller bunu 30 adet 500 oktetlik datagramlara böler. Her datagram ağ üzerinden tek tek yollar ve bunlar karşı tarafta yine 15000 oktetlik bir bilgi olarak birleştirilir. Doğal olarak önce yola çıkan bir datagram kendisinden sonra yola çıkan bir datagramdan sonra karşıya varabilir veya ağ üzerinde oluşan bir hatadan dolayı bazı datagramlar yolda kaybolabilir. Kaybolan veya yanlış sırada ulaşan datagramların sıralanması veya hatalı gelenlerin yeniden alınması hep üst seviye protokollerce yapılır.

TCP/IP katmanlardan oluşan bir protokoller kümesidir. Her katman değişik görevlere sahip olup altındaki ve üstündeki katmanlar ile gerekli bilgi alışverişini sağlamakla yükümlüdür. Aşağıdaki şekilde bu katmanlar görülmektedir.

			FTP			
Uygulama	SMTP	RLOGIN		TELNET	DOMAIN	TFTP
Taşıma	TCP				UDP	
Yönlendirme	IP			ICMP		
	IEEE 802.2 / LAPB/ HDLC					
Fiziksel	Ethernet, X.25, Token-Ring, Dial-up, vs.					

Şekil 2.1. TCP/IP katmanları

TCP/IP katmanlarının tam olarak ne olduğu, nasıl çalıştığı konusunda açıklama yapmak gerekirse;

TCP/IP’nin kullanıldığı en önemli servislerden birisi elektronik postadır (e-posta). E-posta servisi için SMTP (Simple Mail Transfer Protocol) protokolü belirlenmiştir. Bu



protokol e-postanın bir bilgisayardan bir başka bilgisayara nasıl iletileceğini belirler. Yani e-postayı gönderen ve alan kişinin adreslerinin belirlenmesi, mektup içeriğinin hazırlanması vs. gibi. Ancak e-posta servisi bu mektubun bilgisayarlar arasında nasıl iletileceği ile ilgilenmez, iki bilgisayar arasında bir iletişimin olduğunu varsayarak mektubun yollanması görevini TCP ve IP katmanlarına bırakır. TCP katmanı komutların karşı tarafa ulaştırılmasından sorumludur. Karşı tarafa ne yollandığı ve hatalı yollanan mesajların tekrar yollanmasının kayıtlarını tutarak gerekli kontrolleri yapar. Eğer gönderilecek mesaj bir kerede gönderilemeyecek kadar büyük ise (örneğin uzunca bir e-posta gönderiliyorsa) TCP onu uygun boydaki segmentlere (TCP katmanlarının iletişim için kullandıkları birim bilgi miktarı) böler ve bu segmentlerin karşı tarafa doğru sırada, hatasız olarak ulaşmalarını sağlar. İnternet üzerindeki tek servis e-posta olmadığı, segmentlerin karşı tarafa hatasız ulaştırılmasını sağlayan iletişim yöntemine tüm diğer servisler de ihtiyaç duyduğu için TCP ayrı bir katman olarak çalışmakta ve tüm diğer servisler onun üzerinde yer almaktadır. Üst seviye uygulama protokollerinin TCP katmanını çağırmaları gibi benzer şekilde TCP de IP katmanını çağırmaktadır. Ayrıca bazı servisler TCP katmanına ihtiyaç duymamakta ve bunlar direkt olarak IP katmanı ile görüşmektedirler. Böyle belirli görevler için belirli hazır yordamlar oluşturulması ve protokol seviyeleri inşa edilmesi stratejisine 'katmanlaşma' adı verilir. TCP ve IP ayrı katmanlardır ve her katman altındaki diğer katman ile konuşmakta diğer bir deyişle onu çağırmakta ya da onun sunduğu servisleri kullanmaktadır. En genel haliyle TCP/IP uygulamaları 4 ayrı katman kullanır. Bunlar:

- Uygulama Katmanı: Kullanıcıya en yakın olan katmandır. (e-posta, ftp, telnet gibi)
- Taşıma Katmanı: Üst seviye uygulama protokollerinin gereksinim duyduğu TCP gibi bir protokol katmanı.
- IP Katmanı: Gönderilen bilginin istenilen adrese yollanmasını sağlayan katman.
- Fiziksel Katman: Belirli bir fiziksel ortamı sağlayan protokol katmanı.

## 2.1. TCP – İletim Denetim Protokolü (Transmission Control Protocol)

TCP'nin temel işlevi; alıcı tarafa ne yollandığının kayıtlarını tutmak, üst katmandan (uygulama katmanı) gelen bilgiyi segmentler haline dönüştürmek, iletişim ortamında kaybolan bilgileri tekrar yollamak, ayrı sıralar halinde gelebilen bilginin doğru sırada ve hatasız olarak ulaşmasını sağlamaktır.

TCP, OSI başvuru modelinde tanımlanan “Taşıma Katmanı”nın işlevlerini yerine getirir. Bu katman, uçtan uca bağlantının sağlandığı ilk katmandır. TCP protokolü, iletiyi parçalara ayırdıktan sonra, her birinin başına bir başlık (header) ekler. Bu başlık, çeşitli alanlar içerir. Bu alanlar, kaynak portu, hedef portu, sıra numarası, alındı onayı (acknowledgement), veri çoğaltımı, veri için yer ayrılması, pencere (window) kontrol toplamı (checksum), acil işareti (urgent pointer) ve bilgidir.

Port numarası, birden fazla kişinin aynı anda dosya yollaması veya karşıdaki bilgisayara bağlanması durumunda TCP'nin herkese verdiği farklı bir numaradır. Üç kişi aynı anda dosya transferine başlamışsa TCP, 1000, 1001 ve 1002 “kaynak” port numaralarını bu üç kişiye verir böylece herkesin paketi birbirinden ayrılmış olur. Aynı zamanda hedef noktasındaki TCP de ayrıca bir “hedef” port numarası verir. Kaynak noktasındaki TCP'nin hedef port numarasını bilmesi gereklidir ve bunu iletişim kurulduğu anda TCP karşı taraftan öğrenir. Ayrıca her segment bir “sıra” numarasına sahiptir. Bu numara ile karşı taraf doğru sayıdaki segmenti eksiksiz alıp almadığını anlayabilir. Aslında TCP segmentleri değil oktetleri numaralar. Diyelim ki her datagram içinde 500 oktet bilgi varsa ilk datagram numarası 0, ikinci datagram numarası 500, üçüncüsü 1000 şeklinde verilir. Başlık içinde bulunan üçüncü önemli bilgi ise “kontrol toplamı” (Checksum) sayısıdır. Bu sayı segment içindeki tüm oktetler toplanarak hesaplanır ve sonuç, başlığın içine konur. Karşı noktadaki TCP kontrol toplamı hesabını tekrar yapar. Eğer bilgi yolda bozulmamışsa kaynak noktasındaki hesaplanan sayı ile varış noktasındaki hesaplanan sayı aynı çıkar. Aksi takdirde segment yolda bozulmuştur bu durumda bu datagram kaynak noktasından tekrar istenir. Aşağıdaki şekilde TCP segmenti görülmektedir.

Kaynak Portu		Hedef Portu						
Sıra Numarası								
Onay (Acknowledgement)								
Data Offset	Ayrılmış	U R G	A C K	P S H	R R T	S Y N	P I N	Pencere (Window)
Kontrol Toplamı (checksum)		Acil işareti (Urgent Pointer)						
Bilgi ..... diğer 500 oktet								

Şekil 2.2. TCP Segmenti

Başlık içinde bulunan diğer bilgiler genelde iki bilgisayar arasında kurulan bağlantının kontrolüne yöneliktir. Segmentin varışında alıcı gönderici noktaya bir “onay” (acknowledgement) yollar. Örneğin kaynak noktasına yollanan “onay numarası” (Acknowledgement number) 1500 ise oktet numarası 1500’e kadar tüm bilginin alındığını gösterir. Eğer kaynak noktası belli bir zaman içinde bu bilgiyi varış noktasından alamazsa o bilgiyi tekrar yollar. “Pencere” bilgisi bir anda ne kadar bilginin gönderileceğini kontrol etmek için kullanılır. Burada amaç her segmentin gönderilmesinden sonra karşıya ulaşıp ulaşmadığı ile ilgili onay (ack) beklenmesi yerine segmentleri onay beklemeksizin pencere bilgisine göre yollamaktır. Zira yavaş hatlar kullanılarak yapılan iletişimde onay beklenmesi iletişimi çok daha yavaşlatır. Diğer taraftan çok hızlı bir şekilde sürekli segment yollanması karşı tarafın bir anda alabileceğinden fazla bir trafik yaratacağından yine problemler ortaya çıkabilir. Dolayısıyla her iki taraf o anda ne kadar bilgiyi alabileceğini “pencere” bilgisi içinde belirtir. Bilgisayar bilgiyi aldıkça pencere alanındaki boş yer azalır ve sıfır olduğunda yollayıcı bilgi yollamayı durdurur. Alıcı nokta bilgiyi işledikçe pencere artar ve bu da yeni bilgiyi karşıdan kabul edebileceğini gösterir. “Acil işareti” ise bir kontrol karakteri veya diğer bir komut ile transferi kesmek vs. amaçlarla kullanılan bir alandır.

## 2.2. UDP – Kullanıcı Datagram Protokolü (User Datagram Protocol)

TCP, mesajı segmentlere bölen ve bunları birleştiren bir katmandır. Fakat bazı uygulamalarda yollanan mesajlar tek bir datagramın içine girebilecek büyüklükte dirler. Bu tip mesajlara en güzel örnek adres kontrolüdür. İnternet üzerindeki bir bilgisayara ulaşmak için kullanıcılar İnternet adresi yerine o

bilgisayarın adını kullanırlar. Bilgisayar sistemi bağlantı kurmak için çalışmaya başlamadan önce bu ismi İnternet adresine çevirmek durumundadır. İnternet adreslerinin isimlerle karşılık tabloları belirli bilgisayarlar üzerinde tutulduğu için kullanıcının sistemi bu bilgisayardan bu adresi sorgulayıp öğrenmek durumundadır. Bu sorgulama çok kısa bir işlemdir ve tek bir segment içine sığar. Dolayısıyla bu iş için TCP katmanının kullanılması gereksizdir. Cevap paketinin yolda kaybolması durumunda en kötü ihtimalle bu sorgulama tekrar yapılır. Bu tip kullanımlar için TCP'nin alternatifi protokoller vardır. Böyle amaçlar için en çok kullanılan protokol ise UDP'dir (User Datagram Protocol).

UDP datagramların belirli sıralara konmasının gerekli olmadığı uygulamalarda kullanılmak üzere dizayn edilmiştir. TCP'de olduğu gibi UDP'de de bir başlık vardır. Ağ yazılımı bu UDP başlığını iletilecek bilginin başına koyar. Ardından UDP bu bilgiyi IP katmanına yollar. IP katmanı kendi başlık bilgisini ve protokol numarasını yerleştirir (bu sefer protokol numarası alanına UDP'ye ait değer yazılır). Fakat UDP, TCP'nin yaptıklarının hepsini yapmaz. Bilgi burada datagramlara bölünmez ve yollanan paketlerin kaydı tutulmaz. UDP'nin tek sağladığı, port numarasıdır. Böylece pek çok program UDP'yi kullanabilir. Daha az bilgi içerdiği için doğal olarak UDP başlığı, TCP başlığına göre daha kısadır. Başlık, kaynak ve hedef port numaraları ile kontrol toplamını içeren tüm bilgidir.

### **2.3. IP – İnternet Protokolü**

TCP katmanına gelen bilgi segmentlere ayrıldıktan sonra IP katmanına yollanır. IP katmanı, kendisine gelen TCP segmenti içinde ne olduğu ile ilgilenmez. Sadece kendisine verilen bu bilgiyi ilgili IP adresine yollamak amacındadır. IP katmanının görevi bu segment için ulaşılmak istenen noktaya gidecek bir “yol” (route) bulmaktır. Arada geçilecek sistemler ve geçiş yollarının bu paketi doğru yere geçirmesi için kendi başlık bilgisini TCP katmanından gelen segment'e ekler. TCP katmanından gelen segmentlere IP başlığının eklenmesi ile oluşturulan IP paket birimlerine datagram adı verilir. IP başlığı eklenmiş bir datagram aşağıdaki şekilde gösterilmektedir:

Versiyon	IHL	Servis Tipi	Toplam Uzunluk	
Tanımlama			Bayrak	Parça offset
Yaşam süresi (TTL)	Protokol		Başlık kontrol toplamı	
Kaynak Adresi				
Hedef Adresi				
TCP başlığı ve iletilen bilgi				

Şekil 2.3. IP Datagram

Bu başlıktaki temel bilgi kaynak ve hedef İnternet adresi (32-bitlik adres, 193.140.181.18 gibi), protokol numarası ve kontrol toplamıdır. Bu sayede varış noktasındaki bilgisayar bu paketin nereden geldiğini anlar. Hedef İnternet adresi ulaşmak istenen bilgisayarın adresidir. Bu bilgi sayesinde aradaki yönlendiriciler veya geçiş yolları (gateway) bu datagramı nereye yollayabileceklerini bilirler. Protokol numarası IP'ye karşı tarafta bu datagramı TCP'ye vermesi gerektiğini söyler. Her ne kadar IP trafiğinin çoğunu TCP kullansa da TCP dışında bazı protokollerde kullanılmaktadır dolayısıyla protokoller arası bu ayırım protokol numarası ile belirlenir. Son olarak kontrol toplamı IP başlığının yolda bozulup bozulmadığını kontrol etmek için kullanılır. Dikkat edilirse TCP ve IP ayrı ayrı kontrol toplamları kullanılmaktalar. IP kontrol toplamı başlık bilgisinin bozulup bozulmadığı veya mesajın yanlış yere gidip gitmediğini kontrol için kullanılır. Bu protokollerin tasarımı sırasında TCP'nin ayrıca bir kontrol toplamı hesaplaması ve kullanması daha verimli ve güvenli bulunduğu için iki ayrı kontrol toplamı alınması yoluna gidilmiştir.

Başlıktaki “Yaşam süresi” (Time to Live) alanı IP paketinin yolculuğu esnasında geçilen her sistemde bir azaltılır ve sıfır olduğunda bu paket yok edilir. Bu sayede oluşması muhtemel sonsuz döngüler ortadan kaldırılmış olur. IP katmanında artık başka başlık eklenmez ve iletilecek bilgi fiziksel iletişim ortamı üzerinden yollanmak üzere alt katmana (bu Ethernet, X.25, telefon hattı vs. olabilir) yollanır.

## 2.4. Fiziksel Katman

Günümüzde pek çok bilgisayar ağı Ethernet'i temel iletişim ortamı olarak kullanmaktadır. Ethernet network kartları haberleşmek için MAC (Media Access Control) adreslerini kullanmak zorundadırlar. Bu adres, her bir network kartına üreticisi tarafından, daha sonra değiştirilemeyecek ve dünyada bir eşi daha olmayacak şekilde verilen hexadecimal bir numaradır. MAC adresinin ilk altı rakamı üretici kodunu belirtir. Büyük üreticilerin birden fazla kodu olabilir. Son altı rakam ise üretici tarafından kendi ürettiği her karta ayrı ayrı verilmiş numaradır. MAC adresi, fiziksel adres olarak da tanımlanabilmektedir. Ethernet, teknoloji olarak yayın teknolojisini (broadcast medium) kullanır. Yani bir istasyondan Ethernet ortamına yollanan bir paketi, o Ethernet ağındaki tüm istasyonlar görür. Ancak doğru varış noktasının kim olduğunu, o ağa bağlı makineler Ethernet başlığından anlarlar. Her Ethernet paketi 14 oktetlik bir başlığa sahiptir. Bu başlıkta kaynak ve hedef Ethernet adresi ve bir tip kodu vardır. Dolayısıyla ağ üzerindeki her makine bir paketin kendine ait olup olmadığını bu başlıktaki hedef noktası bilgisine bakarak anlar. Bu noktada Ethernet adresleri ile İnternet adresleri arasında bir bağlantı olmadığını belirtmekte yarar var. Her makine hangi Ethernet adresinin hangi İnternet adresine karşılık geldiğini tutan bir tablo tutmak durumundadır. Tip kodu alanı aynı ağ üzerinde farklı protokollerin kullanılmasını sağlar. Her protokol başlıktaki tip alanına kendine has numarasını koyar. Kontrol toplamı (Checksum) alanındaki değer ile komple paket kontrol edilir. Alıcı ve vericinin hesapladığı değerler birbirine uymuyorsa paket yok edilir. Ancak burada kontrol toplamı başlığın içine değil de paketin sonuna konulur. Ethernet katmanında işlenip gönderilen mesaj ya da bilginin (bu bilgi paketlerine frame adı verilir) son hali Şekil 2.4'teki duruma gelir.

Ethernet hedef adresi	
Ethernet varış (ilk 16 bit)	Ethernet kaynak (ilk 16 bit)
Ethernet kaynak adresi (son 32 bit)	
Tip Kodu	
IP başlık, TCP başlık, iletilen bilgi ..... bilginin sonu	
Ethernet kontrol toplamı (checksum)	

Şekil 2.4. Ethernet Paketi

Bu paketler (frame) hedef noktasında alındığında bütün başlıklar uygun katmanlarca atılır. Ethernet arayüzü Ethernet başlık ve kontrol toplamını atar. Tip koduna bakarak protokol tipini belirler ve Ethernet cihaz sürücüsü bu datagramı IP katmanına geçirir. IP katmanı kendisi ile ilgili katmanı atar ve protokol alanına bakar, protokol alanında TCP olduğu için segmenti TCP katmanına geçirir. TCP sıra numarasına bakar, bu bilgiyi ve diğer bilgileri iletilen dosyayı orijinal durumuna getirmek için kullanır. Sonuçta bir bilgisayar diğer bir bilgisayar ile iletişimi tamamlar.

### **3. VoIP MİMARİLERİ**

#### **3.1 H.323 Mimarisi**

Karşılıklı olarak çalışan iki adet IP Telefonu veya klasik telefon cihazlarını IP ortamında görüştüren cihazların birbirleriyle görüşürken, bir çağrı oturumu açarken, kapatırken, vb. işlemleri yapmak için kullandıkları çeşitli protokoller vardır. Değişik üreticilerin sağladıkları cihaz veya telefonların birbirleriyle görüşebilmesi için ortak bir dil kullanmaları gerekmektedir. Bu amaçla çeşitli protokoller geliştirilmiştir. Bunlardan şimdilik en yaygın olanı H.323'tür.

##### **3.1.1 H.32x Ailesi**

H.320-serisi; ses, video ve grafik haberleşmesinin temel video/telefon kavramlarını düzenler. H.320, uyumlu ses/video giriş ve çıkışları için ortak format ve multimedia terminallerden iletişim linklerinin kullanılması, ses ve görüntü sinyallerinin senkronize edilmesi için protokoller sağlayarak ses ve görüntü bilgilerinin işlenmesi için gereksinimleri belirler.

ITU (International Telecommunication Union – Uluslararası Telekomünikasyon Birliği), H.323 protokol kümesini video konferans uygulamasının paket veri şebekeleri üzerinden yapılmasını sağlamak için geliştirmiştir. VoIP Forumu, H.323 protokol kümesini IP ses ve faks transmisyonu için Uyumluluk Anlaşmalarının (Interoperability Agreement - IA) bir parçası olarak adapte etmiştir.

H.323, LAN üzerinden multimedia haberleşmesi için gereken elemanlar, prosedürler, protokoller, ekipman ve servisleri tanımlar. Bunlar; local area network, firma networkleri, metropolitan area network, wide area network, dial-up network ve İnternet'de ses/görüntü haberleşmesi sağlamak için gereklidir. (Netaş/Nortel Networks, 2000)



### 3.1.2 H.323

ITU tarafından iki ya da daha fazla taraf arasında IP benzeri QoS desteği olmayan bir ağ üzerinde ses ya da görüntü trafiğini taşımak için geliştirilen H.323 standardı, bir protokol grubudur. Önceleri yerel ağlar üzerinde çoklu ortam konferansı için geliştirilmiş, fakat sonradan IP üzerinden ses uygulamasını kapsayacak şekilde genişletilmiştir. Bu standardın tanımlanmasında Microsoft, IBM, Intel, telefon operatörleri ve ISP'lerden oluşan bir çok kurum ve firmanın geniş katılımı ve desteği sağlanmıştır. İnternet telefonu amacıyla kullanılan en geniş ve en etkin standartlardan birisidir. Ses ile beraber tüm çokluortam (data, ses, video, resim gibi) uygulamalarını desteklemektedir. H.323 standardı bir şemsiye standart olup birçok standardı kapsamaktadır. Bu standartlar ses kodlama, video kodlama, sistem kontrol, çoklama, çokluortam yayın senkronizasyonu ve yapısını içermektedir. (Kara vd., 2000) Bu standartlar PSTN, Mobil, ATM, F/R, LAN, WAN, IP tabanlı İnternet gibi networkleri içermektedir. IP telefonun etkileşmek zorunda kalacağı sistemlere ilişkin ITU standartlarından bazıları şunlardır:

- H.323 LAN networkleri için Görüntülü Telefon sistemleri ve ekipmanlarının standardını içeren bir protokoldür. QoS gibi parametreler içermemektedir. (ITU 96c)
- H.324 PSTN networklerinde kullanılan görüntülü telefon sistemi ve ekipmanlarının standartlarını belirleyen bir protokoldür. H.324/M ise GSM gibi hücreli Mobile networkler için geliştirilmiş bir standarttır. (ITU 96d)
- H.310 Genişbandlı ses ve görüntülü iletişim sistemlerini ve terminallerini kapsamayan bir standarttır.
- H.321 Genişbandlı ISDN networkleri için görüntülü telefon terminalleri standartlarını belirler.
- H.322 LAN networkleri için görüntülü telefon sistemleri ve terminallerini kapsamayan bir standarttır. QoS parametreleri içermektedir.

