İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

UMTS ŞEBEKESİ'NDE IP

YÜKSEK LİSANS TEZİ

Müh. Nuran DEMİRCİ

Anabilim Dalı : ELEKTRONİK VE HABERLEŞME MÜHENDİSLİĞİ

Programı : TELEKOMÜNİKASYON MÜHENDİSLİĞİ

HAZİRAN 2008

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

UMTS ŞEBEKESİ'NDE IP

YÜKSEK LİSANS TEZİ
Müh. Nuran DEMİRCİ
(504041316)

Tezin Enstitüye Verildiği Tarih : 5 Mayıs 2008
Tezin Savunulduğu Tarih : 10 Haziran 2008

Tez Danışmanı : Prof.Dr. Günsel DURUSOY
Diğer Jüri Üyeleri Prof.Dr. Ümit AYGÖLÜ (İ.T.Ü)
Yrd.Doç.Dr. Demir ÖNER (M.Ü.)

HAZİRAN 2008

ÖNSÖZ

Bana, bu çalışmada görüş ve önerileriyle katkı sağlayan, yardımlarını esirgemeyen ve üniversite eğitimim süresince yol gösteren başta değerli hocam sayın Prof. Dr. Günsel DURUSOY olmak üzere bütün hocalarıma, beni bugünlere getiren, her zaman bana destek olan aileme, çalışmalarımda katkısı olan tüm arkadaşlarıma, başta yöneticilerim olmak üzere destek veren iş arkadaşlarıma teşekkürü bir borç bilirim.

Haziran 2008 Nuran DEMİRCİ

İÇİNDEKİLER

KISALTMALAR

1G : 1st Generation
2G : 2nd Generation
3G : 3rd Generation
3GPP : Third Generation Partnership Project
AAA : Authorisation, Authentication and Accounting
AAL2 : ATM Adaptation Layer Type 2
AAL5 : ATM Adaptation Layer type 5
ACK : Acknowledgement
AH : Authentication Header
AF : Assured Forwarding
AMR : Adaptive Multi Rate
AMPS : Advanced Mobile Telephony System
APM : Application Transport Message
ARP : Adress Resolution Protocol
AS : Application Server
ATM : Asynchronous Transfer Mode
AuC : Authentication Centre
AUTN : Authentication token
AVP : Attribute Value Pairs
BCF : Bearer Control Function
BE : Best Effort
BGCF : Breakout Gateway Control Function
BICC : Bearer Independent Call Control
BIWF : Bearer Interworking Function
BSC : Base Station Controller
BSS : Base Station Subsystem
BTS : Base Transceiver Station
CBR : Constant Bit Rate
CDMA : Code Division Multiple Access
CK : Ciphering Key
CN : Core Network
COPS : Genel Açık Denetim Hizmeti
CS : Circuit Switched
CSF : Call Service Function
CSCF : Call Server Control Function
DHCP : Dynamic Host Configuration Protocol
DSCP : Diffserv Code Point
Diffserv : Differentiated services
DL : Downlink (Forward Link)
DNS : Domain Name Service

DTMF : Dual Tone Multiple Frequency
EDGE : Enhanced Data rates for Global/GSM Evolution
EF : Expedicted Forwarding
EIC : Equipment Identity Centre
EIR : Equipment Identity Register
ESI : End System Identifier
ESP : Encapsulating Security Payload
ETR : ETSI Technical Report
ETS : European Telecommunication Standard
ETSI : European Telecommunications Standards Institute
FDD : Frequency Division Duplex
FM : Frequency Modulation
FEC : Forward Equivalence Class
GGSN : Gateway GPRS Support Node
GMSC : Gateway MSC
GPRS : General Packet Radio Service
GSM : Global System for Mobile communications
GSN : GPRS Support Nodes
GTP : GPRS Tunneling Protocol
GTP-C : GPRS Tunnelling Protocol for Control Plane
GTP-U : GPRS Tunnelling Protocol for User Plane
HLR : Home Location Register
HSS : Home Subscriber Server
HTTP : Hyper Text Transfer Protocol
IAM : Initial Address Message
ID : Identifier
IETF : Internet Engineering Task Force
IGRP : Interior Gateway Routing Protocol
IK : Integrity Key
IMEI : International Mobile Equipment Identity
IMPI : IM Private Identity
IMPU : IM Public Identity
IMS : IP Multimedia Subsystem
IMSI : International Mobile Subscriber Identity
Intserv : Integrated Service
IP : Internet Protocol
IPBCP : IP Bearer Control Protocol
IPSec : IP Security
IPv4 : Internet Protocol Version 4
IPv6 : Internet Protocol Version 6
ISDN : Integrated Services Digital Network
ISIM : IM Service Identity Module
ISP : Internet Service Provider
ISUP : ISDN User Part
ITU : International Telecommunication Union
ITU-T : International Telecommunications Union Telecommunications

IWU : Inter Working Unit
I-CSCF : Interrogating CSCF
Ki : Individual subscriber authentication key
L1 : Layer 1
L2 : Layer 2
LAN : Local Area Network
LER : Label Edge Router
LIB : Label Information Base
LLC : Logical Link Control
LSR : Label Switching Router
MAC : Medium Access Control
MAP : Mobile Application Part
MEGACO : Media Gateway Control Protocol
MGCF : Media Gateway Control Function
MGCP : Media Gateway Control Protocol
MGW : Media Gateway
MCC : Mobile Country Code
MNC : Mobile Network Code
MPLS : Multiprotocol Label Switching
MRFC : Media Resource Function Control
MRFP : Media Resource Function Process
MS : Mobile Station
MSC : Mobile Switching Centre
MSCS : MSC Server
MT : Mobile Termination
MTP : Message Transfer Part
MU3A : MTP3 Adaptation Layer
NAS : Network Access Server
NAT : Network Adres Translation
NDS : Network Domain Security
NBAP : Node B Application Part
NE : Network Element
NMT : Nordic Mobil System
NSAP : Network Service Access Point
OMAP : Operations, Maintainance and Administration Part
OSI : Open System Interconnection
PCM : Pulse Code Modulation
PCRF : Policy and Charging Rules Function
PCS : Personal Communication System
PCU : Packet Control Unit
PDF : Policy Decision Function
PDP : Packet Data Protocol
PDN : Packet Data Network
PDU : Protocol Data Unit
PHB : Per-Hop-Behaviour
PLMN : Public Land Mobile Network
PPP : Point-to-Point Protocol