Çizelge 3.1. H.323 Protokol Yapısı

Uygulama Seviyesi	Audio Uygulaması	Video Uygulaması	Sistem Kontrol		Data Uygulaması
	G.711 G.722 G.723.1 G.728 G.729	H.263 H.261		H.225.0 Call Signalling	H.245 Control Protokol
Sunum Seviyesi	RTP		RTCP	H.225.0	
Oturum Seviyesi	UDP		TCP		T.120
Transport Seviyesi	UDP		TCP		
Network Seviyesi	IP				
Link Seviyesi	CSMA/CD, Token Ring Protocol				
Fiziksel Seviye	Ethernet, Token Ring LAN				

H.323 spesifikasyonu, 1996'da ITU'nun Çalışma Grubu 16 tarafından onaylanmıştır. Versiyon 2 ise, Ocak 1998'de onaylanmıştır. Standart, kapsam açısından geniş olup, noktadan-noktaya ve çok noktalı konferansların yanısıra, hem bağımsız sistemleri hem de kişisel bilgisayar teknolojilerini içerir.

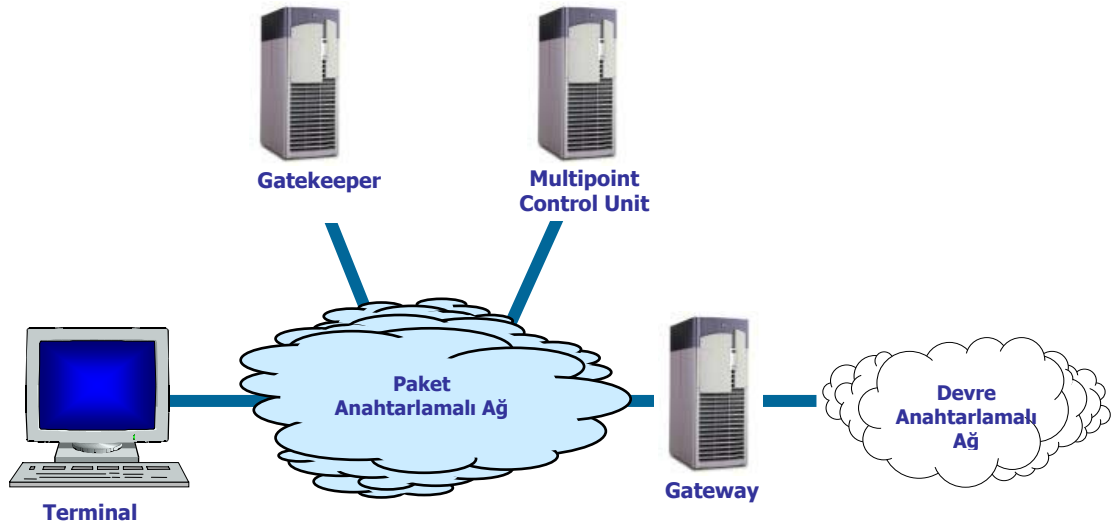
ITU SG16 çalışma grubu G.729 kodlama standardını ve H.323 multimedya standardını IP telefonu uygulamalarında default (varsayılan) standart olarak Ocak 1998 tarihinde onaylayarak belirlemiştir. G.729 standardında 8 Kbps kodlama teknolojisi kullanılmaktadır. G.723.1'in en büyük avantajı ise iki farklı kodlama oranını desteklemesidir. (5,3-6,3 Kbps). G.723.1 kodlama teknolojisi özellikle PSTN şebekesindeki uygulamalar için geliştirildiğinden H.324 ve H.324/M terminal standartları ile son derece uyumlu olarak çalışmaktadır. Bununla beraber H.323 terminal standardı ile de uyumu sağlanarak internet uygulamalarında kullanılmaktadır.

Ayrıca H.323 standardı G.711 (64 Kbps PCM), G.722, G.728, G.729, MPEG-1 Audio kodlama standartlarını desteklemektedir. H.323 terminal standardı GSM, IS-54, IS-95 gibi standartları ile de başarıyla kullanılmaktadır.

H.245 sistem kontrol protokolü ise tüm ses standartlarında kontrol ve sinyalleşme protokolü olarak kullanılmaktadır.

### 3.1.3 H.323 Bileşenleri

Şekil 3.1’de bileşenleri görülen H.323 standardı dört farklı tip uç birim tanımlar. Bu uç birimler; Geçit Denetim Sistemi (Gatekeeper), Ağgeçidi (Gateway), Çok Noktalı Kontrol Birimi (Multipoint Control Unit – MCU) ve Terminallerdir.



Şekil 3.1. H.323 Bileşenleri

#### 3.1.3.1 Geçit Denetim Sistemi (Gatekeeper)

Gatekeeper, H.323 kullanan bir şebekenin en önemli bileşenidir. Bölgesindeki tüm çağrılar için bir merkez nokta olarak çalışır ve kayıtlı uç noktalara çağrı kontrol servislerini sağlar. Genel olarak, H.323 gatekeeper bir sanal santral şeklinde çalışır.

ETSI/TIPHON tanımı ile gatekeeper “Terminallerin ve ağgeçitlerinin (gatewaylerin) kayıt, kabul ve statü (Registration, Admission and Status – RAS) takibinden sorumlu olan ağ modülüdür. Gatekeeperlar bölge (zone) yönetimini ve çağrı işleme/işaretleme işlevlerini de yerine getirirler.” (Kara vd., 2000)

Gatekeeperların kullanılma amacı, çağrıları yaparken makine adresleri yerine makinelere verilecek takma isimleri kullanabilme, ağdaki bandgenişliği kullanımının

yönetilmesi, Gateway ve MCU gibi ağ kaynaklarının yönetilebilmesidir. Gatekeeper orjinal H.323 tanımında video konferansları sırasında ağa erişimi kontrol eden bir birim olarak tasarlanmıştır. Zamanla adres dönüşümü benzeri fonksiyonlarını da kazandı. Bandgenişliği denetimi ise ücretlendirme ihtiyaçları sonucunda ortaya çıktı. Gatekeeperların sağlayabileceği bir diğer servis de çeşitli doğrulama (authantication) yöntemlerini kullanarak bir çağrıya güvenlikle ilgili opsiyonların eklenmesidir. İşaretleşmede kullanılan Q.931 ve H.245 mesajları gatekeeper tarafından yönlendirilebilir ve çağrılar hakkında istatistiksel bilgilerin toplanması sağlanabilir. Call forwarding (çağrı yönlendirme) ya da call transferring (çağrı nakletme) gibi telefon hizmetleri de gatekeeperlar aracılığı ile verilebilmektedir.

### **3.1.3.2 Ağgeçidi (Gateway)**

Ağgeçidi, PSTN ağları ile IP ağları arasındaki arayüzler ya da geçiş elemanı olarak çalışan başka bir ifade ile interworking fonksiyonlarını yerine getiren modüldür. Bir ağgeçidi, paket anahtarlamalı bir ağ üzerindeki H.323 uyumlu terminaller ile devre anahtarlamalı bir ağdaki diğer H.323 terminalleri veya diğer bir ağgeçidi arasında gerçek zamanlı çift yönlü trafik sağlayan bir ağda son nokta olarak çalışır.

IP ağ ile PSTN ağ arasındaki çağrı kurulum ve kaldırma (call setup and clearing) işlemlerini de ağgeçitleri üstlenir. Video, ses ve data formatları arasındaki dönüşüm, bilginin kodlanması/çözmesi ve paketlenmesi işlemleri de ağgeçitlerinde gerçekleştirilir.

Genel olarak ağgeçitlerinin amacı paket anahtarlamalı ağ ile devre anahtarlamalı ağ arasındaki çağrıları her iki yönde şeffaf bir şekilde sonlandırmaktır.

### **3.1.3.3 Çok Noktalı Kontrol Birimi (MCU – Multi-point Control Unit)**

MCU'lar, ağ'da ikiden fazla terminalin ya da ağgeçidinin çoklu bir konferansa katılımlarını sağlamaya yarayan cihazlardır. Sonradan çoklu bir konferansa dönüşebilecek ikili görüşmeler de MCU'lar aracılığı ile sağlanabilir. MCU, bir

kontrol ünitesi (Multipoint Controller-MC) ve işlemciden (MP-Multipoint Processor) oluşur. En basit hali ile MCU tek bir MC'den oluşur, MP seçimli bileşendir.

MC'nin temel görevi, H.245 Kontrol Protokolü yardımıyla konferans görüşmelerin kontrol ve işaretlenmesini gerçekleştirmesidir. İşaretleşme ile, terminaller arası ses, görüntü ve veri bilgilerinin temel nitelikleri tanımlanmaktadır. Ayrıca şebekeye sağladığı kontrol görevi ile, hangi ses, görüntü ve veri bilgilerinin konferans görüşmesine tabi tutulacağını tespit etmektedir. MC bileşeni, bir terminal, gatekeeper, gateway veya MCU üzerinde işlev görebilir. Diğer yandan, MP'nin ana görevi, MC kontrolü altında uç birimlerden gelen bilgi dizisini alıp bağlaşma fonksiyonunu yerine getirdikten sonra konferans görüşmesini gerçekleyen uç birimlere iletilmesini sağlamaktır. (Abazi, 2000)

### **3.1.3.4 Terminaller**

Terminaller uç noktalarda gerçek zamanlı iki yönlü haberleşme sağlayan yerel ağ istemcileridirler (Kişisel bilgisayarlar, IP telefonları v.b.). Tüm H.323 Terminalleri H.245, Q.931, RAS (Registration Admission Status – Kayıt Kabul Durum) ve RTP (Real Time Transport Protocol – Gerçek Zamanlı Taşıma Protokolü) protokollerini desteklemelidir. H.245, kanal kullanım izni için, Q.931 çağrı kurulması ve sinyalleşme için, RTP gerçek zamanlı olarak ses paketlerinin taşınması için, RAS ise Gatekeeper ile haberleşme için kullanılan protokollerdir. (VoIPTurk, İnternet Telefonu Standartları, 2004)

### **3.1.4 H.323'ün Yararları**

H.323 avantajları aşağıdaki gibi özetlenebilir;

#### **Standart Ses Sıkıştırması**

H.323, ses ve video veri akışlarının (stream) sıkıştırılması için standartlar oluşturduğu için, farklı üreticilerin cihazlarının bir arada çalışmasını sağlar.

**Network Türünden Bağımsızlık**

H.323, ortak network mimarilerinin en üstünde çalışmak üzere tasarlanmıştır. Network topolojisi ve bandgenişliği yönetimi geliştikçe H.323 tabanlı çözümler, bu gelişmiş imkanlardan faydalanabilecektir. Örneğin, ses ve verinin ortak bir Ethernet kablolama sistemi üzerinden kombine edilmesiyle büyük maliyet indirimleri sağlanabilir.

**Platform ve Uygulamadan Bağımsızlık**

H.323, herhangi bir donanım veya işletim sistemine bağlanmamıştır. H.323-uyumlu platformlar; birçok boyutta ve şekilde kullanılabilir. Bunlardan bazıları PC'ler, özel platformlar, IP telefonlardır.

**Bandgenişliği Yönetimi**

Video ve ses trafiği, bandgenişliğini yoğun olarak kullanır ve networkü etkileyebilir. H.323, bandgenişliği yönetimi ile bu sorunu kaldırmayı hedeflemiştir. Network Yöneticileri, networkleri içinde eş zamanlı H.323 bağlantılarının sayısını veya H.323 uygulamaları için geçerli olan bandgenişliğini sınırlayabilirler. Bu sınırlar, kritik trafiğin bozulmamasını sağlar.

**Çoklu Nokta (Multicast) Desteği**

H.323, çok noktalı konferansları destekler. Multicast, networkteki hedeflere tekrarlama yapmaksızın tek bir paket gönderir. Unicast ise, her noktaya ayrı paket gönderirken broadcast, tüm hedeflere paket gönderir. Unicast veya broadcast, paketlerin network boyunca tekrarlanması nedeniyle, networkü meşgul eder. Multicast transmisyonu, multicast grubundaki tüm istasyonların tek bir veri okumaları nedeniyle, bandgenişliğini daha verimli kullanır.

**Esneklik**

Bir H.323 konferansı, farklı yetenekte uç noktalar içerebilir. Örneğin, sadece ses yetenekleri olan bir terminal, video ve/veya veri yetenekleri olan terminallerle bir konferansa katılabilir.

### 3.2 SIP (Session Initiation Protocol – Oturum Başlatma Protokolü)

H323 çok yönlü ve oldukça kompleks bir protokoldür bundan dolayı çok fazla emek ve masraf gerektirir. H323'ün bu karmaşık yapısına alternatif olarak SIP ortaya çıkmıştır. SIP IP telefonu uygulamaları için özelleşmiş, var olan protokollerin belirli kısımlarını alarak H323'e göre daha küçük ve etkili bir protokol haline gelmiştir.

SIP bir ya da birden fazla katılımcının yer aldığı oturumları kurmak, değiştirmek ve sonlandırmak için tasarlanmış bir kontrol protokolüdür. Bu protokole göre bir çağrı başlatıldığı zaman gelen çağrı, çağrıyı başlatan tarafa servis veren bir sunucuya yönlendirilir. Çağrının yönlendirildiği sunucu çağrıyı reddedebilir ya da başka bir sunucuya ya da terminale yönlendirebilir. Çağrı bu şekilde cevap verecek bir sunucu buluncaya kadar ağda hiyerarşik olarak iletilir. SIP güvenilirliği kendisi sağlayıp TCP'nin güvenlikle ilgili normlarını kullanmaya gerek duymaz. SIP ilgili oturumda hangi codec'in kullanılacağına karar vermek için SDP (Oturum Tanımlama Protokolü-Session Description Protocol) olarak adlandırılan bir protokol kullanır.

#### 3.2.1 SIP Bileşenleri

- **SIP Kullanıcı Aracı (SIP User Agents):** SIP'i destekleyen uç aygıtlara SIP kullanıcı araçları adı verilir. SIP'in temel amacı kullanıcı araçları arasında kurulacak oturumlara olanak sağlamak. Bir kullanıcı aracı kullanıcılardan talimat ya da girdi alır ve diğer kullanıcı araçlarıyla oturum kurmak ya da kaldırmak için kendi tarafında aracılık yapar.

- **SIP Gateway:** Bir SIP gateway farklı bir sinyal protokolü kullanan bir ağ ile SIP ağı arasında arayüz görevi gören bir uygulamadır.

- **SIP Sunucu (SIP Server):** SIP sunucuları, SIP isteklerini kabul eden ve bunlara cevap gönderen uygulamalardır.

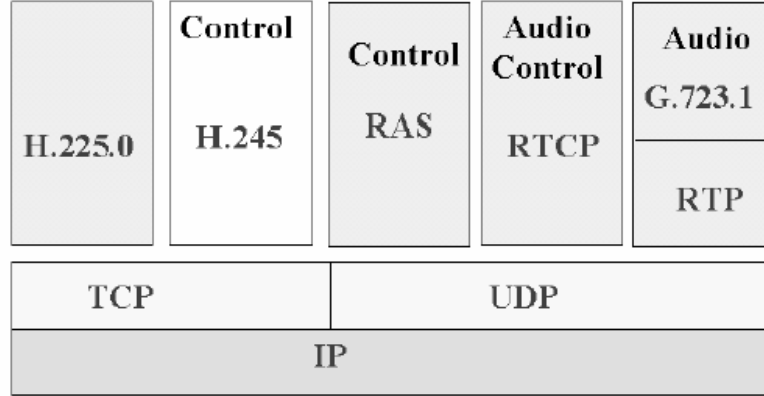
### 3.2.2 SIP'in Sağladığı Hizmetler

- Kullanıcı yeri (User location): Haberleşme için kullanılacak uç sistemin belirlenmesi.
- Arama kurulumu (Call setup): Arayan ve aranan telefonların zil çaldırması ve çağrı parametrelerinin kurulması.
- Kullanıcı uygunluğu (User availability): Aranan tarafın haberleşmeye dahil olma isteğinin belirlenmesi
- Kullanıcı kabiliyetleri (User capabilities): Kullanılacak medya ortam ve medya parametrelerini belirlenmesi.
- Arama karşılama (Call handling): Çağrının transferi ve sonlandırılması.



#### 4. H.323 PROTOKOLLERİ

H.323 protokol kümesi, TCP/IP'nin üstünde bulunan bir protokol kümesidir ve internet üzerinden multimedya uygulamalarını sağlar.



Şekil 4.1. H.323 protokoller topluluğu

##### 4.1. Kodlama Teknikleri

Ses analizinde iki önemli teknik kullanılır; dalga formu kodlama (waveform coding) ve ses kodlama (voice coding - vocoding). PCM gibi dalga formu kodlama metotları, doğrudan analog konuşma tarafından üretilen dalga formunu sinyalin örneklenmesi ve her örnekleme genliğinin en yakın değerine dönüştürülmesiyle kodlar. Bu işlem “quantizing”, gerçek genlik ile örneklenen değer arasındaki farklılık da “quantizing hatası” olarak adlandırılır.

Bir vocoder (ses kodlayıcı), orijinal konuşmaya benzer bir sinyal üretmek için girişi kullanır. Bunu yaparken, vocoder her konuşma örneğini uygun parametre setini tanımlamak amacıyla analiz eder. Bu parametreler, konuşmayı daha sonra bir sentezleme işlemi üzerinden yeniden oluşturacak olan alıcıya gönderilir. Vocoder'ler, daha az bandgenişliği gerektirir. (Netaş/Nortel Networks, 2000)

#### 4.1.1. Kodlama Standartları

IP üzerinden ses haberleşmesi uygulamalarındaki en temel işlem sesin sıkıştırılmasıdır. Bu amaçla çeşitli teknik ve standartlar uygulanmaktadır. Hedef, iyi ses kalitesi ve düşük sayısallaştırma gecikmesidir. Bu sıkıştırma ve çözümleme işlemini yapan cihazlara genellikle Codec (Coder-Decoder ya da enCOde-DECode) denilmektedir. (Kara vd., 2000) Aşağıda sıkıştırma metotları ve bunlar ile ilgili standartlar konusunda kısa açıklamalar verilmiştir :

- **G.711 PCM** : Günümüz PSTN sistemlerinde standart olarak kullanılan 64 Kbit PCM ses kodlama tekniği ile ilgili ITU standardıdır. 64 kbit/s'de PCM ses kodlama tekniğini açıklar. G.711'de, kodlanmış ses, genel telefon şebekesinde (PSTN) veya PBX'ler üzerinden sayısal ses iletimi için hazır durumdadır.
- **G.723.1** : 5,3 kbit/s ve 6,3 kbit/s olmak üzere çift hızlı ses codec standardıdır. (ITU 96a) Çok düşük bir bit oranında konuşma veya ses sinyali bileşenlerinin sıkıştırılmasında kullanılabilen bir sıkıştırma tekniğini tanımlar. Daha düşük olan bit oranı sistem tasarımcılarına ek esneklik sağlarken, yüksek olan bit oranı, biraz daha yüksek ses kalitesi sunar.
- **G.726-ADPCM** : Adaptive Differential PCM. 32 Kbit'lik bir kodlamadır. 40, 32, 24, ve 16 kbit/s'de ADPCM kodlamayı açıklar. ADPCM-kodlanmış ses, paket ses, PSTN ve eğer PBX şebekeleri ADPCM desteklemek üzere konfigüre edilmişse PBX şebekeleri arasında transfer edilebilir.
- **G.728- CELP** : Sesin 8 kbit/s'de kullanılan bir ses sıkıştırma algoritması (CELP - Code Excited Linear Prediction) yöntemi ile 16 kbit'te kodlanması metodudur. CELP sıkıştırmasının 16 kbits düşük gecikme varyasyonunu tanımlar. CELP ses kodlamasının, PSTN üzerinden iletim için genel bir telefon formatına dönüştürülmelidir.
- **G.729-CS-ACELP** : Bu standart CS-ACELP (Conjugate Structure - Algebraic Code Excite Linear Prediction) sıkıştırma tekniğini açıklamaktadır. Bu teknikte ses 8 Kbit'e kadar sıkıştırılmaktadır. Bu standardın iki varyasyonu vardır. (G.729 ve G.729 Annex A) Bu iki standart matematiksel

karmaşıklıkta farklılık göstermektedir. Temel olarak ikisi de 32 kbit ADPCM'e benzer ses kalitesi vermektedir.

- **GSM (13 kbps)**
- **IS-54 (7.95 kbps)**
- **IS-95 (9.6 kbps)**
- **PDC (6.7 kbps)**

#### **4.1.2. Temel Sıkıştırma Tipleri**

1997'de, VoIP Forumu Internet telefonu uyumluluğu için önemli bir adım olan G.723.1 codec'te standartlaştırma üzerinde anlaşmıştır. G.723.1 codec, düşük bandgenişliği ortamlarında çalışabilmesi nedeniyle seçilmiştir.

Normal telefon sistemi tarafından kullanılan PCM standardı kadar kaliteli olmamakla birlikte, G.723.1 kabul edilebilir konuşma kalitesi sağlayan bir kodlayıcıdır.

G.723.1 minimum karmaşıklık kullanarak yüksek bir kalitede konuşmayı sağlamak üzere optimize edilmiştir. Müzik ve diğer ses sinyalleri, konuşma kadar kaliteli olarak sağlanamaz, fakat bu kodlayıcı kullanılarak sıkıştırılabilir.

##### **4.1.2.1. G.723.1**

Tipik bir IP telefon uygulamasında, bir çift IP gateway tarafından karşılıklı bağlanmış PSTN/GSM kullanıcıları arasındaki telefon çağrıları, ayrı RTP/UDP/IP bağlantıları tarafından taşınır. Gelen konuşma örneklemelerini sıkıştıran IP gateway'deki Codec'ler, konuşma örneği başına 5 ile 24 byte arası boylarda paketler üretir. G.723.1, 30 ms aralıklarla 20 veya 24 byte konuşma paketi üretir.