PS : Packet Switched
PSTN : Public Switched Telephone Network
P-CSCF : Proxy CSCF
P-TMSI : Packet TMSI
QoS : Quality of Service
R4 : Release 4
R5 : Release 5
R99 : Release 1999
RAB : Radio Access Bearer
RADIUS : Remote Authentication Dial-In User Service
RAN : Radio Access Network
RANAP : Radio Access Network Application Part
RAND : RANDom number (used for authentication)
RFC : Request For Commands
RLC : Radio Link Control
RLCP : Radio Link Control Protocol
RLP : Radio Link Protocol
RM : Resource Management
RNC : Radio Network Controller
RNSAP : Radio Network Subsystem Application Part
RRC : Radio Resource Control
RSVP : Resource Reservation Protocol
RTP : Real Time Protocol
RTCP : Real Time Control Protocol
S-CSCF : Serving CSCF
SA : Security Association
SCCP : Signalling Connection Control Part
SCTP : Streaming Control Transport Protocol
SDES : Source Descriptor
SDP : Session Description Protocol
SDU : Service Data Unit
SEG : Security Gateway
SGSN : Serving GPRS Support Node
SGW : Signalling Gateway
SigComp : Signalling Compression
SIGTRAN : Signalling Transport
SIM : GSM Subscriber Identity Module
SIP : Session Initiation Protocol
SMS : Short Message Service
SPI : Security Parameter Index
SRES : Signed RESponse (authentication)
SS7 : Signalling System No. 7
SSL : Secure Socket Layer
TCP : Transmission Control Protocol
TDD : Time Division Duplex
TDM : Time Division Multiplex
TE : Terminal Equipment

TEID	:	Tunnel End Point Identifier
TLLI	:	Temporary Logical Link Identity
TLS	:	Transport Layer Security
TMSI	:	Temporary Mobile Subscriber Identity
TOS	:	Type of Service
UAC	:	User Agent Client
UAS	:	User Agent Server
UDP	:	User Datagram Protocol
UDVM	:	Universal Decompressor Virtual Machine
UE	:	User Equipment
UL	:	Uplink
UMTS	:	Universal Mobile Telecommunications System
UP	:	User Plane
URI	:	Uniform Resource Identifier
UTRAN	:	Universal Terrestrial Radio Access Network
VoIP	:	Voice Over IP
VLR	:	Visited Location Register
VPN	:	Virtual Private Network
VRID	:	Virtual Router Identity
VRRP	:	Virtual Router Redundancy Protocol
WAP	:	Wireless Application Protocol
WCDMA	:	Wideband Code Division Multiple Access
WTLS	:	WAP Transport Layer Security
WWW	:	World Wide Web
XRES	:	Expected User Response

TABLO LİSTESİ

ŞEKİL LİSTESİ

Sayfa No

UMTS ŞEBEKESİ'NDE IP

ÖZET

Telekomünikasyon teknolojisi, büyük bir ivme ile gelişmekte ve kullanım alanı giderek yaygınlaşmaktadır. Mobil telekomünikasyon sistemleri, kullanıcılara yer ve konumdan bağımsız olarak iletişim kurma imkanı sağlayan haberleşme sistemleridir. UMTS (Evrensel Mobil Telekomünikasyon Sistemi), standartları 3GPP çalışma grubu tarafından oluşturulan 3. nesil mobil iletişim sistemidir. UMTS'in amacı, mobil kullanıcıların daha yüksek hızlarda iletim yapmasını ve zengin içeriklere sahip uygulamaları kullanabilmesini sağlamaktır.

İnternet, yakın geçmişte hayatımıza giren ve günümüzde dünya çapında yaklaşık 1,3 milyar kişi tarafından kullanılan bir haberleşme ağıdır. IP (Internet Protocol) ise İnternet sisteminde kullanılan temel bir protokoldür. Sektördeki teknolojik gelişmeler ve artan talepler sonucunda, telekomünikasyon şebekeleri ve sunulan hizmetler çok çeşitli hale gelmiştir. İdeal olan, tek bir şebeke üzerinden farklı tiplerde trafiğin ve hizmetlerin sunulabilmesidir. Mobil şebekeler ile sabit şebekeleri ortak bir yapıda buluşturmak, ideal şebeke yapısına ulaşmamızı sağlayacaktır. TÜM-IP şebekesi, yakınsama olarak adlandırılan bu gelişmeye örnek teşkil eder.

IP'nin kullanım oranının dünya çapında artış göstermesi, yakınsamayı sağlayacak ortak şebeke yapısının IP tabanlı olmasını gerektirmiştir. Bu yapı ile uçtan uca tamamen IP tabanlı iletim gerçekleştirilebilir. Kullanıcıların İnternet'e konumdan bağımsız olarak her yerde erişme ve hızlı veri iletimi yapabilme talepleri doğrultusunda, UMTS ile IP arasında sıkı bir ilişki oluşmuştur. Bu sıkı ilişki, UMTS şebekesinde, IP'nin kullanım alanını genişletmesini sağlamıştır. UMTS'in aşamalı olarak, IP tabanlı bir şebekeye dönüşümü, TÜM-IP'ye geçişte önemli bir adımdır.

Tez konusu olarak IP'nin, UMTS şebekesinin hangi bölümlerinde kullanıldığı, UMTS'in oluşumundan bugüne kadar olan sürümlerinde, IP'nin kullanım alanının genişlediği bölümler ve IP tabanlı bir UMTS şebekesine geçiş aşamaları ayrıntılı olarak incelenmiştir. UMTS Versiyon 5 (R5) ile uçtan uca tamamen IP tabanlı bir UMTS şebekesine geçiş mümkün olmuştur. R5 ile şebekeye eklenen IP Multimedya Alt Sistemi (IMS) bu geçişte önemli bir rol oynamıştır. IMS ile birlikte, IP uygulamaları belirli bir standarda kavuşturulmuştur.