Mobil ortamlarda kullanılan çoğu codec, konuşma örnekleme başına 10 byte'dan daha küçük boyutta paketler üretir. Küçük boyutlu paketler, RTP kullanılarak transfer edildiğinde, şebekede yüklenme meydana gelir. Tek bir konuşma paketi için

RTP/UDP/IP overhead, 40 byte (12+8+20)'dır. RTP/UDP/IP içinde paketlenmiş 10 byte'lık ses paketinin %80'lik bir ek yükü (overhead) vardır.

#### **4.2. Video Standardı**

Video standardı H.261 ve H.263 protokolü ile sağlanmaktadır. H.261 düşük bit oranlarını desteklememektedir. Bu terminal standartları, video sinyallerinin hem kodlama hem de kod çözme işlemlerini kapsamaktadır. ISDN ağlarında ise H.320 videokonferans terminal standartları kullanılmaktadır. Bu standart 128 Kbps'lik bir bandgenişliğinden ses, video ve data transferine imkan vermektedir. Bu standartlar H.323 ile uyumlu çalışmaktadırlar ve H.320 terminal ISDN standardı ile H.261 ve H.263 görüntü standartları birbirini desteklemektedir. (VoIPTurk, İnternet Telefonu Standartları, 2004)

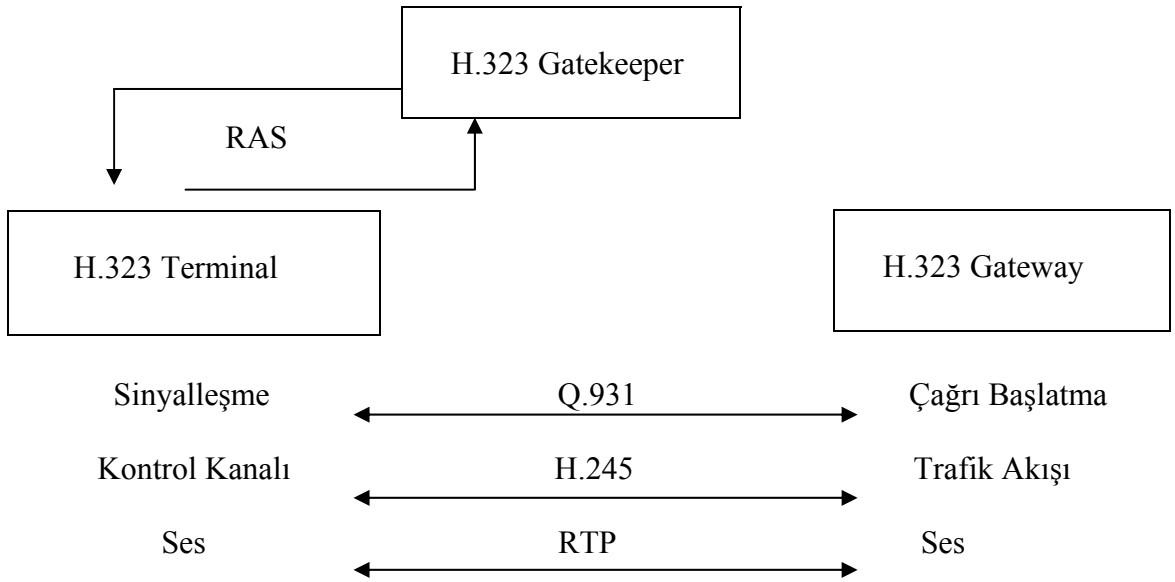
#### **4.3. H.225 Kayıt, Kabul ve Durum Protokolü (Registration, Admission and Status - RAS)**

RAS, uç birimleri (terminaller ve gateway) ile gatekeeper arasında tanımlanmış bir protokoldür. RAS genel olarak, uç birimlerin bir gatekeeper ile kayıt, kabul kontrolü ve iletişim bandgenişliği değişiklikleri durumu üzerinde işlev görmektedir. Bu amaçla mesajların deęiş-tokuşu için RAS, bir işaretleşme kanalı kullanmaktadır. Bu kanal, "RAS kanalı" olarak adlandırılmaktadır. (Abazi, 2000)

H.323 terminalleri arasında sesin transferi süreci, genelde dört basamakta sağlanır: Kayıt, kabul ve durum mesajlaşması için kullanılan güvenilir olmayan kanal, RAS kanalıdır. Bir çağrının başlatılması için genel yaklaşım, RAS kanalından zorunlu bir kabul istek mesajının gönderilmesi, takiben bir güvenilir kanalda bir başlangıç kurulum (Setup) mesajı tarafından transport adresinin (bu adres, kabul onay mesajında geri döndürülebilir veya arayan terminal olarak bilinebilir) gönderilmesidir.

Bu başlangıç mesajının bir sonucu olarak, çağrı kurulum işlem sırası, Q.931 çalışması temel alınarak başlatılır. İşlem sırası, terminalin “Bağlan” (Connect) mesajının içinde üzerinden H.245 kontrol mesajlarını göndermek için güvenilir bir transport adresi almasıyla tamamlanır.

Güvenilir H.245 kontrol kanalı kurulduğunda, ses, video ve veri için ek kanallar, H.245 lojik kanal prosedürleri kullanılarak kurulabilir. H.225.0 terminalleri, sesi gecikmeyi asgariye indirmek için RTP kullanarak güvenilir olmayan kanallar üzerinden gönderir.



Şekil 4.2. RAS Çalışması

#### 4.4. H.225 Çağırma İşaretleme Protokolü

ITU-T H.225 protokolü, ISDN ağları için tasarlanmış ve Q.931 işaretleme protokolü temel alınarak geliştirilmiştir. İki H.323 uç birimi arasındaki çağırmanın kurulması ve sonlanması kontrolünü üstlenmektedir. H.225, ses, görüntü ve veri bilgileri ile paket tabanlı şebekenin kontrol bilgileri arasındaki yönetimin nasıl gerçekleştirilebileceğini açıklamaktadır. (Abazi, 2000)



Şekil 4.3. H.225 Çağırma İşaretleşme Protokolü

#### 4.5. H.245 Kontrol İşaretleşme Protokolü

ITU-T H.245 protokolü, telefon tabanlı olmayan işaretler için hat transmisionunu gerçekleştirmektedir. Daha doğrusu, terminal mesajlarının bilgi sözdizimini (syntax) ve bu mesajların kullanılmasındaki prosedürü (akış kontrolü) belirtmektedir. H.222.0, H.223 ve H.225 protokolleri tarafından kullanıldığı için, genel kontrol protokolünü temsil etmektedir. Terminal niteliklerinin belirlenmesi, mantıksal kanal işaretleşmeleri gibi mesaj bilgileri H.245 ile gerçekleştirilmektedir. Mesaj türleri istek, onay ve red komutlarıyla tanımlanmıştır.



Şekil 4.4. H.245 Kontrol Protokolü

#### 4.6. T.12x Veri Haberleşme Protokolleri

ITU-T'nin T.12x tavsiyeleri bir çoğul-ortam konferans görüşmesi için veri haberleşmesini tanımlamaktadır. T.12x standartları, bir çoğul-ortam konferans görüşmesi için gerçek-zamanda dosya ve grafiksel bilgilerinin dağılım bütünlüğüdür. Örneğin, T.120 tavsiyesi bir konferans görüşmesi sırasında uç birimler arasında ses-resim (audiovisual), ses-grafik (audiographic) uygulamalarını desteklemektedir.

#### 4.7. H.235 Güvenlik Protokolü

H.323 çerçevesi içinde güvenlik hizmetlerine değer katmak için geliştirilen bir protokoldür. Başlıca yerine getirdiği işlevler; doğrulama ve gizlilik-şifrelemedir (privacy-encryption). (Abazi, 2000)

H.235 standardı, güvenlik ile uğraşırken dört genel sorunu belirlemiştir: İzin (Authentication), bütünlük (Integrity), kişiye özellik (Privacy) ve inkarın reddi (non-Repudiation). İzin (Authentication), konferansa katılan uç noktaların gerçekten söyledikleri kişi olduklarından emin olmak demektir. Bütünlük (Integrity), bir paket içindeki verinin gerçekten verinin değişmeden sunumu olduğu anlamına gelir. Kişiyi özellik/Gizlilik (Privacy/Confidentiality), araya girilse bile anlaşılamayacak şekilde veriyi gizli dinleyicilerden saklayan şifreleme ve şifre açma mekanizmalarının sağlanmasıdır. İnkarın reddi (non-Repudiation), kendisinin orada olduğunu bildiğiniz halde bir konferansa katıldığını reddeden bir kişiye karşı koruma demektir.

#### 4.8. Gerçek-Zamanlı Taşıma Protokolü (Real-Time Transport Protocol – RTP)

RTP, IETF tarafından geliştirilmiş bir standarttır. H.323 ile beraber kullanılmaktadır. RTP uçtan uca bir işletim protokolüdür ve UDP üzerinde çalışır. RTP çokluortam uygulamalarında iki önemli görevi yerini getirir. RTP'nin en önemli görevi senkronizasyon mekanizmasını sağlamaktır. Diğer bir görevi ise datanın resim ve ses kodlamasını tanımlamaktadır. (Kara vd., 2000)

RTP (Real-time Transport Protocol) gerçek zamanlı veriler için kullanılan gayet sağlam bir protokoldür. UDP'nin en üst düzeyinde çalışacak şekilde dizayn edilen RTP, IP telefonu da dahil olmak üzere çok sayıda uygulama tarafından kullanılır. Paket tabanlı şebekelerde ses ve video verilerinin gönderilmesi sırasında tercih edilen protokol RTP'dir. İletim kalitesini sunucuya bildiren RTCP (Real-time Transport Control Protocol) de RTP ile kullanılır.

RTP, özel bir RTP başlığındaki her UDP paketine bir zaman etiketi ve bir dizi numarası verir. Zaman etiketi, RTP paketiyle taşınan içeriğin sunum ya da kompozisyonuyla ilgilidir. Bu bilgi içeriğin doğru hızda oynatılmasını sağlar. Streaming içerik sunumunun senkronizasyonu için de RTCP ile birlikte bu etiket kullanılır. Bir iletim spesifikasyonu zaman etiketi ve diğer RTP alanlarının yorumlanmasına ait tanımlar içerir. Dizi numarası ise alıcı tarafından paket kayıplarını tespit etmek için kullanılır. Kayıp paketlere ait istatistikler de sunucuya RTCP üzerinden ulaştırılabilir.

#### **4.9. Gerçek-Zaman Kontrol Protokolü (RTP Control Protocol – RTCP)**

RTCP, RTP'nin bir parçası olup RTP'de bulunan özelliklerin yanı sıra ISDN networklerinde videokonferans ve video telefonu için gerekli QoS parametrelerini de desteklemektedir. Zamanlama, yeniden yapılandırma, kayıp sezme, güvenlik ve içerik tanımlama dahil olmak üzere gerçek-zaman özellikli uygulamalar için destek sağlayan bir protokoldür. RTP'yi kontrol etmek amacıyla geliştirilmiştir.

RTCP protokolü ile ses ve video bilgilerinin oturum kontrol fonksiyonları, data oranları ve diğer parametreleri ayarlanabilmektedir. Ayrıca RTCP ile ses ve video sinyalleri kontrol edilebilmektedir.

#### **4.10. RTSP (Real-Time Streaming Protocol)**

RTSP (Real-Time Streaming Protocol) veri akışı uygulamaları için bir oturum kontrol protokolü olarak kullanılır. RTSP'deki bazı özellikler HTTP'den alınmıştır. Özellikle tek yönlü gerçek-zamanlı veri akışı için geliştirilmiştir (Web üzerinden radyo yayını gibi). İstemci tarafındaki bir veri akışı uygulaması RTSP'yi kullanarak veri akışı (streaming) sunucusu ile bir oturum başlatabilir. İstemci bu oturum ile sunucudan; veri akışının başlatılmasını, veri akışına ara verilmesini, akışın yenilenmesini, ileri alınmasını, akışın durdurulması ve oturumun kapatılmasını isteyebilecektir. (Ericsson Mobility World, 2004)



## 5. İNTERNET ÜZERİNDEN SESİN (VoIP) KALİTESİ

Geleneksel telefon trafiğini taşımak için internet veya intranet gibi bir veri iletişim alt yapısını kullanma yeteneği, büyük olanaklar yaratmıştır. Ancak, genel telefon şebekesi üzerinden ses iletiminin tersine internet üzerinden ses, genellikle düşük kalitede olup yeterince güvenli değildir. Bu nedenle Servis Kalitesi (Quality of Service - QoS), önemli bir parametredir. QoS her zaman uçtan uca bağlantıya göre belirlenir.

Servis kalitesi, aynı hattı paylaşan verilerin sınıflandırılmasını ve bu şekilde kullanıcıya göre önem taşıyan verilerin öncelikli ve kayıpsız olarak iletilmesini sağlamak amacıyla kullanılan bir özelliktir. Sesin data hatları üzerinden gönderilmesi esnasında kaplayacağı bandgenişliği, data ile birlikte eşzamanlı kullanılma şartları, servis kalitesi gibi önemli değerler, VoIP teknolojisinin verimli kullanılması için gerekli kriterleri oluşturmaktadır.

VoIP gerçekleştirilen bir network içerisinde sesi ileten cihazların (router) QoS desteğini sağlıyor olmaları gerekmektedir. Aksi takdirde, hatlardan geçen dataların yoğunluk kazandığı esnada yapılan telefon görüşmeleri yeterli bandgenişliğine sahip olamayacakları için kesilebilmektedir. Bu nedenle sesin önceliklendirilmesi gereken durumlarda router'lar üzerinde gerçekleştirilecek QoS ayarları ile ses dataları önceliklendirilir ve konuşma olduğu sürece data ne kadar yoğun bile olsa sesin engellenmesine izin vermez. Böylece kesintisiz ve kaliteli bir görüşme imkanı yaratılmış olur.

VoIP'te dijital sinyal işlemcisi ses sinyalini framelere (çerçevelere) ayırır ve ses paketleri haline çevirir. Bu ses paketleri İnternet Protokol kullanılarak ITU'nun H.323, ses, video ve bilgi taşıma kurallarına göre networkte taşınır. VoIP gecikmeye duyarlı bir uygulamadır ve VoIP'i başarıyla kullanabilmek için baştan sona iyi dizayn edilmiş bir networke sahip olmak gerekir. VoIP, servisin kaliteli olması için bazı protokoller ve networkte ince ayarlar gerektirir. Ağ trafiğini yönlendirme de, sesli bağlantıların devamlılığını garantiye almak için dikkate alınmalıdır.

### 5.1. Servis Kalitesinin Önemi

Günümüzde çok çeşitli ağ trafiği bulunmakta, ve her trafik türünün kendine özgü bantgenişliği, gecikme, kayıp ve kesintisiz çalışma özellikleri bulunmaktadır. İnternet'in kat ettiği inanılmaz büyüme ile günümüzde çoğu ağ trafiği IP-temelli olmuştur. Tek bir uçtan-uca iletim protokolü, ağ ekipmanlarının bakımının daha az karmaşık olması ve daha düşük işletme maliyetleri açısından oldukça faydalıdır. Ancak bu faydaların yanında, IP'nin bağlantısız bir protokol olduğunu da gözardı etmemek gerekir, örneğin IP paketleri ağ üzerinde hareket ederken önceden belirlenen bir yol izlemezler. Bu da ağ üzerindeki servis kalitesinin önceden tahmin edilememesine yol açmaktadır.

IP protokolü ilk tasarlanırken bir paketin varış noktasına güvenle ulaşmasını sağlamak amacı hedeflenmiş, ancak o noktaya giderken geçen zaman göz önüne alınmamıştı. Şimdiki IP ağları farklı türlerde uygulamaları da desteklemek zorunluluğundadır. Bu uygulamaların büyük çoğunluğu ise düşük gecikme gerektirir. Aksi takdirde, uç kullanıcı ciddi ölçüde etkilenebilir ya da uygulama tamamen çalışmaz duruma gelir.

Bir ses uygulamasını göz önüne alalım. Ses uygulamaları kamusal ses ağları üzerinde son derece sınırlı kalıpları olan TDM (Time Division Multiplexing-Zaman Bölünmeli Çoğullama) teknolojisi ile taşınır. Ses trafiği TDM ağları üzerinde sabit ancak çok küçük bir gecikme yaşarken aşağı yukarı hiç kayba uğramaz. Ses uygulamaları da doğru işleyebilmek için bu tür kalıplara ihtiyaç duyarlar. Ses uygulamalarının kullanıcıların beklentilerini karşılamak için aynı seviyede "TDM ses" kalitesine gereksinimleri vardır.

Herhangi bir "TDM ses" uygulamasını alalım ve onu bir IP ağı üzerine taşıyalım. IP ağlarında ses paketleri önceden tahmin edilemeyen ve değişik seviyelerde gecikmeler yaşayabileceği gibi ağ tıkanıklıkları olduğu zaman paketler atılabilmektedir. Görüldüğü üzere, IP ağları ses uygulamalarının gereksinim duyduğu yapıya sahip değildir. IP ağlarına QoS teknikleri uygulanarak kabul edilebilir, istikrarlı ve önceden tahmin edilebilir ses kalitesi olan VoIP desteği sağlanabilir. (Nortel Networks Netaş – Servis Kalitesine İlk Adım, 2004)

## 5.2. Sistem ve QoS Kontrol

Sistem kontrolü H.323 protokolü için H.245 standardı ile tanımlanmıştır. H.245 standardı ile yayın ve senkronizasyon ve H.225.0 ile de paketleme standardı belirlenmiştir. Noktadan noktaya tüm kontrol işlemleri H.245 tarafından sağlanmaktadır. Farklı ortamlar arasında kanalların açılması, kapatılması kanalların tek yönlü veya çift yönlü kullanılması gibi işlemler H.245 kontrol protokolü tarafından sağlanır. Ayrıca H.245 ile PSTN networkü ile IP networkü arasında DTMF gibi sinyallerin dönüşümü ve kontrolü de sağlanmaktadır. H.245 kontrol protokolü hem H.323 hem de H.324 protokollerini desteklemekte ve bu protokoller arasındaki çalışma düzenini sağlamaktadır. H.323 protokolü QoS parametrelerini desteklememektedir. Ses ve video paketleri UDP üzerinden gönderilmesi durumunda paket kayıpları söz konusu olacağından ve UDP'nin özelliği gereği paketler tekrar gönderilmeyeceğinden QoS parametrelerini desteklememektedir. H.245 kontrol protokolü ise TCP protokolünün kullanımına izin vermektedir. Dolayısıyla kayıp paketler tekrar gönderilebilmektedir. Böylece TCP protokolünün kullanılmasıyla QoS parametreleri tanımlanabilmektedir. (Kara vd., 2000)

## 5.3. Servis Kalitesi Uygulamaları

QoS, bir kullanıcının ya da uygulamanın ağdan aldığı genel servis deneyimini tanımlamak için kullanılan geniş kapsamlı bir ifadedir. QoS'nin içinde teknoloji, mimari ve protokollerin geniş bir yelpazesi bulunmaktadır. Ağ işletmecilerinin ağda uçtan-uca QoS sağlayabilmeleri için, ağ bileşenlerinin ağ üzerinden geçen veri akışına istikrarlı bir şekilde müdahalede bulunmasını sağlamaları gereklidir.

Ağ uygulamaları kullanıcı taleplerine ya da uygulama gereksinimlerine göre gruplanabilir. Bazı uygulamalar kişiler arasında, bazıları ise bir kişi ile ağa bağlı cihazın uygulaması arasında olabilmektedir (Bir PC ve bir web sunucusu arasında). Bazı uygulamalar ise yönlendiriciden-yönlendiriciye gibi ağ cihazları arasında olabilmektedir. (Nortel Networks Netaş – Servis Kalitesi Uygulamaları, 2004)

### 5.3.1. Etkileşimli uygulamalar

Bazı uygulamalar, iki ya da daha fazla kullanıcının aktif olarak katılımı ile "etkileşimli" olabilmektedir. Bu kullanıcıların ağ uygulamasından gerçek-zamanlı olarak cevap alma talepleri bulunur. Bu bağlamda "gerçek-zaman", alıcı ile gönderenin arasında gecikme ve gecikme değişiminin minimum olduğunu ifade etmektedir. Telefon görüşmeleri gibi bazı etkileşimli uygulamalar yüz yıldan bu yana telefon şirketlerinin devre anahtarları üzerinde "gerçek-zamanlı" olarak çalışmaktadır. Ses uygulamalarının belirli ölçüdeki QoS gereksinimlerinin aynı standartlar ile VoIP gibi paket ses sistemlerinde de sağlanması gerekmektedir.

Diğer etkileşimli uygulamalar arasında video konferansı ve etkileşimli oyunlar bulunmaktadır. Etkileşimli uygulamalar gerçek-zamanlı çalıştığından paket kaybı en aza indirgenmiş olmalıdır. Telefonda konuşurken, sık sık kelimelerin bazı kısımlarının kaybolduğu düşünüldüğünde, QoS seviyesi bu durumda "yetersiz" olarak ifade edilecektir.

Etkileşimli uygulamalar UDP-temelli olduklarından, TCP-temelli uygulamalarda olduğu gibi kayıp ya da devre dışı kalan paketler yeniden iletilmez. Bununla beraber, etkileşimli uygulamalar zamana duyarlı olmaları sebebiyle paketlerin yeniden gönderilmesi fayda sağlamayacaktır. Örneğin, bir ses paketi kaybolduğunda, konuşma süreci devam ettiğinden ve kaybolan paketin ait olduğu bölüm geçmiş zaman dilimi içinde kaldığından göndericinin o kısmı yeniden göndermesinin de bir anlamı olmayacaktır.