Günümüzde UMTS şebekeleri büyük çoğunlukla ATM tabanlı olarak hizmet vermektedir. Sabit şebekelerde IP kullanım oranının büyük artış göstermesi, kullanıcıların mobil olarak da aynı hız ve kalitede bu hizmeti almak istemeleri, IP'nin UMTS şebekesindeki gelişimini tetiklemiştir. Genel eğilim ve yapılan çalışmalar, ATM tabanlı iletimden IP tabanlı iletime geçişi destekleyici niteliktedir.

IP IN UMTS NETWORK

SUMMARY

Telecommunication technology makes improvement ve becomes widespread day by day. Mobile telecommunication systems provide subscribers communicate each other without any boundary of location and time. UMTS is a 3rd generation mobile cellular communication system whose standards are made by 3GPP working group. UMTS system's aim is that subscribers can use mobile applications with rich content and increase the communication speed.

Internet is a network which is used by around 1,3 billion people worldwide. IP is a package of standards that used for Internet. Due to increasing demand and technological developements, different types of services can de provided by Intenet nowadays. However, these services are designed for fix network subscribers. Ideal architecture is based on fixed-mobile convergence. All-IP structure is an example of this network type.

Usage of IP has been increasing day by day. Therefore, it is thought that convergence will be based on IP standard natively. Subscribers want to access Internet with high speed not only from their fix neworks bu also from their mobil equipments. The reason of strong relationship between UMTS and IP come from that. To reach the ALL-IP network, UMTS system evolution will be the key point.

In this study, the main subject is IP participaiton in UMTS system as a transport standart and UMTS evolution steps by this point of view. In addition, detailed examination of IP based UMTS structure is done. With UMTS Release 5, end to end IP based UMTS transmission is provided. IP Multimedia Subsystem is added to UMTS core network and this developement has made good improvement in UMTS network structure. IP applications reach a standart with IMS for both mobile and fix IP Networks.

Today, the most popular UMTS system transport standart is ATM. Rise in IP usage, access to information easily and communication with rich content without any restrictive condition, make IP extends in UMTS system. Researches about this manner and tendency about IP cause UMTS evolution in transport layer from ATM towards IP.

1. GİRİŞ

Telekomünikasyon, yaşanan teknolojik gelişmeler ile birlikte, insan yaşamının vazgeçilmez ve temel bir ihtiyacı haline gelmiştir. Gelişmiş ülkeler incelendiğinde, istisnasız hepsinde telekomünikasyon sektörünün gelişmiş olduğu gözlenmektedir. Başka bir deyişle, telekomünikasyon sektöründe yaşanan gelişme ve yenilikler ile ülkelerin gelişmişlik dereceleri arasında sıkı bir korelasyon bulunmaktadır.

Sayısal mobil hücresel telekomünikasyon sistemlerinin temelleri, 1980'li yılların başlarında atılmıştır. 1G olarak adlandırılan 1. nesil mobil telekomünikasyon sistemleri ile başlayan süreç, GSM'in oluşumu ile büyük bir ivme kazanmıştır. Mobil abonelerin zaman ve konumdan bağımsız olarak zengin içerikli, gerçek zamanlı olan ya da olmayan uygulamaları kullanmak ve yüksek hızlarda veri iletimi yapabilmek için oluşturdukları talep doğrultusunda, 1998 yılında 3. nesil Ortaklık Projesi (3GPP) kurulmuştur. 3GPP, 3. nesil mobil iletişim sistemi olan UMTS sistemini ve onun standartlarını oluşturan organizasyondur. Aynı süreç içerisinde, sabit hatlar üzerinden sunulan İnternet ağı dünya çapında genişleyerek günümüzde yaklaşık 1,3 milyar civarında kullanıcıya hizmet verir duruma gelmiştir. Donanım ve yazılım sektöründe yaşanan gelişmeler ile birlikte, artık birçok hizmet İnternet üzerinden verilebilmektedir. İnternet dünyası ile mobil iletişim dünyasında yaşanan bu gelişmeler neticesinde, her iki sistemin bir arada verimli bir şekilde çalışmasını sağlayacak düzenlemelere ihtiyaç duyulmuştur. UMTS şebekesinde IP'nin yer edinmesini ve gelişmesini tetikleyen unsurlar şunlardır:

- Maliyet odaklı yaklaşımda, IP tabanlı bir UMTS sistemi oluşturmanın diğer alternatiflere oranla daha ucuza mal olması (İnternetin yaygın kullanılması, IP şebeke elemanlarının maliyetini düşürmüştür)
- İnternet dünyasında sunulan hizmetlerin aynı şekilde mobil şebekelerde de sunulabilmesi olanağı
- IP şebekelerinde yapılan yeniliklerin, mobil şebekelerde de kolay uygulanabilir hale gelmesi

- IP'de, son dönemde özellikle gerçek zamanlı iletişimin belirli bir kalitede sunulabilmesi ile ilgili çalışmaların yoğunlaşması sonucunda UMTS'te IP'nin yaygınlaşabilmesine olanak sağlanması
- Operatörlerin gelecekte kablosuz ağlara entegrasyonunun, IP tabanlı şebeke ile basit olarak sağlanabilmesi

Yapılan bu çalışmada, IP'nin UMTS şebekesindeki yeri ayrıntılı olarak incelenmiş, günümüze gelene kadar UMTS sisteminde yapılan ve yapılmakta olan değişim ve gelişim aşamaları çeşitli yönleriyle ortaya konmuştur. Tezde genel çerçeve, UMTS sisteminin kendisi değil, IP'nin UMTS üzerindeki değişim ve gelişim alanlarına etkisi olarak çizilmiştir.

2. bölümde, UMTS sisteminin genel şebeke özellikleri incelenmiş; mobil haberleşme sistemlerinin kısa tarihçesi aktarılmıştır. Ek olarak bir UMTS şebekesindeki şebeke elemanları, bu elemanlara ilişkin yürütülen fonksiyonlar ve elemanlar arasıdaki bağlantıları sağlayan arabağdaşımlar belirtilmiştir.

3. bölümde, IP protokolü genel özellikleri ile ele alınmış; OSI katmanlı yapısında şebeke katmanı ve taşıma katmanına ilişkin bilgi verilmiştir. Son kısımda ise, IPv4 adreslerinin kısıtlanması ve IPv4'ten IPv6'ya geçiş incelenmiştir.

4. bölümde, UMTS'e ait ilk sürüm olan Sürüm 99 (R99), IP standardı çerçevesinde incelenmiş; ilk kısımda UMTS R99 genel şebeke özellikleri aktarılmıştır. Daha sonra, UMTS şebekesinde IP standardının kullanıldığı şebeke bölümleri ele alınmıştır. GPRS çekirdek şebekesi, IP standardı yönünden incelenmiş ve bağlantı kurulumlarına ilişkin protokoller açıklanmıştır. Son kısımda ise, IP'nin UMTS'e getirdiği güvenlik ve QoS mekanizmaları üzerinde durulmuştur.

5. bölümde, UMTS'e ait 2. sürüm olan UMTS R4 konusu işlenmiştir. İlk kısımda UMTS R4'e ilişkin şebeke yapısı ve R4 ile birlikte UMTS şebekesinde uygulanan softswitch mimarisi incelenmiştir. Softswitch mimarisi sayesinde kontrol ve kullanıcı verisi ayrı ayrı iletilmeye ve işlenmeye başlanmıştır. Bu ayrım sonucunda, farklı birimlerin birbirlerini kontrol etmesi için MEGACO (Medya Geçit Kontrol) protokolü benimsenmiştir. R4'ün UMTS'e getirdiği bir diğer yenilik, taşıyıcıdan bağımsız çağırma kontrolü yapılabilmesidir. Böylece, çekirdek şebeke içerisinde ATM, TDM veya IP tabanlı iletim yapılabilmesi mümkün olmuştur. Bu gelişme ile gerçek zamanlı trafiğin IP domeni üzerinden iletilmesi elverişli hale gelmiştir. Bu

tezde IP tabanlı yapı üzerinde durulmuştur. Ayrıca, VoIP ve RTP hakkında bilgi verilmiştir.

6. bölümde UMTS'in bir sonraki sürümü olan UMTS R5 ayrıntılı olarak incelenmiş ve R5 ile birlikte UMTS şebekesine katılan IP Multimedya Alt Sistemi (IMS) derinlemesine işlenmiştir. Bu bağlamda, Oturum Başlatma Protokolü, Oturum Açıklama Protokolü ve Genel Açık Denetim Hizmeti protokolü detaylı olarak incelenmiştir. Daha sonra, işaretleşme işaretlerinin iletimini sağlamak amacıyla oluşturulan işaretleşme iletimi (SIGTRAN) protokolü hakkında bilgi verilmiştir. Son kısımda ise, Radyo Erişim Şebekesi'nde IP'nin kullanımı incelenmiştir.

Sonuçlar bölümünde, yapılan çalışmada varılan sonuçlar ve geleceğe ilişkin yorumlar yer almaktadır.

2. UMTS SİSTEMİ VE ÖZELLİKLERİ

2.1. UMTS Sisteminin Genel Özellikleri

Hücresel mobil sistemlerin temelleri, 1G olarak adlandırılan standartlar ile 1980'li yılların başında ortaya çıkmıştır. İlk sistemlerin özelliği; analog, FM kullanan, tam dupleks hücresel mobil haberleşme hizmeti sunmalarıdır. Bu sistemlere örnek olarak; 800 MHz frekans bandına çalışan ve Amerika'da geliştirilen hücresel bir sistem olan İleri Mobil Telefon Sistemi (AMPS), 450 ve 900 KHz'de çalışan ve Avrupa'da oluşturulmuş bir sistem olan Nordic Mobil Sistemi (NMT) verilebilir. 1987 yılında, Avrupa'da "Groupe Speciale Mobile" adlı grubun çalışmaları sonucunda, kısaca GSM (Mobil İletişim için Evrensel Sistem) olarak bilinen 2G standardı oluşturulmuştur. GSM, iletişimde bir devrim gerçekleştirmiş, bugün dünyada milyonlarca aboneye hizmet sunan bir standart haline gelmiştir. 1998'de GPRS ve sonrasında EDGE standartları ile birlikte İnternet, mobil şebeke içerisine dahil olmuştur. 3G standartizasyon çalışmaları, 1998'de kurulan 3. Nesil Ortaklık Projesi (3GPP) tarafından yürütülmüştür. 3GPP, temel olarak GSM'i geliştirme yöntemi izlemiş ve UMTS'i buna göre şekillendirmiştir. 2000 yılı Mart ayında, UMTS'e ilişkin ilk sürüm (R99) oluşturulmuş, 2001 Mart ayında ikinci sürüm olan UMTS R4, 2003 yılı ortalarında ise UMTS R5 standartlarını geliştirilmiştir. 2004 yılı 2. çeyreğinde ise R6 standartları tamamlanmıştır.

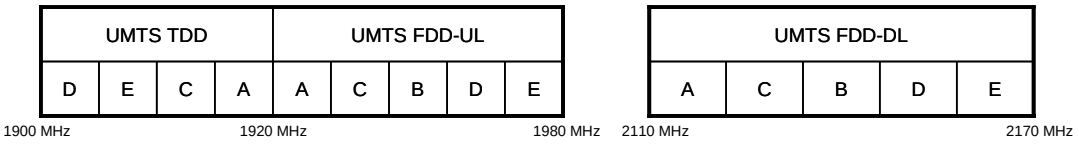
UMTS'in ortaya çıkmasının ana nedenleri aşağıdadır:

- Ses-dışı servislere artan yoğun ilgi
- İnternet'in mobil şebekelerde kullanım oranının artması
- Sabit şebekelerde alınan hizmetlerin mobil şebekelerde de talep edilmesi
- Yüksek hızlarda veri iletim gereksinimi
- Mobil uygulama içeriklerinin zenginleşmesi
- İletim bandının verimli kullanılması

- GSM pazarının doyuma ulaşması sonucu operatörlere yeni gelir kaynağı yaratması
- Genişband iletimin mobil şebekelerde uygulanmasına olanak tanınması

UMTS, kodlama tekniği olarak Genişband-CDMA (WCDMA) kullanır. Bu teknik, aynı frekansı birçok abonenin aynı anda kullanmasına imkan sağlar. Aboneleri birbirlerinden ayıran özellik, kullanıcıların her birinin ortogonal (dik) kodlarla temsil edilmeleridir.