### 5.3.2. Duyarlı uygulamalar

Bazı uygulamalar bir kişi ile ağ cihazları uygulaması arasında bulunmaktadır. Uç kullanıcıların beklentisi bu uygulamaların duyarlı olması, yani ağa bağlı cihazın gönderilen talebin mümkün olduğunca kısa sürede cevaplanmasıdır. Bu uygulamalara çoğunlukla "gerçek zamana yakın" da denilmektedir. Bu tür uygulamalarda paket gecikme süresinin, gecikme değişimlerinin ve kayıpların düşük olması gerekmektedir. Ancak, duyarlı uygulamaların QoS gereksinimleri gerçek-zamanlı, etkileşimli uygulamalarda olduğu kadar katı değildir. Akan medya

uygulamaları arasında internet radyo (konuşmalar ve müzik) ile ses/görüntü yayınları (haberler, eğitim, öğretim ve filmler) bulunmaktadır. Akan uygulamalar, medyanın işleminin çok uzun süre almaması gerektiğinden ağın duyarlı olmasına gereksinim duyarlar. Bu uygulamalar aynı zamanda, ağın bazı sinyal türlerine duyarlı olmasını da gerektirirler.

Kaybolmuş akan medya paketlerinin yeniden iletimi, ortamda yeterince depolama alanı olduğu sürece uygulama düzeyinde protokollerle gerçekleştirilir. Bu gerçekleşmezse, kaybolan paketler devre dışı bırakılır, bu da ortamda (ses ya da görüntü) bozulmalara neden olur.

### **5.3.3. Zamanlı uygulamalar**

Bir kişi ile ağa bağlı cihazın uygulaması arasındaki bazı uygulamalar "gerçek zamana yakın" performansa ihtiyaç duymasalar da, bilginin zamanında iletimi her şart altında gereklidir. Buna örnek olarak, e-posta uygulamalarının saklanarak daha ileri bir zamanda gönderimi ve dosya iletimleri gösterilebilir. Bu uygulamaların önemleri, iş önceliklerine göre belirlenecektir. Bu tür uygulamalarda paketlerin sınırlı bir gecikme ile gelişleri gerekmektedir. Örneğin; bir e-postanın varış noktasına ulaşması birkaç dakika alıyor ise bu kabul edilebilir, ancak iş ortamında bu e-postanın varış noktasına 10 dakikada ulaşması çoğu zaman kabul edilemez. Aynı sınırlı gecikme durumu dosya transferleri için de geçerlidir. Bir dosyanın transfer işlemi başladığında gecikme ve gecikme değişimi çoğu kez dosya transferinin birkaç dakika alması sebebiyle farkedilmez. Zamanlı uygulamalar TCP temelli iletişim kullanırlar, bu yüzden paket kayıpları da, kaybolan paketlerin yeniden iletimini mümkün kılan ve dolayısıyla gerçek anlamda kayıp yaratmayan TCP ile yönetilmektedir.

## 6. SERVİS KALİTESİNE ETKİ EDEN PARAMETRELER VE ANALİZLERİ

Genel telefon şebekesi üzerinden geçen ses transmisyonu ile karşılaştırıldığında, VoIP ürünlerinin güvenilirlik ve servis kalitesi (QoS) sorunları vardır. Tezin bu bölümünde, servis kalitesine etki eden parametreler ve çözüm yolları tartışılacaktır.

### 6.1. Bandgenişliği

Bandgenişliği, servis kalitesini etkileyen en büyük parametrelerden biridir. Kullanıcılar, herhangi bir zaman diliminde diğer kullanıcıların bandgenişliği kullanımına bağlı olarak daha az veya daha çok bandgenişliği kullanırlar. Ağ üzerindeki trafiğin az olduğu şartlarda kullanıcı daha yüksek bandgenişliği kullanabilir, ancak bu süreklilik taşıyan bir durum değildir. Bu durum kullanıcılar tarafından özellikle ağ üzerinde erişimin yoğun olduğu saatlerde daha açık olarak fark edilebilir. (Nortel Networks Netaş – Servis Kalitesine İlk Adım, 2004)

### 6.2. Gecikmeler

Ağ üzerindeki gecikme, bir uygulamanın iletim sürecinde ağın giriş ve çıkış noktaları arasında hareket ettiği zaman dilimidir. Gecikme, ses, görüntü ve faks iletimleri gibi normalin dışındaki gecikmelerde zaman aşımına uğrayıp, iptal olan uygulamalar üzerinde önemli QoS sorunları yaratmaktadır. Bazı uygulamalar az miktarlardaki gecikmeleri tolere edebilmekte, ancak belirli bir süre aşıldıktan sonra QoS sorunu kaçınılmaz hale gelmektedir.

#### 6.2.1. Paket Gecikmesi

Paket gecikmesi, kaynaktan gönderilen paketin çıkış zamanı ( $T_{kaynak}$ ) ile hedefe ulaşan paketlerin ulaşma zamanı ( $T_{hedef}$ ) arasındaki farktır. (Metin, 2001)

$$\text{Paket Gecikmesi} = T_{hedef} - T_{kaynak}$$

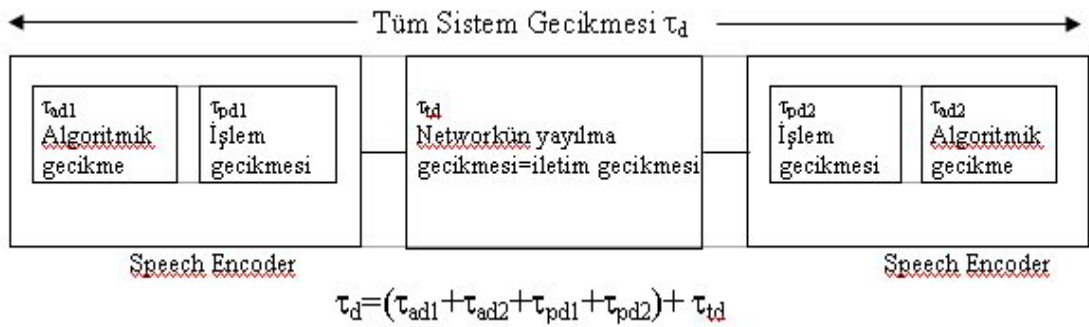
Sesin geliştirilmesi tasarımında göz önüne alınması gereken en önemli konulardan biri, iki uç nokta arasındaki tek yönlü gecikmenin en aza indirilmesidir. Ses trafiği

gerçek zamanlı trafiktir; ses paketinin iletiminde çok fazla gecikme olursa konuşma anlaşılmaz olur. Gecikme, ses şebekesinin bir parçasıdır ve çok sayıda farklı faktörden kaynaklanır.

Konuşma ve görüntü teknolojisi gerçek zamanlı bir trafik içerdiğinden zamana bağlı gecikmelere karşı oldukça duyarlıdır. Gecikmeler kodlama teknolojisinden, network ve iletişim altyapısından kaynaklanmaktadır.

ITU 96a Recommendation G.114'e göre izin verilen maksimum gecikme süresi 400 ms olarak tespit edilmiştir. Ancak gerçek hayatta ve interaktif bir konuşmada bu değer oldukça yüksek olarak değerlendirilmektedir. SQEG'e göre bu değer oldukça yüksek bulunmuştur ve tek yönlü gecikmenin 200 ms'nin altında olması gerektiği belirtilmektedir. Ses teknolojisindeki gecikmeler şu sebeplerden kaynaklanmaktadır:

- Algoritma ve kodlama işlemi için gereken gecikmeler. Bu gecikmelerin toplamı kodlama ve kodlamanın karşı taraftan çözülmesi için gereken zaman olarak düşünülmelidir.
- Network'ün durumuna bağlı olarak iletimde ve işlemde meydana gelen gecikmeler.



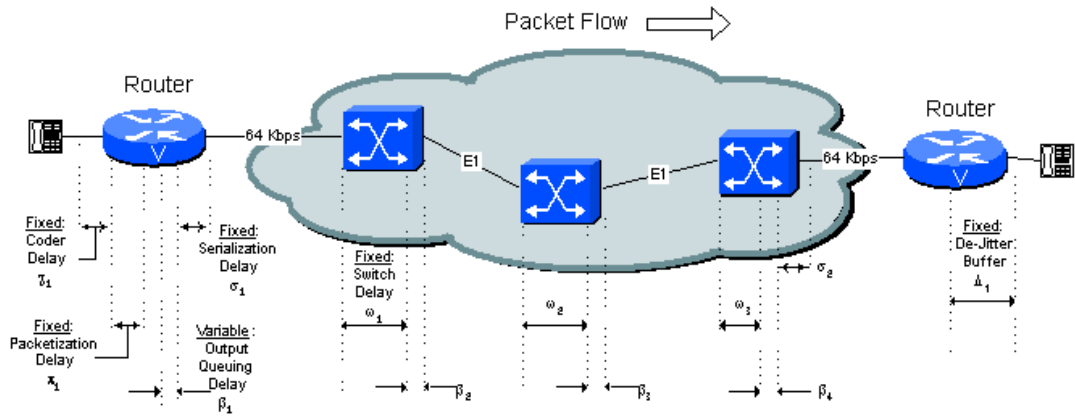
Şekil 6.1. Gecikme Kaynakları (1)

Bu durumda PSTN şebekesinde G.723.1 standardına göre gecikme süresi 97,5 ms olarak verilmektedir. Bu gecikmenin 37,5 ms'si algoritmada meydana gelen gecikmeler, 40 ms'si işlem için gereken zaman ve 20 ms ise iletimde meydana gelen

gecikmeleri kapsamaktadır. G723.1 standardı PSTN şebekelerinde görüntülü telefon standardı olarak kullanılmaktadır. İnternet ortamında ise bu süreler elbetteki daha uzun olacaktır. İnternet uygulamalarında en çok kullanılan standart G.729 olarak bilinen standarttır. Bu standarda göre kodlama için kaybedilen zaman yalnızca 25 ms olarak öngörülmektedir. İletimde meydana gelen kayıplar ise network durumuna ve kullanılan cihazların işlem kapasitesine göre değişimler göstermektedir.

### 6.2.2. İşlem Gecikmesi

İşlem gecikmesi (Coder Delay), kodlama işleminin kendisi ve kodlanmış örneklemelerin paket şebekesi üzerinden transmisyonu için bir pakete toplanmasından kaynaklanır. Kodlama gecikmesi, işlemci icra zamanı ve kullanılan algoritmanın her ikisinin de bir fonksiyonudur. Sıklıkla, paket şebekesi yükünü azaltmak için çoklu ses kodlayıcı frame'leri, tek bir pakette toplanır.



Şekil 6.2. Gecikme Kaynakları (2) (Cisco Systems, Voice Quality - Understanding Delay in Packet Voice Networks, 2004)

### 6.2.3. Network Gecikmesi

Network gecikmesi, ağdaki bağlantıların kapasitesinin ve ağ üzerinden geçirilen paketler üzerinde yapılan işlemlerin bir fonksiyonudur. (ARGE-TEK, 2004) Bir IP şebekesi (İnternet veya İnternet) üzerindeki gecikme, network trafiğindeki yoğunluk,



eişim isteyen kullanıcı sayısı, trafik tipi, transmision hızı gibi faktörlere bağılı olarak deęişir. ITU-T G.114, gecikme süreleri için ařağıdaki sınırları tavsiye etmektedir:

0 ile 200 ms arası: Coęu kullanıcı uygulamaları için kabul edilebilir.

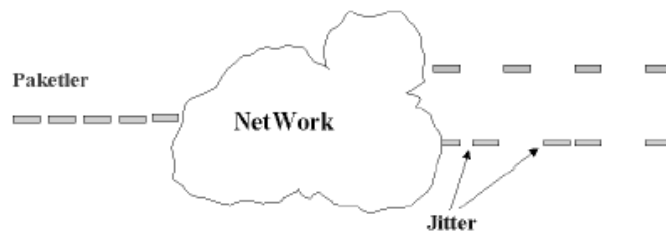
200 ile 400 ms arası: Sistem yöneticilerinin, kullanıcı uygulamalarının iletim kalitesindeki gecikme etkisinden haberdar olduęu sürece kabul edilebilir.

400 ms üzeri: Genel network planlama amaçları için kabul edilemez.

### 6.3. Gecikme Deęişiklikleri (Jitter)

Gecikme deęişiklikleri, belirli bir trafik akışında birbiri ardına gelen paketlerin deęişken karakterdeki gecikmelerinin ölçüsüdür. Gecikme deęişiklięinin ses ve video gibi gerçek zamanlı ve gecikmeye duyarlı uygulamalar üzerinde önemli etkileri olabilir. Söz konusu gerçek zamanlı uygulamalar paketleri sabit bir hızda ve aralarında sabit süreler olduęu halde almak isterler. Varış hızı deęişkenlik gösterdikçe uygulamanın performansı etkilenir. Gecikme deęişiklikleri minimum seviyede olduęunda sorun yaşanmayabilir, ancak arttıkça uygulama kullanılmaz hale gelecektir.

Paketler giriş arayüzü kuyruęına girdikçe, alındıkları sırayla uygun çıkış arayüzü kuyruęuna yerleştirilirler. Bu temel kuyruk metodu, sıklıkla FIFO (First In, First Out - İlk giren ilk çıkar) olarak tanımlanır. FIFO sıralaması, bir geliş arayüzünden bir çıkış arayüzüne trafięin depola-ve-yönlendir (store-and-forward) mantığıyla ele alınması amacıyla standart bir metod olarak varsayılır. VoIP içinde düşük QoS'e etki eden önemli faktörlerden ikisi, paket gecikmesi ve network jitter'idir. Network gecikmesi, bir paketin networkü ortalama geçiş zamanını tanımlar. Jitter, bir paketin varış zamanındaki deęişkenlięi tanımlar. Gecikme bir ortalamadır, jitter ise standart sapmadır. Her ikisi de ses kalitesinin tanımlanmasında önemlidirler.



Şekil 6.3. Jitter

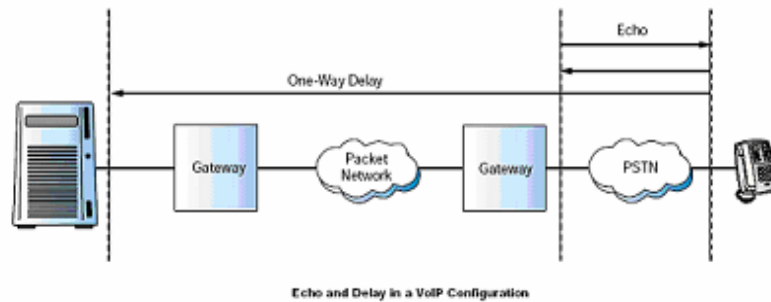
## 6.4. Network Sıkışması

Network sıkışmasının ortadan kaldırılması, VoIP için aşılması gereken en önemli konudur. Sıkışma ile ilgili problemlerden kaçınmak için, şebeke kaynakları rezerve veya garanti edilmelidir. Bir IP şebekesinde sıkışma; gecikme ve paket kayıplarına neden olur. Bir ses şebekesindeki fazla gecikmenin iki sonucu, eko ve konuşmaların üst üste binmesidir (talker overlap) .

### 6.4.1. Eko (Echo)

İki telli telefon kablosu, dört telli PBX arayüzü veya bir telefon santrali arayüzüne bağlandığında, iki teli dört tele çevirmek için hibrid adı verilen özel bir elektrik devresi kullanılır. Hibrid devreleri dönüşüm yeteneği açısından çok verimli olmakla birlikte, sinyal enerjisinin küçük bir yüzdesi dönüştürülmez ve araya geri döndürülür. Bu durum, eko olarak adlandırılır. Eğer arayan abone PBX veya santrale yakınsa, eko fark edilmeyecek kadar hızlı olarak geri döner. Bununla birlikte, gecikme 15 milisaniyeden daha uzun ise, arayan bir eko duyabilir. Bu durumu önlemek için VoIP gateway'leri, eko önleme (echo cancellation) özelliği sağlarlar.

IP şebekesindeki gecikmenin 50 milisaniyeden çok daha büyük olabilmesi ve bunun sonucunda uzak-uç hibriden gelen ekonun yakın uçta alınması nedeniyle, eko önleme VoIP üreticileri için özellikle önemlidir. Uzak-uç eko önleme, bu durumu ortadan kaldırmaktadır.



Şekil 6.4. VoIP konfigürasyonunda eko ve gecikme (The University of North Carolina, Voice over Internet Protokol – Quality of Service, 2004)

### 6.4.2. Konuşmaların Üst Üste Binmesi (Talker Overlap)

Şebeke gecikmesi 150 ms'yi aştığı zaman, iki konuşmacı yavaş yavaş birinin konuştuğu, diğerinin dinlediği ve konuşmacı bitirinceye kadar beklediği bir yarı-dupleks moda dönüşmeye başlar. Eğer aboneler bekleme süresini iyi ayarlayamazlarsa, birbirlerinin konuşmasını "kesmeye" başlarlar.

IP şebekeleri, paketlerin tamamının iletilmesi ve hatta doğru sırayla iletilmesinde bir garanti veremez. Paketler, aşırı yükte ve sıkışma (örneğin, link hataları veya uygun olmayan kapasiteden kaynaklanan) zamanlarında silinir. Bir abone, tek bir ses paketi kaybını farketmez, bununla birlikte yetersiz bandgenişiği nedeniyle peş peşe birkaç paketin atılması, kabul edilemez bir seviyede bozulmaya neden olabilir.

### 6.4.3. TCP Sıkışma Kontrolü

Sıkışma (Congestion), datagram'ların bir veya daha fazla anahtarlama noktasında aşırı yüklenmesinden kaynaklanan ciddi gecikmenin bir nedenidir. Son noktalar, genellikle sıkışmanın nerede ve neden olduğunun detaylarını bilmezler. Son nokta açısından, bu sadece artan gecikme demektir. Maalesef, çoğu transport protokolü, zaman aşımı ve tekrar transmisyonu kullanır, böylece sıkışmaya karşı daha fazla datagram göndererek tepki verirler. Sıkışmadan kaçınmak için, mevcut TCP standardı, iki teknik önerir; Çarpmalı Azaltma (Multiplicative Decrease) ve Yavaş - başlama (Slow-start).

Sıkışmayı kontrol etmek için TCP, pencere (Window) boyutunu Çarpmalı Azaltma (Multiplicative Decrease) adı verilen bir süreçten azaltır. Eğer onaylama (acknowledgement) alınmazsa, TCP pencere boyutunu yarı yarıya azaltır. Bu işlemden sonra oluşan her kayıpta pencere boyutunu üstel olarak azaltılır ve işlem, minimum bir segment olana kadar tekrarlanır. Sıkışmanın sonunda TCP, Yavaş-başlama (Slow-start) adı verilen bir metot ile kendini toplar. Başlangıç pencere boyutu, tek bir segment'tir. Başarılı bir onaylama alınmasıyla pencere boyutu iki

katına çıkarılır. Bu iki katına çıkarma işlemi, pencere boyutu maksimum sınırına ulaşına kadar her başarılı onaylama ile devam eder.

## 6.5. Kayıplar

Fiziksel iletim ortamında hatalar oluşması ile kayıplar meydana gelebilir. Örneğin, BER (Bit Error Rate - Bir Hata Oranı) ölçümlerine göre karasal hatların büyük çoğunluğunda kayıp oranı oldukça azdır. Ancak, uydu, mobil ya da sabit kablosuz ağlar gibi kablosuz bağlantılarda BER oranı çevresel faktörler ile sis, yağmur, RF karışması, dolaşım sırasındaki hücre atlama gibi şartlara; ağaçlar, binalar ve dağlar gibi fiziksel engellere göre değişiklikler gösterebilir.

### 6.5.1. Kayıp Paket Telafisi

Bir paket şebekesindeki kayıp ses paketleri, serviste ciddi bir bozulma yaratabilir. Mevcut IP şebekelerinde, tüm ses frame'leri veri olarak işlem görür. Aşırı yüklerde ve sıkışma altında, ses frame'leri veri frame'lerine eşit olarak işlenir ve duruma göre silinebilir. Bununla birlikte, veri frame'leri, zamana karşı duyarlı değillerdir ve düşürülen veri paketleri, tekrar gönderme süreci üzerinden uygun olarak düzeltilebilirler. Ancak, kayıp ses paketleri, bu şekilde kurtarılamaz.

Kayıp frame'ler problemi ile ilgili olarak yazılım tarafından kullanılan bazı yapılar şunlardır:

Kayıp paketin hedef abone tarafından dinlenildiğinin varsayıldığı süre boyunca alınan son paketin yeniden çalınmasıyla kayıp konuşma paketleri için araya eklemek. Bu yapı, sürekli olmayan frame'ler arasındaki zamanı dolduran basit bir metottur. Kayıp frame olaylarının sık sık olmadığı durumlarda iyi çalışır. Bir sıra boyunca bir kaç tane kayıp paket varsa iyi çalışmaz. Bandgenişliği kullanımını göze alarak fazladan bilgi gönderilmesi. Temel yaklaşım, ses bilgisi paketinin n'inci paketini (n+1)'inci paket boyunca çoğaltır ve gönderir. Bu metodun kayıp paket için kesin olarak düzeltme olasılığı avantajı vardır. Bununla birlikte bu yaklaşım, daha fazla bant genişliği kullanır ve daha çok gecikme yaratır.

## 6.6. İletim Öncelikleri

İletim önceliği ağ modülünden çıkmakta olan trafiğin hangi sırada iletileceğini belirler. İletim önceliği olan trafik, iletim önceliği olmayandan daha önce iletilir. İletim öncelikleri, ağ modüllerinin kuyruklama mekanizmalarının trafiğe getireceği gecikme miktarlarını da belirlemektedir. Örneğin, e-posta gibi gecikmeyi tolere edebilecek olan uygulamalar, ses ve video gibi gecikmeye hassas olan gerçek-zamanlı uygulamalardan daha düşük iletim önceliğine sahiptirler. Gecikmeye hassas olmayan bu uygulamalar, gecikmeye hassas uygulamalar iletimde iken kuyrukta bekletilebilirler.

En basit şekliyle iletim öncelikleri, yüksek öncelikli trafiğin her zaman düşük öncelikli trafikten önce iletildiği basit iletim öncelik yapısını kullanırlar. Bu işlem tipik bir öncelik planlama (kuyruklama) özelliği ile gerçekleştirilmektedir. Bu yaklaşımın en zayıf yönü, bandgenişliği sınırlaması olmayan ortamda yüksek öncelikli iletimin gönderilerek, düşük öncelikli iletimlerin hiçbir zaman gönderilememe riski olmasıdır.

### 6.6.1. IP Önceliği

IP önceliği (precedence), trafiğin farklı servis sınıflarına bölünmesi yeteneğini sağlar. IP önceliği özelliği, her paket için servis atanmasında bir sınıf tanımlamak için IP başlığındaki Servis Tipi (Type of Service - TOS) alanını kullanır. IP önceliği, varolan uygulamalarda değişiklik yapmadan ve karmaşık şebeke sinyalleşme gerekmeden servis sınıflarının kurulmasını etkinleştirir. Bir Router'ın IP datagram'ları işleminde öncelik verebilmesini sağlamak amacıyla bir öncelik mekanizması tanımlamak için TOS alanı kullanılabilir.

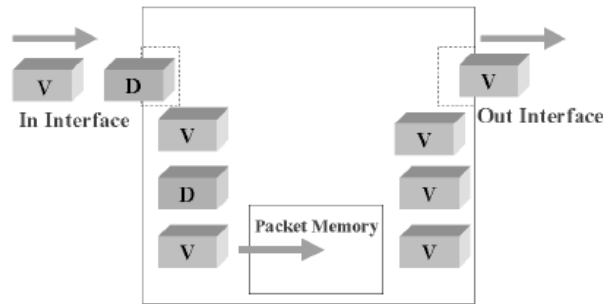
### 6.6.2. Öncelik Sıralaması – Tamponlama

Akıllı tampon yönetimi, gecikme kontrolü için önemli bir mekanizmadır. Veri uygulamaları için, FIFO yapısı genellikle en uygun olarak görülür. Bununla birlikte ses, veriye nazaran gecikmeye karşı daha hassastır. Bu nedenle, hem erişim

cihazlarında hem de network içinde kullanılacak bir öncelik sıralama metodu, paket anahtarlama şebeke üzerinden sesin başarıyla iletilmesi açısından önemli bir faktördür.

Verilerin tamponlanması, ağ üzerinde gecikmeyi engelliyerek, uygulamaların kesintisiz akışını sağlar. Trafik, tamponlamayı değişken oranda devreye sokar fakat düzenli oranda geri teslim eder. Ancak, büyük tamponlama gönderici ve alıcı arasında büyük gecikme anlamına gelmektedir. İnsan kulağı 150 milisaniye hızdaki veriyi algılayabilir. Buna karşılık MAN bağlantıda iletimde gidiş-geliş ortalama gecikme 50 milisaniye dolayındadır. Bu nedenle iki yönlü iletimde her yön için iletimin 50 milisaniyeden daha fazla olmaması gerekir.

Öncelik Sıralaması (Priority queuing), belli trafik tiplerinin tanımlanması ve çıkış kuyruğunun önüne konması kavramını temel alır. Çıkış kuyruğundaki tercih sırasını gösteren yüksek (high), orta (medium), alçak (low) gibi öncelik seviyesi mevcuttur. Bu sıralama yaklaşımının olası bir dezavantajı, yüksek öncelikli trafiğin hacminin alışıksız şekilde yükselmesi halinde, tamponun dolması nedeniyle sırada bekleyen normal trafiğin silinmesidir.



Şekil 6.5. Öncelik Sıralaması

## 6.7. Atılım Öncelikleri

Atılım öncelikleri hangi iletimin devre dışı bırakılacağını belirlemektedir. Trafik, ağ modülündeki tıkanıklık ya da trafiğin belirlenmiş olan profilinin dışına çıkması

durumlarında (trafiğin belirlenmiş olan bandgenişliğini belirli bir süre için aşması gibi) devre dışı bırakılır. Tıkanıklık durumunda, yüksek atılım önceliği olan trafik, düşük atılım önceliği olandan daha önce devre dışı bırakılır. Benzer QoS performans gereksinimleri olan trafikler atılım önceliklerine göre alt gruplara ayrılabilirler. Böylelikle, iletimin ağ modülündeki tıkanıklık durumunda aynı performans seviyesinde kalması sağlanmış olur.

### **6.8. Konuşma Kalitesinin Ölçümü**

ITU içinde bir çalışma grubu olarak yer alan SQEG (Speech Quality Expert Group) tarafından konuşma kalitesinin ölçümü için bir dizi test yöntemi geliştirilmektedir (ITU 96k ve ITU 961 gibi). ITU tarafından geliştirilen ve genellikle kullanılan test yöntemine ACR (Absolute Category Rating – Mutlak Kategori Oranı) adı verilmektedir. Bu yöntem ile test yapılacak standartlar gerçek test ortamında belirli bir süre teste alınmaktadır. Bu zaman içerisinde rasgele seçilen konuşmalar 8 ile 10 saniye arasında dinlenmekte ve konuşma kalitesi ölçülmektedir. Her ölçüm sonunda 1 ile 5 arasında konuşma kalitesi notu verilmektedir. Bu süreç belirli bir süre tekrarlandıktan sonra gerçek konuşma kalitesinin ortalama değeri hesaplanmaktadır. 1 ile 5 arasında verilen bu değere Ortalama Kanı Skoru (MOS – Mean Opinion Score) adı verilmektedir. Her codec, belli bir ses kalitesi sağlar. Üretilen ses kalitesini tanımlamak için kullanılan bir ortak karşılaştırma kriteri, MOS'dur.

Konuşma kalitesindeki 1 değeri en kötü durumu, 5 değeri ise en iyi durumu ifade etmektedir. MOS'un 3'ün üzerindeki değerleri ses kalitesi açısından kabul edilebilir bulunmaktadır. MOS'un 4'ün üzerinde olması ise kaliteli bir ses kodlamasını ve transferini ifade etmektedir. Yeni geliştirilen konuşma kodlama tekniklerinin MOS değerlerinin 4'ün üzerinde olmasına dikkat edilmekte ve çalışmalar bu yönde sürdürülmektedir. Aşağıdaki çizelgede bazı kodlama standartlarının MOS değerleri verilmektedir.

Çizelge 6.1. Kodlama/Sıkıştırma yöntemlerinin karşılaştırılması

Sıkıştırma Yöntemi	Bit Oranı (kbps)	Frame Boyu (ms)	MOS Değeri
G.711 (PCM)	64	0,125	4,1
G.729 (CS-ACELP)	8	10	3,92
G.729 x 2 Encoding	8	10	3,27
G.729 x 3 Encoding	8	10	2,68
G.729a CS-ACELP	8	10	3,7

### 6.9. Rastgele Erken Sezme (Random Early Detection - RED)

Daha önce bahsedilen TCP sıkışmasını önleyici metotları ilk kez Van Jacobson 1988'de incelemiştir. Van Jacobson ve Sally Floyd, 1993'te Rastgele Erken Sezme (Random Early Detection - RED) kavramını dokümanete etmiştir. RED, tam bir sıkışma çökmesinden kaçınmak için, keyfi seçilen akışlardan rastgele paketleri düşüren bir mekanizma sağlar. RED'in prensibi, tüm TCP akışının aynı anda sıkışmayla karşılaşması ve sonraki paketlerin kaybedildiği bir durumdan kaçınmaktır. RED kuyruk derinliğini takip eder ve kuyruk dolmaya başladığında, üzerinden paket düşürülecek TCP akışlarını rastgele seçer. RED'in paket düşürmeye başlayacağı eşik seviyesi ve kuyruğun ne kadar hızla dolduğuna bağlı olarak yapılacak paket düşürme oranı, genellikle network yöneticisi tarafından ayarlanır. Kuyruk ne kadar çok dolarsa, o kadar çok sayıda akış seçilir ve o kadar çok sayıda paket düşürülür.

RED'in üzerinden paket atılacak akışları rastgele seçmesinden dolayı adil olduğu söylenebilir. RED için ağırlıklı davranış sağlayan birden fazla mekanizma vardır. Bunlardan biri RED'in varyantıdır ve sıkışma zamanlarında trafiğin ayırt edilmesi için istenen sonucu sağlar. Bu metot Ağırlıklı Rastgele Erken Sezme (Weighted Random Early Detection) olarak adlandırılır.



### **6.9.1. Ağırlıklı Öncelik (Weighted Precedence)**

#### **6.9.1.1 Ağırlıklı RED (Weighted RED – WRED)**

WRED, farklı servis sınıfları için farklı performans karakteristikleri sağlamak için IP Önceliği ile RED yeteneklerini bir araya getirir. Böylece daha yüksek öncelikli paketler için tercihli trafik uygulaması oluşturulur. WRED, ayrıca sıkışma koşulları altında sıkışmayı daha da arttırmadan tercihli trafik uygulanmasını sağlar. Network operatörlerinin minimum ve maksimum kuyruk derinliği eşiklerini ve her servis sınıfı için düşme olasılıklarını tanımlama esneklikleri vardır.

#### **6.9.1.2. Ağırlıklı Adil Kuyruklama (Weighted Fair Queuing – WFQ)**

WFQ, düşük gecikme gerektiren yüksek öncelikli trafik için hızlı iletişim sağlar. Geriye kalan bandgenişliği, düşük öncelikli trafik kaynakları arasında paylaşılır. WFQ, IP önceliği ve trafik hacmi gibi parametrelere dayanarak link trafiğini yüksek öncelik ve düşük öncelik akışlarına böler. Yüksek öncelikli akımlar hemen servis alırlar. Düşük öncelikli akımlar, kalan bandgenişliğinden oransal pay alır ve sıkışma zamanlarında düşük öncelikli akımlardan paketler düşürülebilir.

### **6.10. Rezervasyon Protokolü (Reservation Protocol - RSVP)**

RSVP, bir uygulama veri akışı için uçtan-uca belirli kalitede servis istemek için kullanılır. Bir host, veri kaynağından gelen belli bir veri akışı için networkten özel bir QoS istemek amacıyla RSVP kullanır. Aynı zamanda yönlendiriciler tarafından, veri akışının geçeceği yol üstündeki tüm düğümlere QoS isteklerinin iletimi, istenen servisin sağlanması için gerekli koşulların oluşturulması ve korunması amacıyla kullanılır. RSVP istekleri genellikle akışın geçeceği yol üzerinde istenilen kaynakların rezerve edilmesi ile sonuçlanır. (Varol, 1999) Alıcı ile gönderici arasındaki tüm host'lar, router'lar ve diğer network yapı elemanları RSVP desteklemek zorundadır. Her biri, QoS isteğini karşılamak üzere bandgenişliği, CPU

ve bellek tamponları gibi sistem kaynaklarını rezerve ederler. Bu nedenle, ISP'ler RSVP QoS rezervasyonları için yüksek ücret talep ederler.

Bilgisayar ağına yüksek-öncelikli veriyi göndermeden önce işaretleme yerine, bir özel oturum için ağ kapasitesinin bir bölümünü yedek olarak saklanması, RSVP'nin bir uygulamasıdır.

RSVP'nin dezavantajı, bu paketlerin bir öncelik sırasında analizi ve işlenmesi amacıyla router'lar için bilgi işleme kaynaklarının gerekmesidir. Bunu kolaylaştırmak için etiket anahtarlama gibi yaklaşımlar halen geliştirilmektedir. Bir başka araştırma alanı, alternatif ve sabit yollar sağlayan yönlendirme servislerini kullanmak için RSVP'nin genişletilmesidir.

#### **6.10.1. RSVP Çalışması**

RSVP QoS kontrol istek mesajları, kaynakların rezerve edilmesi için tüm düğümlere (router ve host'lar) iletim hattı boyunca gönderilir. RSVP'nin alıcı tarafından başlatıldığına dikkat edilmelidir. RSVP, sadece bir yönde istekte bulunur. Multicast için, rezervasyon isteğinin sadece aynı kaynak akış için başka bir rezervasyonla birleşeceği bir noktaya gitmesi gerekir. Bu alıcı-temelli tasarım, geniş multicast gruplar ve dinamik grup üyeliği oluşturmak için kullanılmaktadır.

Alıcı - Gönderici hattı boyunca her düğümde, RSVP istenen akış için bir kaynak rezervasyonu yapmaya çalışır. Her ara düğümde bir istek için iki genel işlem yapılır. Bunlar, bir rezervasyon yapılması ve isteğin üst akışa yönlendirilmesidir.

İstek, kabul ve politika kontrollerine göre yerine getirilir veya reddedilir. Bu kontroller, RSVP'nin bir parçası olmayan ve geri planda bulunan bütünleşik servisler mekanizmalarından gelen bilgileri kullanır. Rezervasyon reddedilirse, RSVP uygun alıcılara bir hata mesajı geri döndürür.

Rezervasyon isteđi, üst akışlar boyunca uygun göndericilere doğru düğümlere yayınlanır. RSVP ayrıca, sistemlerin kaynakları bırakmasını sağlayan çözme mesajlarını da tanımlar.

RSVP, protokol yığındaki transport protokolünün yerini kullanır ancak bu arada oturum katmanı (session layer) servislerini de sağlar ve IP'nin (IPv4 veya IPv6) üstünde çalışır (herhangi bir veri göndermez). RSVP, bir İnternet kontrol protokolü (IGMP veya ICMP gibi) olup, bir yönlendirme protokolü değildir.

### **6.10.2. RSVP Sınırlamaları**

Orijinal RSVP, geniş networkler için fazla uygun değildir. Çeşitli trafik akışları için kaynakların rezerve edilmesi, tüm WAN router'ları ve diğer Katman 3 linkleri boyunca her akış için "durum" bilgisinin (oturum ayarları ve bandgenişliği bilgisi gibi) korunması demektir. Bu durum, kaynaklara ek trafik için kapasiteyi azaltacak olan büyük bir yük oluşturabilir.

RSVP'yi daha gerçekçi yapmak için bir kaç öneri vardır. Bu önerilerden biri, akışları 802.1 ve diğer "öncelik" sistemlerine eşlemek için bir mekanizmayı içermektedir. Gelişmeler, bir RSVP istemcisinin network cihazlarını yeni bir akışı desteklemek için hangi sınıfların uygun oldukları ve o anda kapasitenin geçerli olup olmadığını sorgulamasını mümkün kılacaktır. Ayrıca, bandgenişliği yöneticisi adı verilen bir bileşen de, yeni bir akışı sağlamak için çeşitli alt networkler boyunca yeterli bandgenişliği olup olmadığını belirlemeye yardımcı olabilir.

Bu gelişmeler, bandgenişliğini yönetmek amacıyla RSVP'ye politika bilgisini vermek isteyen network yöneticileri için büyük bir yardım olacaktır. Ayrıca her router'da RSVP yerine (daha fazla idari karmaşıklık nedeniyle) Diffserv (RSVP'ye göre daha düşük işlem yükü nedeniyle) desteklemeyi tercih eden servis sağlayıcılar için de uygun bir çözüm sağlanmış olacaktır.

## **6.11. Çoklu Protokol Etiket Anahtarlama (Multiprotocol Label Switching - MPLS)**

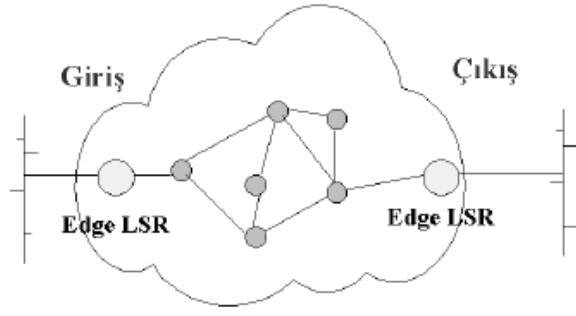
IETF, 1997'de bir çalışma grubu oluşturmuştur ve birçok tartışmadan sonra, "Multiprotocol Label Switching" terimi, üreticiden bağımsız standart olarak seçilmiştir. MPLS uygulamaları olarak ATM-temelli WAN'larda IP şebekelerinin kullanılması, paket-temelli networklere trafik-mühendisliği sağlanması, IP QoS sağlama ve IP-temelli Sanal Özel Networkler'in (VPN-Virtual Private Networks) kullanılması gösterilebilir.

### **6.11.1. MPLS Çalışması**

MPLS'de, IP paketleri, networke girdikleri ilk MPLS cihazı tarafından bu etiketlerle 'paketlenirler' (encapsulated). MPLS uç router'ı, IP başlığının içeriğini analiz eder ve paketin başlığına eklenecek uygun bir etiket seçer. MPLS'in etkisi, mevcut IP yönlendirmenin tersine, bu analizin sadece IP başlığında taşınan hedef adresinden daha fazlasının temel alınarak yapılması gerçeğinden kaynaklanır. Network içindeki tüm alt networklerde paketin yönlendirme kararının verilmesinde IP başlığı değil, MPLS etiketi kullanılır. En sonunda, MPLS etiketli paketler networkü terk ederken başka bir uç router'ı etiketleri çıkarır.

MPLS terminolojisinde, paket işleyen node veya router'lar, Etiket Anahtarlama Router'lar (Label Switched Routers - LSR) olarak adlandırılır. MPLS router'lar, paketleri MPLS etiketini temel alarak verilen anahtarlama kararıyla yönlendirirler.

LSR'nin iki geniş kategorisi vardır. Network ucunda, istenen etiketleri uygulayan (veya çıkararak) yüksek performanslı paket sınıflandırıcılarına ihtiyaç vardır ki bunlar, MPLS uç router'ı (MPLS edge routers) olarak adlandırılır. Merkezdeki LSR'lerin etiketlenmiş paketleri çok yüksek band genişliklerinde işleme yeteneğinde olması gerekir.



Şekil 6.6. Networkün giriş ve çıkışında bulunan LSR'ler  
(Etiket Anahtarlama Router'ları)

## 7. IP ÜZERİNDEN SES HABERLEŞMESİNDE SERVİS KALİTESİNE ETKİ EDEN PARAMETRELERİN ANALİZİ İÇİN KULLANILAN TEKNİKLER VE TEST SONUÇLARI

### 7.1. Kullanılan Test Programı

#### 7.1.1. NetMRG

NetMRG programı SNMP ile alınan aygıt bilgilerini RRDtools yardımı ile grafik haline dönüştüren ve verileri veritabanında saklayan bir PHP arayüz programıdır. Programın özelliği, network üzerindeki cihazlardan (Şekil 7.1) belirtilen network aygıtı üzerinden SNMP ile hangi verilerin alınacağını göstermek (Şekil 7.2) ve bu aygıtlardan gelen bilgileri veritabanında saklayarak istenildiği zamanda grafiklere dönüştürmektir (Şekil 7.3).



Şekil 7.1. Data Alınacak Cihaz/ların Seçildiği Menü

Standart ayarlar içerisinde bu grafikleme işlemi günlük, haftalık, aylık ve yıllık olmak üzere (Şekil 7.4) dört şekilde sürekli olarak oluşturulmaktadır. İstenildiğinde kendi belirlemiş olduğumuz zaman aralıklarındaki verileri de saatlik olarak grafikleme imkanı da sunmaktadır.

**NetMRG** Generic Company  
Logged in as admin

<b>Monitoring</b>	History : All Groups : AKILLI SINIF Sub-Devices for AKILLI SINIF		
Groups	<b>Sub-Devices</b>	<b>Type</b>	<b>Add</b>
Device Types	Ethernet/1	Interface	<Parameters> <View> <Duplicate> <Edit> <Delete>
Notifications			
<b>Reporting</b>			
Device Tree			
Event Log			
Slide Show			
<b>Graphing</b>			
Custom Graphs			
Template Graphs			
<b>Tests</b>			
Scripts			
SNMP			
SQL			
<b>Admin</b>			
Users			
Prefs			
Logout			
<b>Help</b>			
About			

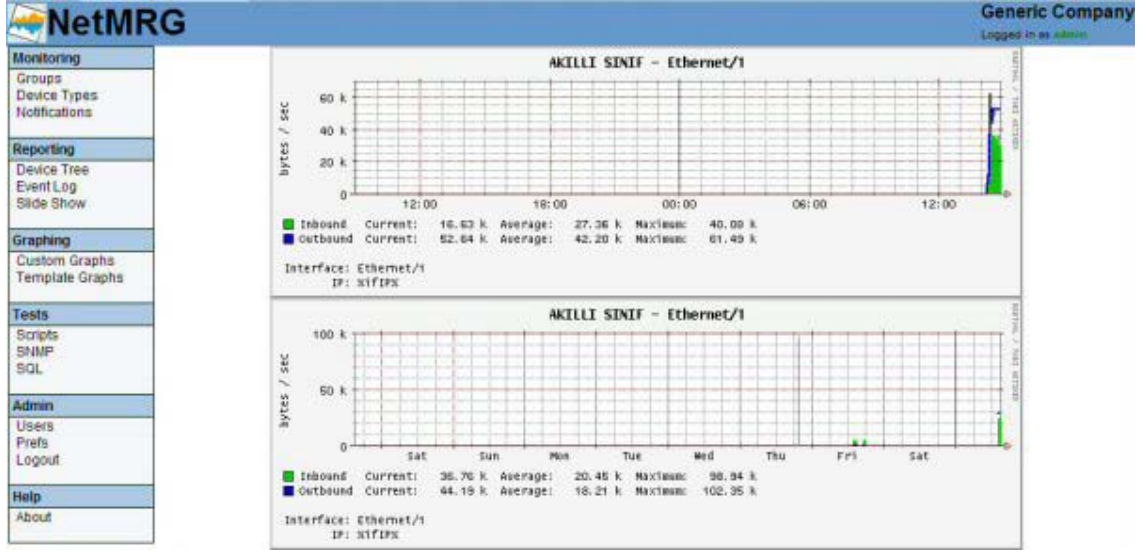
Şekil 7.2. Veri Alınacak Cihazın Interface'i

Verilerin grafiklere dönüştürülme işlemleri 5'er dakikalık aralıklarla gerçekleştirilmektedir, ancak bu zaman aralığı istenildiği gibi değiştirilebilir.