UMTS'te bir taşıyıcının frekans bant aralığı 5 MHz'dir. Bir taşıyıcı ile bir mobil şebeke, tüm aboneleri arasında iletişim sağlayabilir. Kapasite ihtiyacı ve birden fazla mobil operatörün kullanması amacıyla toplam 60 MHz'lik bant genişliği UMTS FDD için ayrılmıştır. Şekil 2.1'de UMTS FDD ve TDD için ayrılan frekans bandları verilmiştir. Lisanslar 5 sınıfa ayrılmıştır. Bu sınıflar da aynı şekil içerisinde verilmiştir.



Şekil 2.1 : UMTS Lisans Frekansları

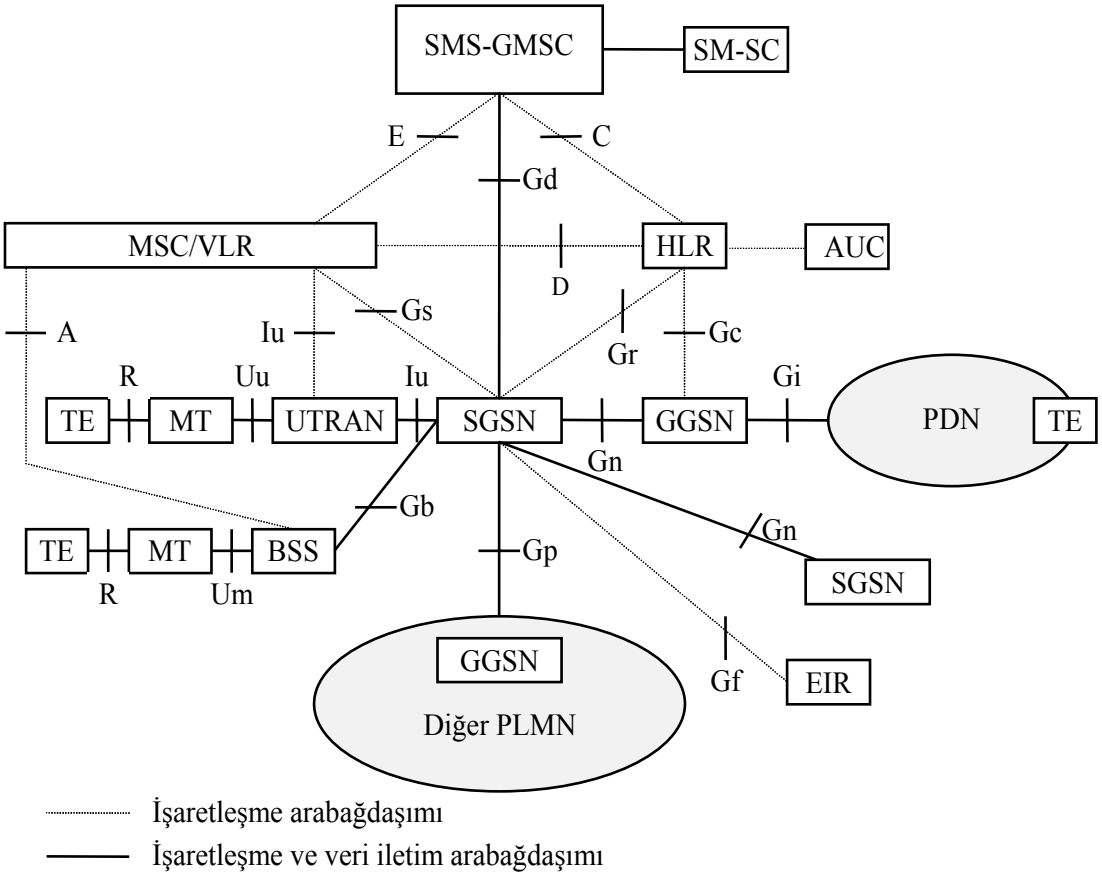
UMTS'in, CS ve PS domeninde sağladığı hız limitleri Tablo 2.1'de verilmiştir. Buna göre veri iletişiminde aşağı yönde (downlink) 384 Kbit/sn'ye kadar hız desteklenmektedir.

Tablo 2.1 : UMTS Sistemi CS ve PS Hız Limitleri

DEVRE BAĞLAŞMASI		PAKET BAĞLAŞMASI		
12.2 (Kbit/sn) (SES)	64 / 64 (Kbit/sn) (UL / DL)	64 / 64 (Kbit/sn) (UL / DL)	64 / 128 (Kbit/sn) (UL / DL)	64 / 384 (Kbit/sn) (UL / DL)

2.2. UMTS Şebeke Elemanları

UMTS Şebekesi, 2 ana domenden oluşur. Bunlar Devre Bağlaşmalı (CS) Şebeke ve Paket Bağlaşmalı (PS) Şebeke'dir. Her iki domeni de içeren UMTS Şebeke Mimarisi'ne ilişkin yapı ve arabağdaşımlar Şekil 2.2'de verilmiştir. Bazı birimler sadece bir domende, bazıları ise her iki domende de görev alır.



Şekil 2.2 : UMTS Genel Şebeke Yapısı

2.2.1 MSC – Mobil Hizmetler Bağlaşma Merkezi

Mobil Hizmetler Bağlaşma Merkezi, UMTS şebekesindeki bağlaşma ve yönetim fonksiyonlarını yürüten önemli bir birimdir; bir MS'e ulaşılmak istendiğinde, bu isteği işler ve MS'e verinin yönlendirilmesini sağlar. CS domeninde görev alır. Kullanıcı verisi ve kontrol işaretleri bu birim üzerinden işlenir. Diğer görevleri;

- Doğrulama
- Mobilite yönetimi
- Bağlaşma fonksiyonları

- Kullanıcı verisini işleme
- Taşıyıcı kurulumu ve yönlendirilmesi

MSC, genellikle şebekede VLR ile bir arada bulunur.

Geçit MSC ise, aynı fonksiyonlara sahip olup, dış şebekeler (Ör: PSTN, ISDN) ile arabağdaşım oluşturan birimdir.