**Monitors for AKILLI SINIF - Ethernet/1**

Test	Data	Graph	Add
UCD - Load Average - 1 min	Value: 0.00 Rate of Change: 0.00 Time Stamp: 2004-05-16 14:50:02		<Edit> <Delete>
UCD - Load Average - 5 min	Value: 0.00 Rate of Change: 0.00 Time Stamp: 2004-05-16 14:50:02		<Edit> <Delete>
UCD - Load Average - 15 min	Value: 0.00 Rate of Change: 0.00 Time Stamp: 2004-05-16 14:50:02		<Edit> <Delete>
Open TCP Connections	Value: 0.00 Rate of Change: 0.00 Time Stamp: 2004-05-16 14:50:02		<Edit> <Delete>
Interfaces - Bytes Out	Value: 98.28 M Rate of Change: 52.64 k Time Stamp: 2004-05-16 14:50:02		<Edit> <Delete>
Interfaces - Bytes In	Value: 69.30 M Rate of Change: 29.11 k Time Stamp: 2004-05-16 14:50:02		<Edit> <Delete>
Interfaces - Errors In	Value: 0.00 Rate of Change: 0.00 Time Stamp: 2004-05-16 14:50:02		<Edit> <Delete>

Şekil 7.3. Interface Üzerinden Alınan Tüm Değerler



Şekil 7.4. Alınan Değerin Saatlik, Haftalık ve Aylık Detaylı Gösterimi

### 7.1.2. Programın Kullanıldığı Platform

Program Linux İşletim Sistemi kullanan bir bilgisayar üzerine kurulmuştur. Bilgisayarın özellikleri; Celeron 300A işlemci, 128MB Ram ve 100Mbit'lik bir ethernet kartı. İşletim sistemi üzerinde kullanılan programlar ise; PHP 4.3 yorumlayıcı, Apache Web Sunucusu, SNMP V2 istemcisi (snmpwalk). Veri tabanı olarak, MYSQL kullanılmıştır. Bilgisayar, veri kayıplarının minimuma indirilmesi için, cihaz ile aynı switch üzerine bağlanmıştır.

### 7.1.3. Yardımcı Programlar

#### 7.1.3.1. RRDtools (Round Robin Database)

RRDtools programının temel olarak işlevi, SNMP ile alınan sayısal değerleri matematiksel işlemlerden geçirerek grafik haline getirmektedir. RRDtools programının grafik işlemi yapabilmesi için iki veriye ihtiyaç vardır. Bu verilerden birincisi, x eksenini oluşturacak olan zaman (dakika, saat, gün yada ay değerleri), diğer veri ise y eksenini oluşturacak olan ve bizim cihazdan aldığımız veridir. Bu



ikinci deęer, yani y eksenini oluřturan veri, bizim aldığımız deęere baęlı olarak deęiřmektedir.

### **7.1.3.2. SNMP – Simple Network Management Protocol (Basit Aę Yönetim Protokolü)**

1988'de, IAB (Internet Activities Board – İnternet Etkinlikleri Yönetim Kurulu), tek bir NMS (Aę Yönetim Sistemi – Network Management System)'den çok üreticili bir network yönetimde oluřan problemi fark etti ve SNMP (Simple Network Management Protocol) geliřtirildi. (Netař/Nortel Networks, 2000) Network elemanlarının üreticiden baęımsız bir Network Yönetim Sistemi'nden yönetilmesine izin veren Basit Network Yönetim Protokolüdür. IP geçitleri ve aęlarının izlenmesi için kullanılır. SNMP sisteminin en büyük avantajı, elemanların grafikler kullanılarak yönetilebilmesidir.

SNMP aslında aę üzerinde bulunan birimler hakkında bilgi toplamak amacıyla geliřtirilmiř kurallar dizisidir. Aynı zamanda birimlerin ortaya çıkan sorunu yönetim istasyonuna ne řekilde bildireceklerine iliřkin bir metot da içermektedir. SNMP mimarisinde iki ana öęe bulunmaktadır: ajan (agent) ve yönetici. Ajan, sunucuya yönetici de, istemciye karřılık gelmektedir. Bir SNMP yönetim istasyonu, aę birimleri üzerinde bulunan ajanlarını sorgulayarak aę iliřkin bilgileri toplar. Bu iřlemin ardından SNMP yönetim istasyonu aę yöneticisine, aęa iliřkin analizleri yapabilmesi için gerekli bilgileri sunar. SNMP protokol grubunda yer alan protokoller řunlardır.

- Structure and Identification of Management Information (SMI)
- Management Information Base (MIB )
- Simple Network Management Protocol (SNMP)

**Yönetim bilgi tabanının yapı ve tanımlamaları (SMI):** SMTP veri tabanı temsilcilerinin yapısını belirler. Bir veri tabanı yapısı oluřturulurken karar verilmesi gereken ilk řey veritabanının yapısıdır.

**Yönetim bilgi tabanı (MIB):** Bir MIB herhangi bir SNMP veritabanında bulunan nesnelere ve girişleri tanımlamaktadır. Bu nedenle SNMP temsilcileri bazen MIB ismiyle de tanımlanmaktadır. MIB tanımlamaları standart, deneysel ve özel MIB olmak üzere üç kategoridedir.

- **Standart MIB:** Internet Standart Group tarafından da onaylanmış nesne türlerini kapsar. İlk standart MIB'ler; MIB I ve MIB II, IP router'ların yönetimi için tasarlanmıştır. RMON (Remote Monitoring) MIB I de internet topluluğu tarafından standart bir MIB olarak onaylanmıştır. RMON MIB II'ye göre biraz farklı bir işlemi yerine getirmek üzere tasarlanmıştır. RMON içinde ağ iletim ortamının izlenmesi amacıyla kullanılacak nesnelere bulunmaktadır. RMON MIB I kullanılarak bir ağ segmentindeki paket trafiği, segmentin kullanım yüzdesi, hatalı paket sayısı gibi bilgiler alınabilmektedir. Aynı zamanda RMON kullanılarak SNMP ajanı bulunmayan birimler de izlenebilmektedir.
- **Deneysel MIB:** Bu kategoriye giren MIB'ler içerisinde ağ ve ağ birimlerinin yönetimine ilişkin daha birime özel (diğer MIB'lerde bulunmayan) tanımlamalar bulunmaktadır.
- **Özel MIB:** Bu MIB'ler ağ konusunda çalışan firmalar tarafından geliştirilmekte ve üreticinin kendi ağ birimlerine ilişkin özel bilgiler toplamak amacıyla kullanılmaktadır. Bu MIB'ler içindeki nesnelere üretici tarafından tanımlanmaktadır.

**Simple Network Management Protocol (SNMP):** Network elementleri ve network yönetim istasyonları arasındaki protokolü tanımlar.

#### 7.1.4. NetMRG İle Grafiklenen Değerler

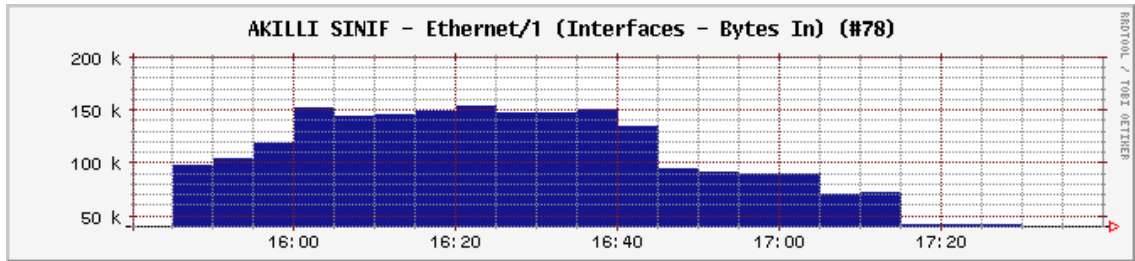
Test aşaması için NetMRG yardımı ile 3 temel veri alınmıştır. Bu veriler; cihaza gelen ve giden paketlerin miktarı (Interface Bytes in ve Interface Bytes out), gelen ve giden paketlerdeki hatalar (Errors in ve Errors out) ve son olarak da 1, 5 ve 15 dakikalık yük miktarı (Load Average 1, Load Average 5 ve Load Average 15). “Interface Bytes In” ve “Interface Bytes Out” değerlerinden faydalanılarak

“Bandgeniřliđi” bilgilerine ulařılabilmektedir ve bu deđerler yardımıyla “Bandgeniřliđinin” nasıl kullanıldıđı hakkında bilgi elde edilmektedir.

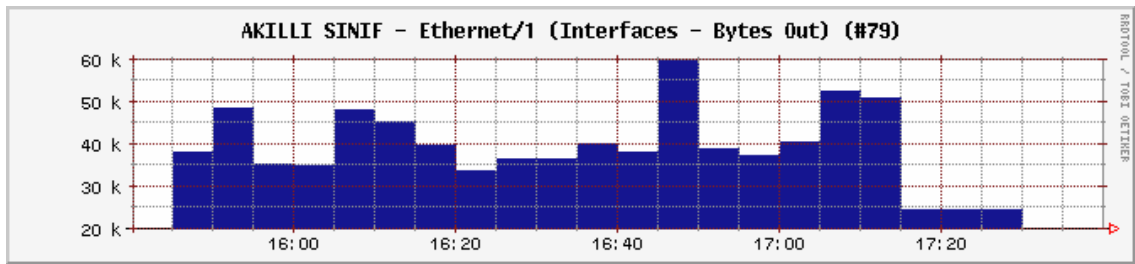
$$\text{Bandgeniřliđi} = \text{Interface Bytes In} + \text{Interface Bytes Out}$$

## 7.2. Uzak Noktadaki Test Sonuları

Bu uygulama Sleyman Demirel niversitesi ile Orta Dođu Teknik niversitesi arasında Akıllı Sınıf aracılıđıyla gerekleřtirilen bir bađlantı sırasında gerekleřtirilmiřtir. İki saat boyunca kaydedilen deđerler ařađıda sunulmuřtur:

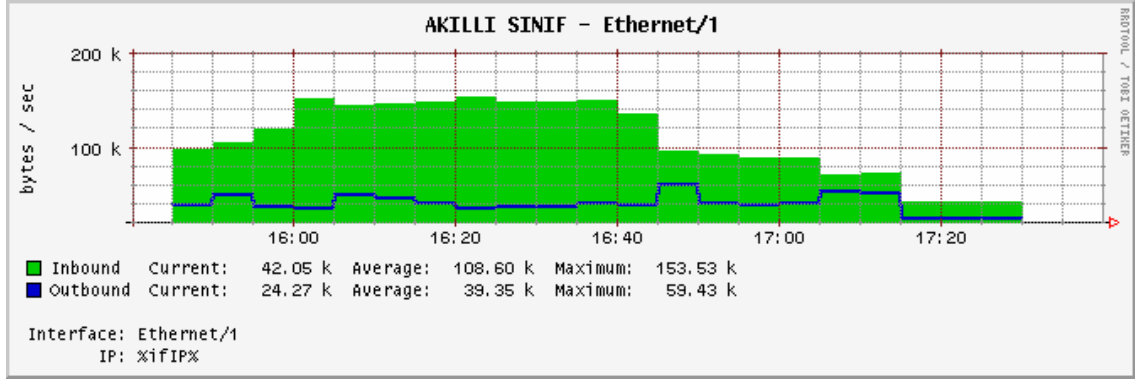


řekil 7.5. Bytes In Grafiđi-1



řekil 7.6. Bytes Out Grafiđi-1

Test ařamasında maksimum 153,53 k giriř deđeri ve maksimum 59,43 k deđerinde ıkıř llmřtr. Ortalama olarak 108,60 k deđerinde giriř ve 39,35 k deđerinde ıkıř elde edilmiřtir.

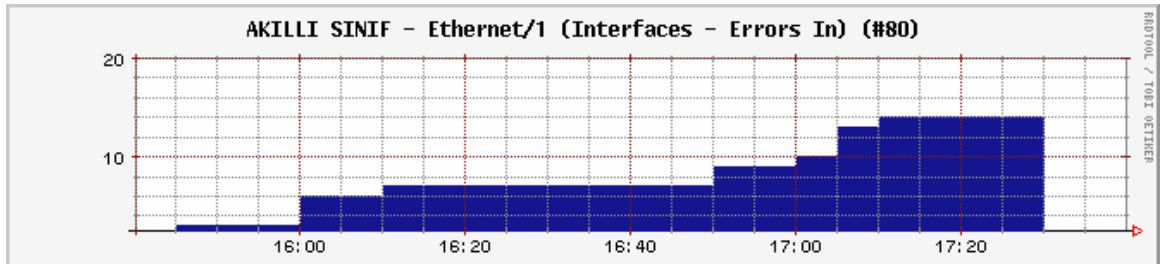


Şekil 7.7. Bytes In ve Bytes Out Grafiği-1

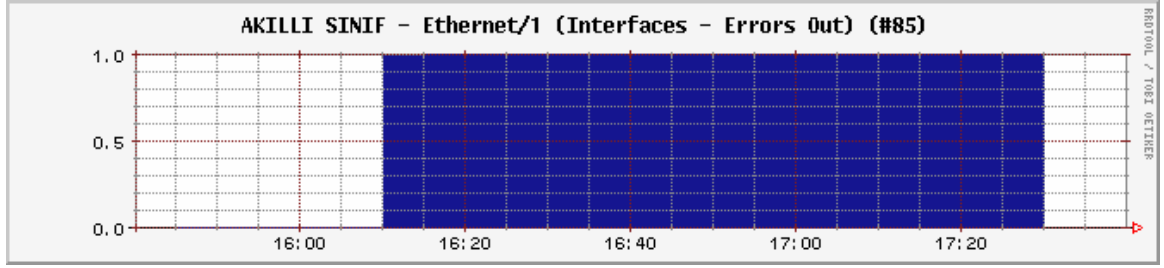
Şekil 7.7’de görülen grafikte giriş ve çıkış trafiği beraber görülmektedir. Yeşil kısım, giriş trafiğini gösterirken, mavi kısım ise çıkış trafiğini göstermektedir.

Bytes In ve Bytes Out değerlerinin toplamı bandgenişliği değerini vermektedir. Bu işleme göre ortalama bandgenişliği 147,95 k ve maksimum bandgenişliği 212.96 k değerindedir.

Uygulama esnasında oluşan network hataları ve paket kayıpları da toplam bandgenişliği hesaplanmasına etki etmektedir. Bu hatalar, Errors In ve Errors Out olmak üzere ikiye ayrılarak incelenmiştir. Errors In grafiği, karşı networkten kaynaklanan paket kayıpları ve network hatalarını içermektedir. Errors Out grafiği ise, bizim paket kayıplarımız ve network hatalarımızı göstermektedir. Bu uygulamada daha çok konuşma karşı taraftan olduğu için Bytes In ve Errors In değerleri daha fazla seviyededir.



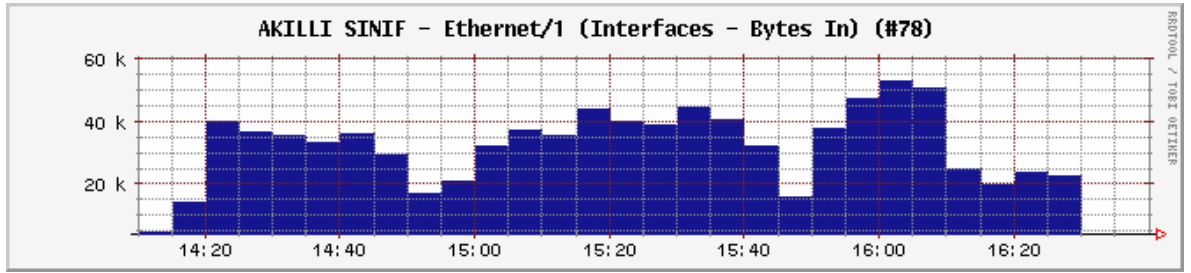
Şekil 7.8. Errors In Grafiği-1



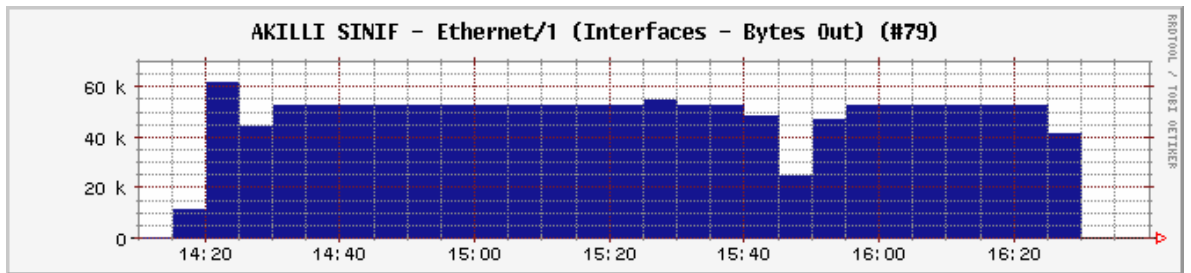
Şekil 7.9. Errors Out Grafiği-1

### 7.3. Yakın Noktadaki Birinci Uygulamanın Test Sonuçları

Bu uygulama Süleyman Demirel Üniversitesi içinde bulunan lokal network üzerinde yapılmıştır. Kaydedilen değerler aşağıda sunulmuştur:

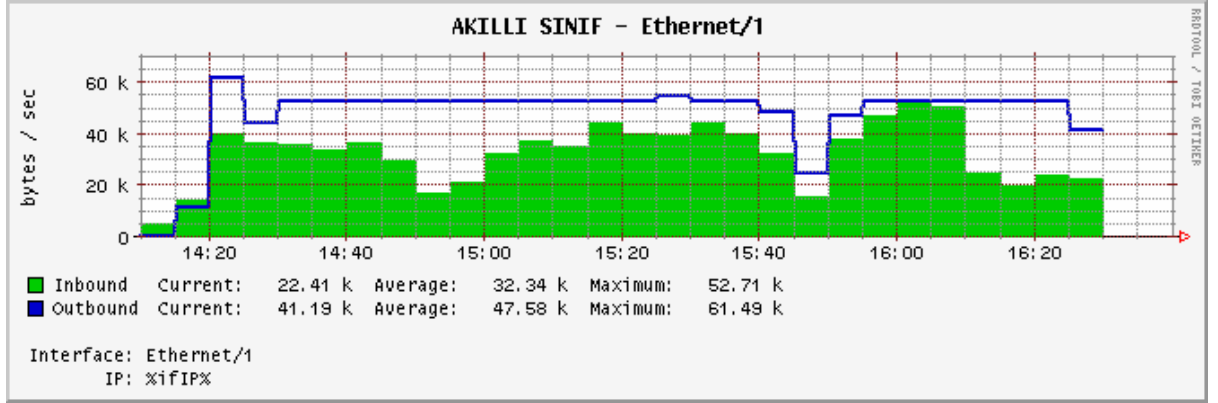


Şekil 7.10. Bytes In Grafiği-2



Şekil 7.11. Bytes Out Grafiği-2

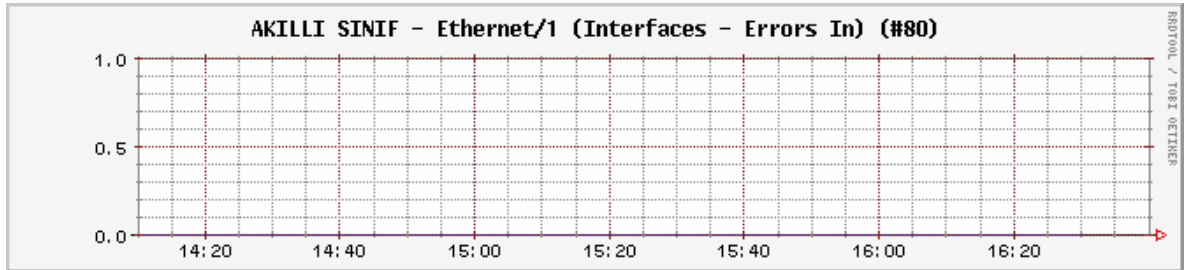
Test aşamasında maksimum 52,71 k giriş değeri ve maksimum 61,49 k değerinde çıkış ölçülmüştür. Ortalama olarak 32,34 k değerinde giriş ve 47,58 k değerinde çıkış elde edilmiştir.



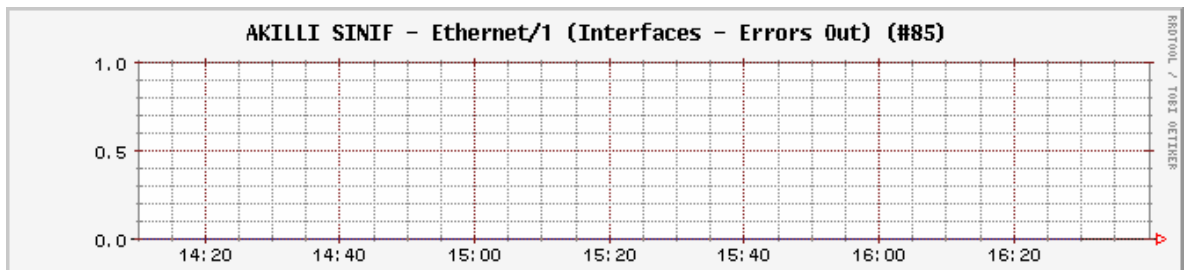
Şekil 7.12. Bytes In ve Bytes Out Grafiği-2

Ortalama bandgeniřliđi lokal network üzerinde 79.92 k ölçölmüşken, maksimum bandgeniřliđi 114,20 k olarak ölçölmüştür.