2.2.2. VLR – Ziyaretçi Yeri Yazıcısı

VLR, HLR'a benzer bir veritabanıdır. MSC ile birlikte aynı lokasyonda bulunur. Bağlı olduğu MSC'nin bölgesindeki abonelere ilişkin geçici kayıtları tutar. MSC, MS'te bir bilgi güncellemesi olması durumunda VLR'daki veritabanını kullanır. Aksi taktirde HLR'dan gerekli bilgiyi alır ve aynı zamanda VLR da güncellenir ve en son bilgiler VLR'da tutulur. VLR da HLR gibi her iki domende de kullanılır.

2.2.3. HLR – Lokal Yer Yazıcısı

HLR, bir UMTS şebekesindeki ana veritabanını oluşturur. Abonelere ilişkin tüm bilgiler bu veritabanında saklanır. Bu bilgilerden bazıları, Uluslararası Abone Kimlik Numarası (IMSI), yetkilendirme anahtarı, aboneye özel kullanıcı hizmetlerdir. HLR, hem CS hem de PS domeninde kullanılır.

2.2.4. SGSN – Hizmet Eden GPRS Destek Düğümü

SGSN, GPRS'in GSM'e eklenmesi ile şebekeye katılan bir birimdir. Sadece PS domeninde kullanılır. Görevi,

- Paketleri işleme
- Yönlendirme
- Doğrulama
- Mobilite yönetimi
- Şifreleme
- Sıkıştırma

SGSN, PS domeni ile ilgili hizmetlerin sunulması ile ilgili abone bilgilerine erişmek için VLR ve HLR ile iletişim halinde olur.

2.2.5. GGSN – Geçit GPRS Destek Düğümü

Dış şebekeler (Ör: IP şebekesi) ile UMTS şebekesi arasında arabağdaşım görevi üstlenir. GGSN de SGSN gibi GPRS'in oluşumu ile birlikte şebekeye yeni katılan bir elemandır. O da sadece PS domeninde görev alır. Başlıca görevleri;

- Dış şebekelerden gelen ve dış şebekelere gidecek paketlerin yönlendirilmesi
- Kod-format dönüşümü
- Güvenlik hizmetlerinin sunulması
- IP adres yönetimi

2.2.6. RNC – Radyo Şebeke Kontrolörü

Radyo Erişim Şebekesi'nin bir elemanı olan RNC, MSC ile Node B arasıdaki bağlantıyı sağlayan birimdir. RNC, erişim şebekesinin en üst düzey şebeke elemanıdır. Kendisine bağlı Node B'lerin kontrolü RNC'te aittir. UMTS'in GSM'de olmayan bir özelliği, RNC'lerin birbirlerine bağlanabilmesidir. Yüksek hızlarda iletişime imkan sağladığı ve yazılımsal özellikleri yoğun olduğu için yüksek kapasiteli işlemciler barındırır.

2.2.7. Node B

Node B, UMTS şebekesinin son uç birimidir ve hava arabağdaşımını kullanarak MS ile iletişim kurar. GSM'deki karşılığı BTS'tir. UMTS sisteminin gerekliliklerini karşılayacak teknik özelliklere sahiptir.

2.2.8. EIR – Cihaz Kimlik Kaydı

EIR bir veritabanı olup, içeriğinde mobil cihazların durumlarına ilişkin bilgiler bulunur. Beyaz, gri ve siyah olmak üzere 3 liste bulunur ve mobil cihazlar, IMEI numaralarına göre bu listeye yazılırlar. EIR'ın amacı, yasal olmayan (Ör: Çalıntı) cihazların tespit edilmesini sağlamaktır.

2.2.9. AUC – Doğrulama Merkezi

AUC, mobil cihazların UMTS şebekesi içerisinde çeşitli elemanlar tarafından doğrulanması sırasında kullanılır. Bir tür veritabanıdır. İçeriğinde, abonelere ait şifre bilgileri, onları üretmek için kullanılan algoritmalar bulunur. Direk HLR'a bağlıdır.

Herhangi bir şebeke elemanı, doğrulama talebinde bulunduğunda, bu isteği HLR'a iletir ve HLR da AUC'dan gerekli bilgileri alarak ilgili şebeke elemanına bilgi sağlar.

2.3. UMTS'teki Arabağdaşımlar

A arabağdaşımı, MSC ile BSC arasında kullanıcı trafiği taşımak amacıyla kullanılan arabağdaşımdır.

Iu arabağdaşımı 2 kısımdan oluşur. CS domenine ilişkin verinin iletimi için Iu-CS, PS domenindeki verinin iletimi için ise Iu-PS arabağdaşımı kullanılır. Radyo Erişim Şebekesi ile MSC arasında kullanılır.

Gs arabağdaşımı, SGSN ile MSC / VLR çifti arasında kullanılır. SGSN, Gs arabağdaşımını yönlendirme alanı ve lokasyon alanı bilgilerini güncellemede VLR ile haberleşmek için kullanır.

D arabağdaşımı, MSC ile HLR arasındaki iletişimi sağlar. MSC, HLR'dan abone ile ilgili bilgileri bu sayede alır.

Gn arabağdaşımı, SGSN ile GGSN arasındaki iletişimi sağlar. Gn arabağdaşımında GTP protokolü uygulanarak hem kontrol işaretleri (GTP-C), hem de kullanıcı verisi (GTP-U) iletilir.

Gr arabağdaşımı, SGSN ile HLR arasında bulunur. SGSN, abone bilgilerine ihtiyaç duyduğunda HLR'dan gerekli bilgileri bu arabağdaşım üzerinden temin eder.

Gb arabağdaşımı, BSC ile SGSN arasındaki iletişim sağlar. GPRS kontrol-kullanıcı işaretlerinin iletimi bu arabağdaşım ile gerçekleştirilir.

Gp arabağdaşımı, GSN birimleri farklı şebekelerde ise bu birimler arasında kullanılan arabağdaşımdır.

Gi arabağdaşımı, GGSN ile dış IP şebekeleri arasında kullanılan arabağdaşımdır. IP paketlerinin dış şebeke ile UMTS şebekesi arasında iletimi bu arabağdaşım ile yapılır.

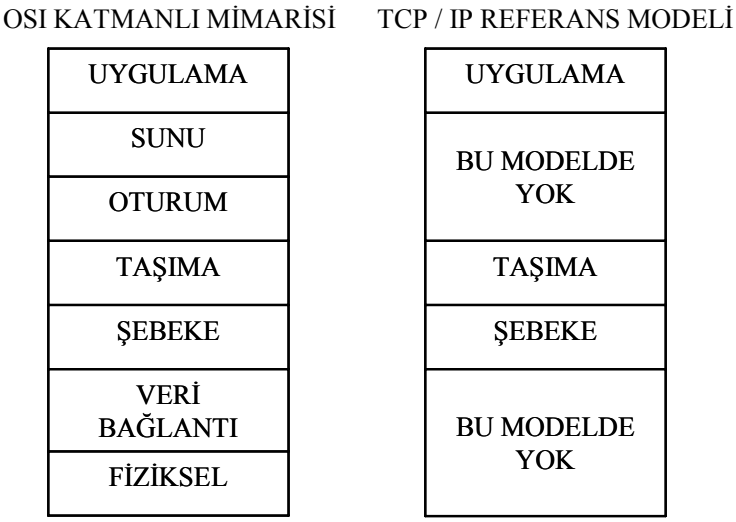
Gc arabağdaşımı, GGSN ile HLR arasındaki bağlantıyı sağlar. GGSN, abone ile ilgili bilgi ihtiyacı olduğunda bu arabağdaşımı kullanır.

3. IP STANDARDI

3.1. IP Protokolünün Genel Özelikleri

İnternet Protokolü'nün (IP) temelleri, 1969 yılında A.B.D. Savunma Bakanlığının iletişim alanında yaptığı çalışmalar ile atılmıştır. Bu çalışmaları yürüten grup ARPANET adını almış ve 1982'de TCP / IP protokol ailesini standart olarak oluşturmuş ve kabul etmiştir. Sonrasında günümüze kadar yapılan geliştirmeler ile bugün dünya çapında yaklaşık 1,3 milyar kişinin kullandığı bir şebeke protokolü haline gelmiştir.

OSI Referans modeli ile TCP / IP referans modeli kıyaslandığında, katmanlı yapıda Şekil 3.1'deki durum ortaya çıkar. Bu iki yapı katmanlar seviyesinde birebir örtüşmez.



Şekil 3.1 : OSI Katmanlı Mimarisi ile TCP / IP Referans Modeli

IP, bu modelde şebeke katmanı protokolü olarak kullanılır. Bir üst katman olan taşıma katmanında ise genellikle TCP ve UDP kullanılır.

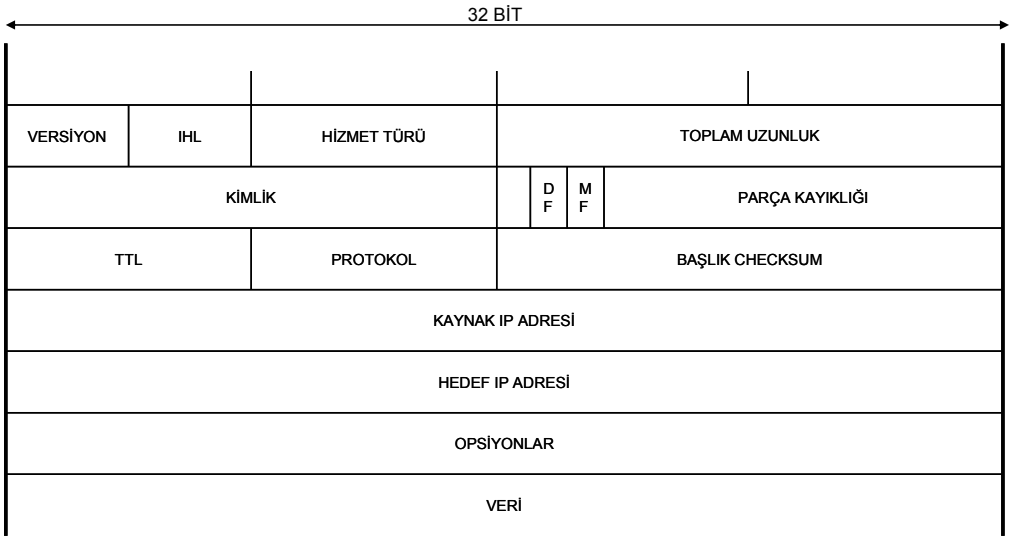
3.2. IPv4 Yapısı

OSI katmanlı mimarisi baz alındığında, IPv4'te en önemli iki katman Şebeke Katmanı ve Taşıma Katmanı'dır. Bu alt bölümde her iki katman incelenmiştir.

3.2.1. Şebeke Katmanı

Şebeke katmanının amacı, kaynak uçtan hedef uca verinin yönlendirilmesini ve iletilmesini sağlamaktır. Bir şebeke katmanı protokolü olan IP de aynı amaca hizmet eder. IP, iletim yapmak için paket bağlaşmalı şebekeleri kullanır; bağlantısız bir protokol olup, paket iletilmeden önce uçtan uca bağlantı kurulmaz. IP'de her şebeke elemanına lojik bir adres atanır. Bu adres sayesinde, iletilecek paket, şebeke içerisinde yönlendiriciler vasıtasıyla hedef uca gönderilir.

Bir IP paketine (IPv4) ilişkin paket formatı Şekil 3.2'de verilmiştir.



Şekil 3.2 : IPv4 Paket Formatı

İdeal halde, 2^{32} = yaklaşık 4 milyar IP adresi vardır. Fakat bu adreslerin bir kısmı çeşitli nedenlerle rezerve edilmiştir. Bir sonraki versiyon olan IPv6'da ise IP adreslerinin sayısı = 2^{128} adet olmuştur. Bölümün son kısmında bu konu incelenmiştir. IPv4 adresleri 5 sınıfa ayrılmıştır. IP adres formatı ve sınıflar Şekil 3.3'te verilmiştir.

Şekil 3.3 : IPv4Adres Formatı ve Adres Sınıfları

3.2.2 Taşıma Katmanı

Taşıma katmanı, şebeke katmanının bir üst seviyesinde bulunur. Bu katmanda genel olarak en sık kullanılan 2 protokol İletim Kontrol Protokolü (TCP) ve Kullanıcı Datagram Protokolü'dür (UDP).