Errors In ve Errors Out grafikleri ařađıda görölmektedir. Ancak lokal network üzerinde herhangi bir paket kaybı veya network hatası gerçekleşmemiřtir.



Şekil 7.13. Errors In Grafiđi-2



Şekil 7.14. Errors Out Grafiđi-2

## 7.4. Yakın Noktadaki İkinci Uygulamanın Test Sonuçları

İkinci uygulamada, iki Linux işletim sistemi kurulu bilgisayar arasında H.323 protokolü kullanarak bir sesli görüşme yapılmıştır. Görüşme öncesinde NetMRG programına Akıllı Sınıf haricinde NetMRG Makinesi'nin arayüzü eklenmiştir (Şekil 7.15). Böylece sistemin, kendi etherneti ile ilgili olayları (bytes in, bytes out, errors in, errors out, load average) grafiklemesi sağlanmıştır. Tüm bu değerlerin grafikleri Şekil 7.16'da görülmektedir.

History: All Groups		Device Groups	
Name	Comment	Add	
Template Group		<View> <Edit> <Delete>	

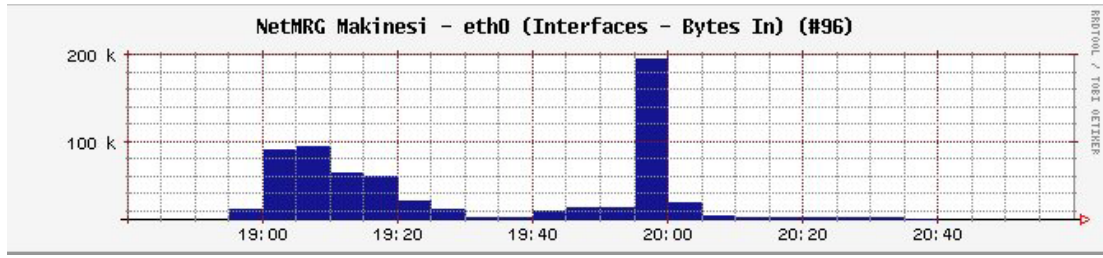
Monitored Devices		SNMP Options		Add	
Name					
AKILLI SINIF		<View Interface Cache>	<Recache Interfaces>	<View Disk Cache>	<Recache Disks>
NetMRG Makinesi		<View Interface Cache>	<Recache Interfaces>	<View Disk Cache>	<Recache Disks>

Şekil 7.15. Akıllı Sınıf ve NetMRG Makinesinin Seçildiği Menü

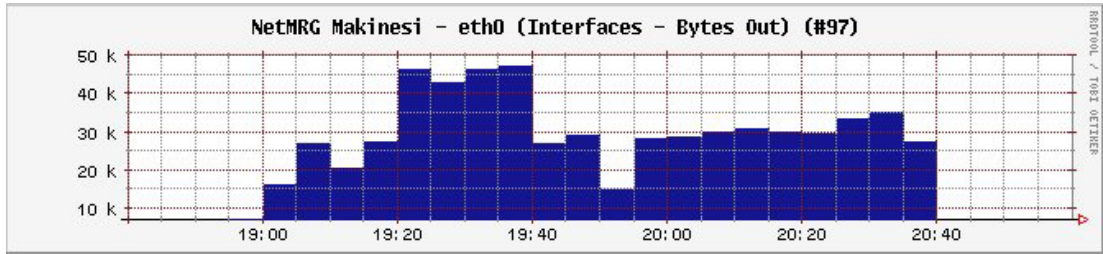
Test	Data	Graph	Add
UCD - Load Average - 1 min	Value: 0.00 Rate of Change: 0.00 Time Stamp: 2004-06-03 15:20:02		<Edit> <Delete>
UCD - Load Average - 5 min	Value: 0.00 Rate of Change: 0.00 Time Stamp: 2004-06-03 15:20:02		<Edit> <Delete>
UCD - Load Average - 15 min	Value: 0.00 Rate of Change: 0.00 Time Stamp: 2004-06-03 15:20:02		<Edit> <Delete>
Open TCP Connections	Value: 0.00 Rate of Change: 0.00 Time Stamp: 2004-06-03 15:20:02		<Edit> <Delete>
Interfaces - Bytes Out	Value: 272.20 k Rate of Change: 37.25 Time Stamp: 2004-06-03 15:20:02		<Edit> <Delete>
Interfaces - Bytes In	Value: 2.18 M Rate of Change: 594.61 Time Stamp: 2004-06-03 15:20:02		<Edit> <Delete>
Interfaces - Errors In	Value: 0.00 Rate of Change: 0.00 Time Stamp: 2004-06-03 15:20:02		<Edit> <Delete>
Interfaces - Errors Out	Value: 0.00 Rate of Change: 0.00 Time Stamp: 2004-06-03 15:20:02		<Edit> <Delete>

Şekil 7.16. NetMRG Makinesinden alınan tüm değerler

Uygulama esnasında elde edilen grafikler aşağıda sunulmuştur:

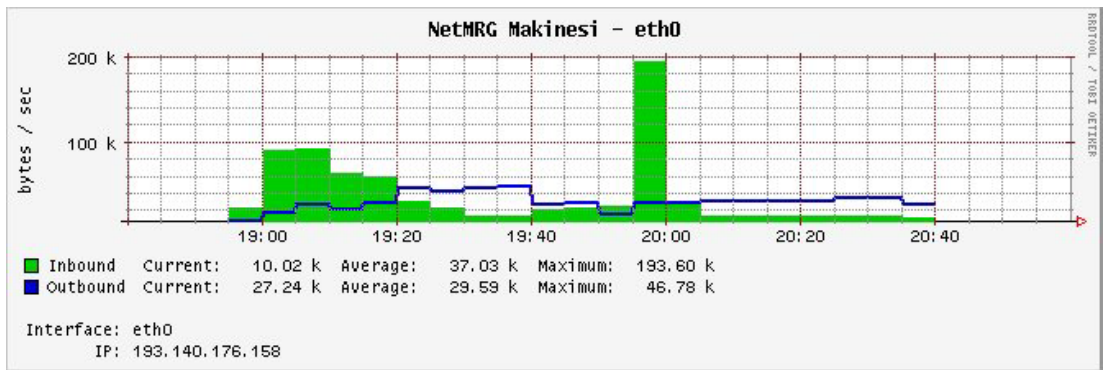


Şekil 7.17. Bytes In Grafiği-3



Şekil 7.18. Bytes Out Grafiği-3

Bu uygulamada maksimum 193,60 k giriş değeri ve maksimum 46,78 k çıkış değeri elde edilirken, ortalama olarak 37,03 k değerinde giriş ve 29,59 k değerinde çıkış elde edilmiştir.

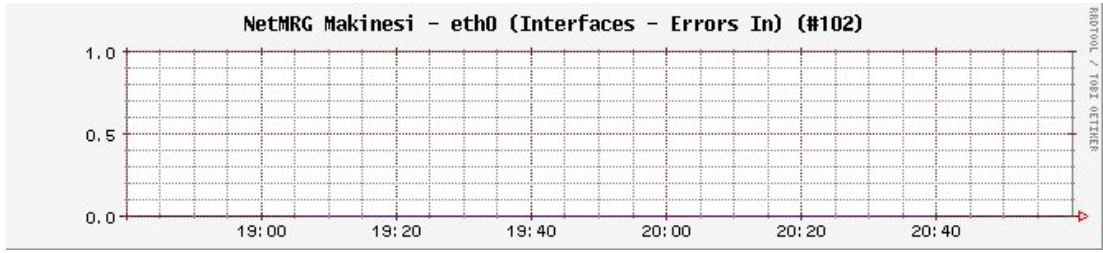


Şekil 7.19. Bytes In ve Bytes Out Grafiği-3

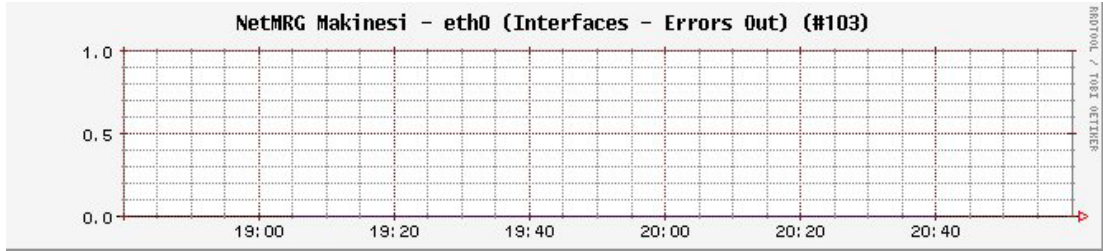


Ortalama bandgeniřliđi lokal network üzerinde 66.62 k ölçülmüşken, maksimum bandgeniřliđi 240,38 k olarak ölçülmüřtür.

Bu uygulamada da, 7.3'de anlatılan yakın noktadaki birinci uygulamaya paralel olarak, aynı řekilde hata gözlemlenmemiřtir. Uygulamaya ait Errors In ve Errors Out grafikleri ařađıda görülmektedir.

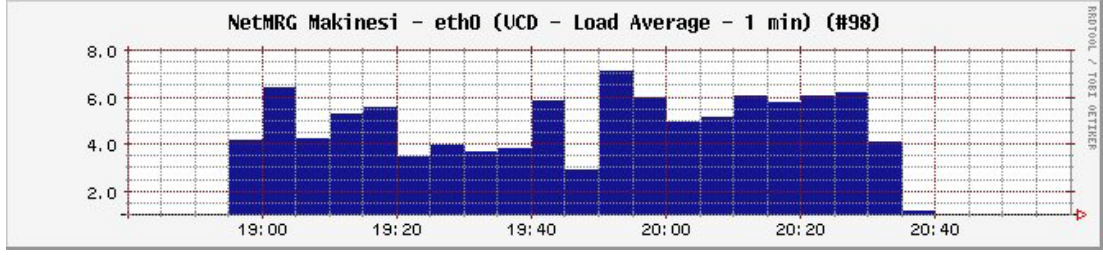


řekil 7.20. Errors In Grafiđi-3

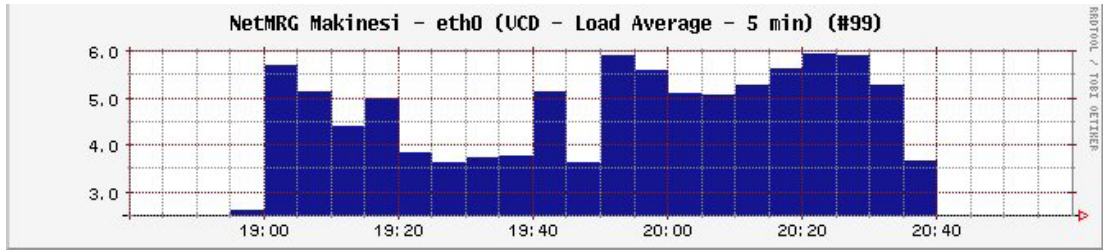


řekil 7.21. Errors In Grafiđi-3

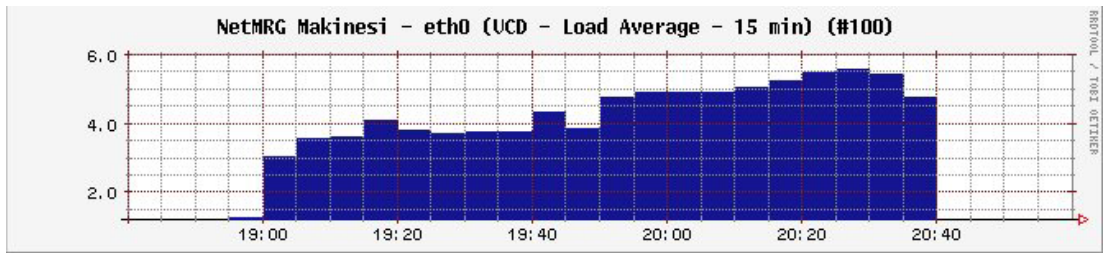
Trafik kaynaklarından gelen toplam trafik ve hat kapasitesi çerçevesinde bandgeniřliđinin kullanılma miktarı, ortalama yükü teřkil etmektedir. Data miktarının iletim esnasında zamana göre ortalama deđerı, ortalama yükü verir. Data paketlerinin bir kaynaktan diđerine 1, 5 ve 15 dakikalık birim zamanlardaki deđerlerinin ortalaması, sırasıyla řekil 7.22, řekil 7.23 ve řekil 7.24'de grafiklenmiřtir.



Şekil 7.22. 1 dakikalık ortalama yük grafiği

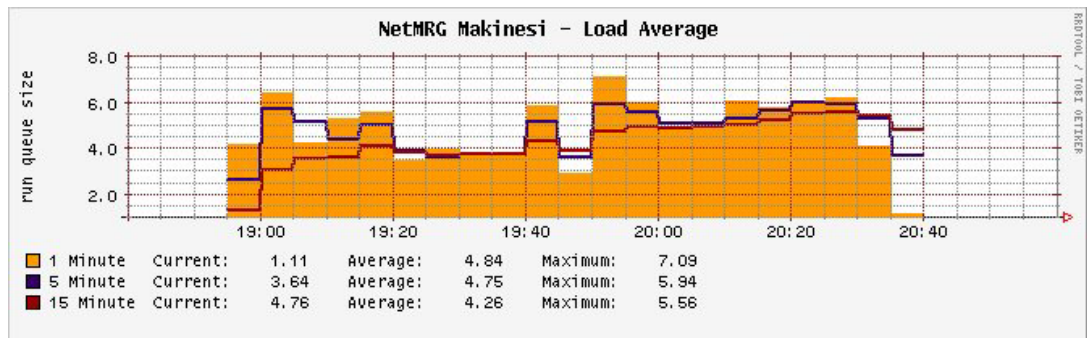


Şekil 7.23. 5 dakikalık ortalama yük grafiği



Şekil 7.24. 15 dakikalık ortalama yük grafiği

Şekil 7.25'de, 1, 5 ve 15 dakikalık ortalama yük grafikleri beraber görülmektedir.



Şekil 7.25. Ortalama Yük Grafiği

### 7.5. Test Sonuç Değerlendirmesi

Uzak nokta ile yapılan uygulamada kullanılan cihazlar aynı marka ve model olup, cihazların kullandıkları sıkıştırma ve kodlama teknikleri birebir aynı konfigüre edilmiştir. Bu sayede, bandgenişliği daha verimli kullanılabilmiştir. Yakın noktada gerçekleştirilen birinci uygulamada ise farklı cihazlar, farklı sıkıştırma ve kodlama teknikleri kullanılmıştır. Bu sebeple, bandgenişliği daha az verimle kullanılabilmiştir. Bu da, uygulama esnasında kullanılan cihazların kalitesinin bandgenişliğine ve dolayısıyla servis kalitesine etki ettiğini göstermektedir.

Aynı şekilde uzak noktadan alınan kayıtlarda hatalar gözlenirken yakın nokta iletişimde her iki uygulama için de herhangi bir hata oluşmamıştır. Bunun sebebi iki farklı nokta arasında veri iletilirken birden fazla cihaz üzerinden (Router, switch vs.) dataların geçmesi olarak değerlendirilmiştir. Buradan, iletim esnasında ne kadar az hop sayısı olursa, hata oluşmasının o ölçüde engellenebileceği sonucu çıkarılabilmektedir. Aynı şekilde uzak nokta uygulaması network trafiğinin yoğun olduğu saatlerde gerçekleştirilmiş, bu da hataların oluşmasına sebep olmuştur. Yakın nokta uygulamalarında hataların oluşmamasının en önemli sebepleri, uygulamaların network trafiğinin sakin olduğu zamanda yapılmış olması ve lokal networkte gerçekleştirilmesi olarak da değerlendirilmiştir.

## 8. SONUÇ

Tüm dünyada haberleşme sistemlerinin temel amacı görüşme yapmak isteyen ile görüşülmek isteyen arasında sürekli açık olan hattı kurmaktır. Bu haberleşme maliyetlerini arttıran en önemli unsurlardan biridir. Uzak mesafe ve uluslararası haberleşme için farklı çözümler üretilmekle beraber maliyet artışının önüne geçilememiştir. İnternet ile PSTN sistemler üzerinde haberleşmenin en önemli farkı da burada yatmaktadır. İnternet üzerinden haberleşmek için haberleşecek iki nokta (yada daha fazla) arasında sürekli açık hat kurulmaz. Her iki tarafta da gönderilecek ses ya da görüntü (ya da sayısal hale getirilebilen herhangi bir veri bloğu) bilgisi sayısallaştırıldıktan sonra sıkıştırılır. Oluşan veri bloğu paketlere bölünür. Veri paketleri İnternet üzerinden gönderilir. Her bir paket farklı ve o anda en optimum olan yoldan hedefe ulaşır. Alıcı tarafta paketler numaralarına göre sıralanır ve birleştirilir. Elde edilen bilgi bloğu konuşma yada görüntünün sayısal sıkıştırılmış halidir. Sayısal veri analog sinyallere çevrilir. Bu tür haberleşme özellikle bilgisayarlar arası iletişim için optimize edilmiştir. Paket anahtarlama yapısı ile en iyi çözümü sunmaktadır. İnternet erişimi sağlanan her noktadan kullanılabilmesi, şehiriçi/ yurtiçi/ yurtdışı ayırımının olmaması, şeffaf ve geliştirilebilir yapısı ile geleceği parlak bir sistemdir.

VoIP, telefon görüşmelerinin ve faksların IP tabanlı bir network üzerinden iletilmesine imkan veren teknolojidir. Bu düşünce ve bu teknoloji, uygulamada kullanıcılara belirli avantajları da beraberinde sunmaktadır. IP üzerinden sesin avantajları:

- **Azaltılmış Maliyetler:** Sesin, mevcut data hatları üzerinden gerçekleştirilmesi ile özellikle uzak mesafe görüşmelerinden doğan telefon fatura maliyetlerindeki azalma. Mevcut WAN üzerinde gerçekleştirilen konuşmaların ücretsiz gerçekleştirilmesi.
- **Basitleştirilmiş Yapı:** Entegre ses ve data sistemleri ile toplam cihaz ihtiyacında azalmanın sağlanması. Yatırım masraflarında azalma ve hem ses hem de data destekleyen cihazlarla sistemlerin daha basit bir yapıya kavuşmasının sağlanması.

- **Gelişmiş Uygulamalar:** Bugünkü telefon sistemlerinin destekleyemediği çoklu ortam ve çoklu servis uygulamalarının (internet, intranet vb.) destekleniyor olmasından dolayı yeni teknolojik gelişmelere uyum imkanının olması.
- **Esnek Çalışma:** Kullanıcılar nerede olurlarsa olsunlar iş dokümanları üzerinde karşılıklı görüşürler. Sesli haberleşme grup ve ekip çalışmaları ile bütünleşir, dokümanlar paylaşılır, fikirler ortaya atılır, karşılıklı notlar iletilir. Bunun anlamı, seyahat masrafları ödemediği toplantılar düzenlenebilir. Eğitim ve öğrenmek kolaylaşır. İş büyümesi gerçekleşir.
- **Zamandan Tasarruf:** Bireyler zamanlarını daha iyi idare ederek kullanabilir ve daha verimli çalışırlar.

Bunların sağlanabilmesi için IP üzerinden yapılan ses haberleşmesinin kesintisiz ve kaliteli olması gerekmektedir. Bu durum her ağ için Servis Kalitesi (QoS) kavramını gerektirir. Bandgenişliği, gecikmeler, paket kayıpları, network trafiğinin yoğunluğu gibi faktörlerin servis kalitesine etkileri sesin iletimi için önemlidir.

Uzun yıllar boyunca, kullanıcıların garanti edilmiş bantgenişliği ve gecikme değerleri istemleri, ancak özel kiralık hatlar kullanılmasıyla sağlanabilmiştir. Eğer ağ gerekli QoS'i yerine getiremiyorsa, bu durumda kullanıcı uygulaması QoS'i sağlamalıdır. İnternet üzerinde hiçbir QoS yoktur. Çalışma "en iyi çabanın sağlanması" ilkesine göre, güvenilir olmayan bir şekilde sürdürülür. İnternet üzerinde çalışan tüm uygulamalar kendi QoS gereksinimlerini bir şekilde sağlamak zorundadır.

İnternet üzerinde QoS olmaması, uygulamaların hiçbir zaman çalışmayacak olması anlamına gelmez. Sadece, uygulamaların her zaman garantili bir şekilde çalışmaması anlamına gelir.

Bir IP şebekesi (İnternet veya İnternet) üzerindeki gecikme, iletimin günü saati, erişim isteyen kullanıcı sayısı, trafik tipi, erişim transmisyon hızı, omurga (backbone) transmisyon hızları gibi faktörlere bağlı olarak değişir.

Şu anda, bir sesli aramanın kalite seviyesi gün boyunca değişebilmektedir. Yoğun saatler sırasında ABD'ye (örneğin GB saatine göre saat 21:00'de) yapılan sesli bir çağrı, saat 05:00'da yapılan benzer bir çağrı ile aynı kalitede olmayabilir. Ancak, bu tür çağrılar her kullanıcının kendi ISP'sine lokal olarak bağlı olması nedeniyle uzak mesafe ücretlendirmesine girmez. Bir İnternet kullanıcısının telefon için kullandığı yazılım, bir intranet ortamında daha büyük hız, kontrol ve verimlilikle kullanılabilir.

Paket kayıpları genellikle taşmalardan ve periyodik olarak networkün tıkanmasından meydana gelir. Bu kayıpların önlenmesi için hem yüksek bantgenişliği hem de güçlü kodlama algoritmaları gereklidir.

Günümüz IP şebekelerindeki gecikmeler, 100 ms'den 600 ms'ye kadar farklılık gösterebilir. VoIP için QoS sağlamak amacıyla network gecikmesi, 200 ms veya daha altında tutulmalıdır. İletimde meydana gelen kayıplar ise network durumuna ve kullanılan cihazların işlem kapasitesine göre değişimler göstermektedir.

IP networkte, network gecikmelerinin yanı sıra bir de paket şebekesinin oluşturduğu gecikme söz konusudur. Çünkü paketler değişken gecikme süreleriyle ve düzensiz olarak (gönderilen sıradan farklı olarak) hedeflerine ulaşabilirler. Bu nedenle tekrar sıralama, paket şebekelerinin oluşturduğu gecikmeyi dengeleme ve paket kayıplarının önlenmesi gerekmektedir.

Bu durumu engellemek için paketlere öncelik tanımlanabilir. IP network trafiği, genellikle düzensizdir ve öncelik sıralaması yoktur. Paketler sıklıkla bir noktadan diğerine iletim esnasında gecikmeli gelir. İletim önceliği olan trafik, iletim önceliği olmayandan daha önce iletilir. Verilerin önceliklendirilmesi, ağ üzerinde gecikmeyi engelliyerek, uygulamaların kesintisiz akışını sağlamaktadır.

QoS olmayan networklerde, uygulamalar yardımı ile networke QoS katılması için çeşitli yöntemler kullanılır (Cambazoğlu, 2000). Bandgenişliği problemi için, birden fazla hatta ters multipleks uygulanır ya da yüksek hızlı özel hatlar kullanılır. Gecikmeyi engellemek için en az sayıda "hop" araştırılır ve daha fazla sayıda noktadan noktaya özel hat kullanılır. Jitter sorunu, alıcıda uyumlu (kararlı) bir

gecikme deęeri elde etmek için jitter tamponları kullanılarak aşılabılır. Networkte meydana gelen bilgi kayıpları (hatalar, paket kayıpları) için, ileri yönde hata düzelten kodlama kullanılır ve uygulamanın, etkileri deęerlendirerek gerekli düzeltmeleri yapmasına olanak tanınır. Güvenilirlik, yedek bağlantılar ve sistemlerle sağlanabilmekte iken, kriptolama, doęrulama/onaylama teknikleri kullanılarak güvenlik sorunu aşılabilmektedir.

## 9. KAYNAKLAR

Abazi, A., 2000. İnternet Protokolü Üzerinden Ses İletimi, İ.T.Ü. Fen Bilimleri Enstitüsü, Y.Lisans Tezi, 58 s, İstanbul.

ARGE-TEK – VoIP (voice over ip) nedir?

[http://www.arge-tek.com/voip\\_detay.html](http://www.arge-tek.com/voip_detay.html)

Baykal, N., 2001. Bilgisayar Ağları. SAS Bilişim Yayınları, 502 s. Ankara.

Cambazoğlu T., 2000. İnternet güvenliği ve servis kalitesi (QoS) -2. Kısım

[http://www.bilirimrehber.com.tr/arastirma/tr\\_arastirma\\_internet\\_guvenligi\\_ve\\_servis\\_kalitesi2.phtml](http://www.bilirimrehber.com.tr/arastirma/tr_arastirma_internet_guvenligi_ve_servis_kalitesi2.phtml)

Cisco Systems - Voice Quality - Understanding Delay in Packet Voice Networks

[http://www.cisco.com/en/US/tech/tk652/tk698/technologies\\_white\\_paper09186a00800a8993.shtml](http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800a8993.shtml)

Ericsson Mobility World – Makaleler

<http://www1.ericsson.com.tr/mobilityworld/articles/features/105805-02052002.htm>

Intertangent Technology Directory, [History of VOIP](#)

[http://www.intertangent.com/023346/Articles\\_and\\_News/1413.html](http://www.intertangent.com/023346/Articles_and_News/1413.html)

İnternet Telefonu Standartları

<http://www.voipturk.com/inttelstandart.php>

Kakadia D., Enterprise QoS Policy Based Systems & Network Management, Sun Microsystems

Kaplan Y., 1999. Veri Haberleşmesi Kavramları. Intrakets, 153 s. İstanbul.



Kara, N., Deveci, S.K., Oktay, A., 2000, Voice Over IP. Türk Telekom Bilişim Ağları Dairesi Başkanlığı, 33 s, Ankara.

Metin, B., 2001. Quality Of Service In IP Networks. Boğaziçi U. Master of Science, 80 s, İstanbul.

Netaş/Nortel Networks Teknik Eğitim Dokümanı, 2000, Voice over IP, 106 s. İstanbul.

Netaş/Nortel Networks Teknik Eğitim Dokümanı, 2000, TCP/IP Genel Bakış, 140 s. İstanbul.

Nortel Networks Netaş – Makaleler – Servis Kalitesine İlk Adım  
<http://www.netas.com.tr/article10.html>

Nortel Networks Netaş – Makaleler – Servis Kalitesi Uygulamaları  
<http://www.netas.com.tr/article11.html>

Varol N., 1999, İnternette Servis Kalitesi. İ.T.Ü. Fen Bilimleri Enstitüsü, Y.Lisans Tezi, 86 s, İstanbul.

Vivere Networks, 2003, QoS Glossary, 16 s.

Voice over Internet Protokol – Quality of Service, 2004, The University of North Carolina  
<http://www.unc.edu/courses/2004spring/law/357c/001/projects/jennwill/VOIP/quality.html>

## EK

### İNDEKS

**ATM – Asynchronous Transfer Mode (Asenkron Transfer Modu):** Çoklu tipte servisler (ses, video, veri) için bilginin küçük, sabit-boyutlu hücrelerde taşındığı hücre transferi için ITU standardı. ATM, LAN ve WAN ortamlarının her ikisinde de kullanılan bir bağlantı-temelli teknolojidir.

**BER – Bit Error Rate (Bit Hata Oranı):** İletilen veri akımında gözlemlenen hata oranı. BER, hata görülmeyen süre yüzdesi veya hatasız veri biti yüzdesi olarak ifade edilebilir.

**CBR – Constant Bit Rate (Sabit Bit Oranı):** ATM networkleri için ATM Forum tarafından tanımlanan QoS sınıfı. CBR, bozulmadan iletimi sağlamak için hassas clocking'e bağımlı olan bağlantılar için kullanılır.

**CCS – Common Channel Signalling:** Devrelerin çoğullanması veya network yönetimi için bir fonksiyonla ilgili sinyalleşme bilgisinin adreslenen mesajlar tarafından tek bir kanal üzerinden taşındığı bir sinyalleşme metodu.

**CELP – Code-Excited Linear Predictive Coding:** 8 kbit/s 'de kullanılan bir ses sıkıştırma algoritması.

**Codec – enCOde/DECOde:** Bir sayısal iletim ortamında taşınması için bir formattaki sayısal veya analog işareti kodlayan ve alınan tarafta ters işlemi gerçekleştiren cihaz. Codec'ler sayısal sıkıştırmayı da destekleyebilir. [17]

**Compression (Sıkıştırma):** Bir veri kümesinin bant genişliğini veya transmisyon/depolama için gereken alanı azaltmak için boyutunun düşürülmesi.

**CTI – Computer Telephony Integration (Bilgisayar Telefon Bütünleşmesi):** Geleneksel haberleşme ekipmanlarının (PBX) bilgisayarlar ve bilgisayar uygulamaları ile birlemesine verilen isim.

**Datagram:** Kaynaktan hedef bilgisayara ve taşıyıcı ağ arasında daha önceki alışverişlere dayanmadan kaynaktan hedefe yönlendirilmek için yeteri bilgiyi taşıyan bağımsız veri taşıma birimi.

**Delay (Gecikme):** (1) Bir çağrının işlem için beklemede geçirdiği zaman. (2) Temel olarak, bilginin bir network veya network segmentini transit geçmek için aldığı süre.

**DTMF – Dual Tone Multi-Frequency (Çift Tonlu Çoklu Frekans):** Bir tuş takımından üretilen, telefon sinyalleşmesinde kullanılan standartlaştırılmış tonlar seti.

**Domain (Etki Alanı):** Yönetimsel bir varlık teşkil eden ağ üzerindeki bir grup ucun oluşturduğu topluluk. Etki alanı üyeleri aynı güvenlik veri tabanını ve yönetim politikalarını paylaşırlar.

**ETSI - European Telecommunication Standarts Institute (Avrupa Telekomünikasyon Standartları Enstitüsü):** CEPT'in 1988'de aldığı karar doğrultusunda kurulan kurum. CEPT'in ağ standartları konusundaki çalışmalarını devralmıştır.

**Frame (Çerçeve):** Bir ağ üzerinden gönderilen bir grup bit. Bir çerçeve denetim, adresleme ve CRC gibi hata tespiti ve düzeltimi bilgisini içerebilir. Boyu ve yapısı, protokole göre değişir.

**Frame Relay:** Paket anahtarlama Geniş Alan Ağı'na, genellikle Yerel Alan Ağı'ndan yüksek hızla bağlanan kullanıcılara, bağlantı yönelimli servis sağlayan bir Geniş Alan Ağı teknolojisi.

**Framing (Çerçeveleme):** Zaman bölümlenmeli olarak çoğullanmış sayısal kanalları birbirinden ayırmak için kullanılan yöntem.

**H.323:** IP omurgaları üzerinden sesin ve görüntünün nasıl iletileceğini tanımlayan Uluslararası Telekomünikasyon Birliği (ITU) tarafından onaylanmış bir standart.

**Hop (Atlama):** Bir ağ paketinin, hedefine varmadan önce kaç düğüm atladığını gösteren yönlendirme terimi. İki ayrı uç arasında bir ağ bağlantısı.

**Host:** (1) İnternette, diğer bilgisayarların iki yönlü erişim sağladıkları herhangi bir bilgisayardır. Ağ üzerindeki bir nokta anlamında kullanılır. (2) Ana bilgisayar (mainframe). Akıllı veya akılsız terminallere hizmet eder. (3) Kendinden daha küçük veya daha az özelliğe sahip olan cihaz veya programa hizmet veren cihaz veya program.

**IAB – Internet Activities Board (İnternet Etkinlikleri Yönetim Kurulu):** İnternette kullanılan protokoller için öngörülerde bulunan ve denetleyen teknik tüzel kişilik.

**ICMP – Internet Control Message Protocol (İnternet Denetim Mesajı Protokolü):** IP katmanında hata ve denetim mesajlarını idare etmek için kullanılan protokol. IP datagramın içinde yer alır.

**IGMP – Internet Group Management Protocol (İnternet Grup Yönetim Protokolü):** Multicast grup üyelerini komşu multicast router'a rapor etmek için IP hostlar tarafından kullanılır. Router'lar bu bilgiyi, multimedya ortamındaki trafiği sınırlayarak yerel ağ bant genişliğini korumak için kullanabilirler.

**IETF – Internet Engineering Task Force (İnternet Mühendislik Görev Gücü):** TCP/IP ve İnternet ile ilgili kısa ve orta vadeli problemlerle ilgilenen bir US komitesi.

**Interface (Arayüz):** İki sistem, bölge veya işlem arasında etkileşimin gerçekleştiği yer veya cihaz parçası.

**İnternet:** Dünya çapında kurulu IP ağlarının birbirine bağlanmasıyla oluşan uluslar arası IP ağı.

**İnternet Telefonu (Internet Telephony):** Ses, faks ve diğer bilgilerin elektronik ortamda iletilmesini sağlayan telefon teknolojisi. Klasik telefon ağlarının yerine İnternet alt yapısını kullanır.

**İnternetnetwork:** Tek bir network olarak fonksiyon gören, router'lar tarafından bağlanan bir networkler topluluğu.

**İntranet:** Kurum içi veri haberleşmesi için oluşturulmuş kapalı ağ.

**IP – Internet Protocol:** Adresleme bilgisini ve paketlerin yönlendirilmesine izin veren bazı kontrol bilgisini içeren bir Network Katmanı protokolü.

**IPv6:** IPv4'ün yerini alacak olan yeni IP sürümü. Bu sayede IP adresleri 32 bit'ten 128 bit'e çıkıyor.

**ISDN – Integrated Services Digital Network (Tümleşik Hizmetler Sayısal Ağı) :** Varolan herkese açık anahtarlı telefon ağı üzerinde veri işaretlerini göndermek, ses ve videoyu sayısallaştırmak için kullanılan bir iletişim standardı.

**ISDN BRI:** Üç kanala bölünmüş olan bir sayısal erişim hattı. Kanallardan ikisi, B kanalı olarak adlandırılır, 64 kbit/s ve sadece veri veya ses için kullanılır. Üçüncü kanal olan D kanalı, 16 kbit/s 'de sinyalleşme için kullanılır.

**ISDN PRI:** Fiziksel ve elektriksel olarak E1 devresini temel alır, fakat iki kanal sinyalleşme için ve 30 kanal kullanıcı trafiği için ayrılmış olacak şekilde

kanallandırılmıştır. ISDN PRI, ülkeye bağlı olarak, E1 veya T1 formatlarında geçerlidir.

**ISP – Internet Service Provider (İnternet Servis Sağlayıcısı – ISS):** İnternet erişimi sağlayan şirket.

**ITU – International Telecommunications Union:** Uluslararası Telekomünikasyon Birliği. CCITT'nin yeni adı. Bir Birleşmiş Milletler uygulama organizasyonu, uluslararası bir standartlar kurulu. ITU, her biri özel alanlar ile ilgili bir dizi grup ile çalışır. Çalışma grubu VII, veri haberleşme ağları ve X serisi tavsiyelerden sorumlu iken, çalışma grubu XVIII ISDN dahil olmak üzere sayısal ağlardan sorumludur.

**LAN – Local Area Network (Yerel Alan Ağı):** Küçük bir coğrafi alanı (bir kaç km'ye kadar) kapsayan yüksek hızlı veri ağı. Tek bir binadaki veya sınırlı bir alandaki iş istasyonlarını, çevre birimlerini, terminalleri ve diğer cihazları birbirine bağlar. Ethernet, FDDI ve Token Ring bu tip ağlarda en çok kullanılan teknolojilerdir.

**Latency (Gecikme):** Bir cihazın bir frame alması ve frame'in hedef porta yönlendirilmesi arasındaki gecikme.

**MAC – Medium Access Control (Ortam Erişim Denetimi):** IEEE tarafından yerel alan ağlarında paylaşılan ortamlara erişimi denetlemek üzere belirlenmiş veri bağı alt katmanlarında biri.

**MOS – Mean Opinion Scores (Ortalama Kani Skoru):** Telefon bağlantılarının ses kalitesini derecelendiren bir sistem. MOS, bağlantı kalitesini değerlendiren geniş sayıda aboneden alınan istatistiksel bir ses kalitesi ölçümüdür.

**Multicast (Çoklu Saçım):** (1) Mümkün olan hedeflerden daha önce tanımlanmış bir kümeye bir paketin iletimi için bir broadcast şekli. (2) Bir gönderici ile ağ üzerinde birden fazla alıcı arasında kurulan iletişim.

**NMS – Network Management System (Ağ Yönetim Sistemi):** Ağın en azından bir bölümünün yönetiminden sorumludur.

**Node (Uç):** (1) Bir iletim ortamı ile birbirine bağlı, bir ağ üzerinde ağ hizmetlerini sunan veya talep eden cihazlar. Node sıklıkla işstasyonu yerine kullanılır. (2) Ağa ulaşan bir ucu tanımlayan genel bir terim.

**Oktet (Sekizli):** Sekiz bitten oluşan veri birimi.

**OSI – Open System Interconnection (Açık Sistem Arabağlantısı) :** Bir iletişim ağındaki herhangi iki nokta arasında mesajların nasıl iletileceğini belirleyen standart veya referans model.

**Paket:** (1) Bir başlık ve (genellikle) kullanıcı verisi içeren bilginin mantıksal bir gruplaması. (2) Birlikte anahtarlanan ve iletilen adres, veri ve denetim bilgisini içeren bir grup bit.

**PBX – Private Branch Exchange:** Abone sistemine dayanan sayısal veya analog telefon santrali, özel veya herkese açık telefon ağlarını birbirine bağlamak için kullanılır. “Plug Board Exchange” olarak da adlandırılır.

**PCM – Pulse Code Modulation (Darbe Kodu Modülasyonu):** Analog bilginin sayısal formda örneklerin sabit bir bit sayısında örneklenmesi ve kodlaması sayesinde transmisyonu.

**Port:** (1) Bir ağ giriş ya da çıkış noktası. (2) Harici bir cihaza bağlantı için bilgisayar üzerindeki bağlantı noktası

**POTS – Plain Old Telephone System:** Modemlerle kullanılan bizim "normal" olarak gördüğümüz telefon sistemi. Kiralık hatları ve sayısal hatları içermez.

**Protokol:** Bilgi iletimi için belirlenmiş kurallar/standartlar kümesi. Protokoller, haberleşen iki birim arasındaki mesajlaşma dışında, hata denetimi ve kontrolü gibi karmaşık detayları da içerirler.

**PSTN – Public Switched Telephone Network (Kamusal Anahtarlamalı Telefon Ağı):** Dünya genelinde yerini alan çeşitli telefon ağı ve servislerini adlandırmak için genel terim.

**QoS – Quality of Service (Servis Kalitesi):** Bir transmisyon sisteminin transmisyon kalitesi ve servis geçerliliğini yansıtan performans ölçüsü.

**RAS - Registration Admission Status (Kayıt Kabul ve Durum Protokolü):** Gatekeeper ile uç birimler arası haberleşme için kullanılan protokol.

**RFC – Request For Comments (Yorumlar İçin Talep):** İnternet protokolleri için hazırlanmış yazılı dokümanlar. Doküman dizisi, 1969’da İnternet protokol takımı ve ilgili deneylerin açıklanmasıyla başlar.

**RSVP – Resource Reservation Protocol:** Bir IP networkü boyunca kaynakların rezervasyonunu destekleyen bir protokol. IP son sistemlerinde çalışan uygulamalar,

RSVP'yi almak istedikleri paket stream'lerinin doğasını (bandgeniřliđi, jitter, maksimum burst ve benzeri) diđer node'lara bildirmek için kullanabilirler.

**RTCP – RTP Control Protocol:** Zamanlama yeniden yapılandırma, kayıp sezme, güvenlik, ve içerik tanımlama dahil olmak üzere gerçek-zaman özellikli uygulamalar için destek sağlayan bir protokol. RTCP, bir İnternet içindeki geniş gruplar için kaynak tanımlama ve gateway'ler için destek (ses ve video köprüleri gibi) ve çok içerik-tek içerik çeviriciler dahil olmak üzere, gerçek-zaman konferans için destek sağlar.

**RTP – Real-Time Transport Protocol (Gerçek Zamanlı Taşıma Protokolü):** UDP üzerinde çalışan, IP omurgalarında sürekli ses ve görüntü akımlarını destekleyen bir İnternet protokolü.

**SDH – Synchronous Digital Hierarchy (Eşzamanlı Sayısal Sıradüzeni):** 155 Mbit/s ve üzeri veri oranları için, ađ işleticileri için tasarlanan, İTU eşzamanlı iletim standardı.

**Segment:** TCP katmanlarının iletişim için kullandıkları birim bilgi miktarı

**SNA – Systems Network Architecture (Sistem Ađ Mimarisi):** Geniş Alan Ađı bağlantısı sağlamak için İBM tarafından geliştirilen ve OSI başvuru modeli gibi 7 katmanlı bir yapıdan oluşan ađ mimarisi.

**SNMP – Simple Network Management Protocol (Basit Ađ Yönetim Protokolü):** Özellikle TCP/IP ađlarında kullanılan ađ yönetim protokolü. Ađ cihazlarının izlenmesi ve kontrolünü, konfigürasyonların, istatistik işlemlerinin, performansın ve güvenliđin yönetimini sağlar.

**SQEG – Speech Quality Expert Group:** İTU içinde konuşma kalitesi ile ilgili çalışan bir grup.

**Stream:** Akış

**TCP/IP – Transmission Control Protocol/İnternet Protocol (İletim Denetim Protokolü/İnternet Protokolü):** (1) ABD Savunma Bakanlıđının 1970'lerde dünya-geneli ara network yapısını desteklemek için geliřtirdiđi protokol bütününün ortak adı. Bütün içinde TCP ve IP, en iyi bilinen protokollerdir. TCP, OSI referans modelinin Taşıma Katmanı'na (4. katman) karşı gelir. Güvenilir veri transferi sağlar. IP, OSI referans modelinin Network Katmanı'na (3. katman) karşı gelir ve

bağlantısız datagram servisi sağlar. (2) İnternet ve diğer networklerde haberleşme için kullanılan taşıma ve uygulama protokolleri demeti.

**TDM – Time-Division Multiplexing (Zaman Bölünmeli Çoğullama):** Çoklu kanallardan bilgilerin tek tel üzerinde önceden atanmış zaman slot'larına bandgenişliği atandığı tekniktir. Bant genişliği, istasyonun gönderecek verisi olsa da olmasa da her kanala atanır.

**UDP – User Datagram Protocol (Kullanıcı Datagram Protokolü):** TCP/IP protokol kümesi içinde yer alan, bağlantı eğilimi olmayan bir Ulaşım Katmanı protokolüdür. TCP protokolüne benzemekle birlikte, aktarılan verinin tek bir datagram içerisine sığabilecek büyüklükte olduğu, sorgulama amaçlı verilerin aktarılması durumunda kullanılır.

**VoIP - Voice Over Internet Protocol:** IP temelli İnternet üzerinden ses sinyallerinin iletimi için geliştirilen sistem.

**VPN – Virtual Private Network (Sanal Özel Ağ):** Herkese açık olan iletişim altyapısını kullanan özel bir veri ağıdır. Tünel protokolü ve çeşitli güvenlik prosedürleri ile izinsiz girişlere karşı korunur.

**WAN – Wide Area Network (Geniş Alan Ağı):** Coğrafi olarak büyük bir alana yayılmış olan iletişim ağı.