3.2.2.1 TCP – İletim Kontrol Protokolü

TCP protokolünün görevi, iki uç birimi arasında uygulama katmanındaki verinin karşılıklı iletimini sağlamaktır. TCP'nin özellikleri;

- Bağlantı Yönelimli olma
- Tekrar iletim
- Akış kontrolü
- Yığılma Kontrolü
- Güvenlik
- Sıralı iletim

TCP, uç birimlerinde bulunan ve soket adı verilen alt birimler arasında uygulanır. Her soket, kendi host'una ait IP adresi ile port nurumarasından oluşan toplam 48 bit'lik bir numaraya sahiptir. Port, TCP segmentinde bulunan ve 16 bit uzunluğunda bir numaradır. Portlar, uygulamaları adreslemek için kullanılır. Örnek olarak FTP için 21 no'lu port, http için 80 no'lu port kullanılır.

3.2.2.2 UDP – Kullanıcı Datagram Protokolü

UDP, bağlantı yönelimli olmayan bir iletim sağlar. TCP'ye göre daha az işaretleşme sayesinde daha hızlı iletim imkanı verir. Fakat TCP'nin yukarıda verilen özelliklerinin hiçbiri UDP'de yoktur. Bir istek-cevaptan oluşan veya düşük trafik yaratacak uygulamalar için bir bağlantı kurup çözmek yerine UDP'yi kullanmak hem daha hızlı iletim sağlar, hem de şebekeye daha az işaretleşme yükü getirir.

3.3. IPv4 Adres Kısıtlaması

GPRS sisteminin mobil operatörlerde IP kullanımını artırması ve dünyadaki sabit-mobil IP şebeke kullanıcılarının günden güne artması nedeniyle, yakın gelecekte IPv4'te adres tahsisi sıkıntısı yaşanması gündeme gelmiştir. Birçok IP adres aralığı gelecekte kullanılması amacıyla büyük İnternet servis sağlayıcıların elinde bulunmaktadır. IP adreslerindeki sıkıntıyı gidermek amacıyla 2 standart geliştirilmiştir.

3.3.1. DHCP – Dinamik Host Konfigürasyon Protokolü

Bu protokolün ana mantığı aynı anda IP servislerini her kullanıcının kullanamayacağı yaklaşımına dayanır. Örneğin bir MS kapalı olabilir veya açık olup aktif bir veri alışverişi yapmıyor olabilir. Bu durumlarda MS'e bir IP atamak gereksizdir. ISP'ler belirli sayıda IP adresini havuz olarak kullanırlar. Bir kullanıcı IP servisi almak istediğinde, ISP ona dinamik olarak kendi IP havuzundan bir adres atar ve oturum bittiğinde IP adresi serbest kalır. Bu sayede kaynak verimli kullanılmış olur. GPRS'te de bir MS, PDP bağlantı aktivasyonu istediğinde, HLR'da ayrı bir tanımlama yapılmadığı sürece DHCP ile dinamik bir IP adresi atanır. MS, bir dış IP şebekesine (Ör: İnternet) bağlanmak istediğinde DHCP, GPRS IP omurgasından bir IP adresi atar. MS anlaşmalı bir intranete bağlanıyorsa, o şebekeye ait IP adresini kullanabilir.

3.3.2 NAT - Şebeke Adres Tercümesi

IP adresleri düşünüldüğünde, DHCP bu adresleri verimli kullanma yöntemi olarak görülebilir. Fakat sayısal olarak IP adreslerinin sayısı değişmez. Örneğin, A şebekesi C sınıfı şebeke adreslemesi kullansın. Bu şebeke 254 IP adresini kullanabilir. UMTS

gibi milyonlarca abonesi olan operatörler, çok daha fazla sayıda IP adresine ihtiyaç duyar.

Tablo 3.1'deki IP adresleri, şebeke içerisinde kullanılabilir adreslerdir. Bu adresler operatöre ait şebeke altyapısı içerisinde dış IP şebekelerine bağlanılmadığı sürece kullanılabilir. Fakat dış IP şebekelerine bağlanıldığında, her kullanıcıya tek IP adresi atanır. Bu sorunun üstesinden gelebilmek için, şebeke içerisinde bir abone PDP bağlantısı kurmak istediğinde, DHCP'ye göre şebeke içi IP adresi atanır.

Tablo 3.1 : UMTS Sistemi İçerisinde Kullanılabilir Adresler

SINIF	ADRES
A	10.0.0.0
B	172.16.0.0 – 172.31.0.0
C	192.168.0.0 – 192.168.255.0

Kullanıcı dış şebekeye geçmek istediğinde NAT, bu iç IP adresini dış IP adresine dönüştürür. Genellikle dinamik tercüme yapılır. NAT işlemi, farklı birimlerde yapılabilmesine karşın genellikle GGSN'lerde gerçekleştirilir. Bir TCP veya UDP paketi, 16 bit'lik port numarasına sahiptir. Bu durum, bir IP adresine $2^{16} = 65536$ farklı port bağlanmasına olanak tanır. Bunların bir kısmı kısıtlansa da çok büyük bir bölümü NAT için kullanılır. Bu sayede tek bir dış IP adresine birçok cihaz aynı anda bağlanabilir. NAT'ın 2 dezavantajı vardır. Birincisi, NAT işlemini gerçekleştiren işlemcinin gücünün sınırlı olmasıdır. Aynı birim, farklı görevleri de aynı anda yürütürse, güç kısıtlaması nedeniyle problem yaşanabilir. Diğer dezavantaj ise NAT'ın UDP'de kullanımı ile ilgilidir. UDP, bağlantı yönelimli bir yapıya sahip olmadığı için, bir çeviri girişi olduğunda, oturumla ilgili herhangi bir bilgi olmadığından, kesilmesi gereken bir giriş için belirli bir süre (timeout mekanizması) beklenmesi gerekir ve bu sürede adres gereksiz yere kullanılmış olur.

3.4. IPv4 – IPv6 Geçişi

IPv4, günümüzde geçerli olan ve İnternet ağını oluşturan şebeke katmanı protokol versiyonudur. IP, oluşumundan itibaren büyük bir yaygınlaşma sürecine girmiş, tahmin edilemeyecek boyutlarda dünya çapında kullanım alanına sahip olmuştur. IPv4'ün bir üst versiyonu olan IPv6'ya geçişin en önemli nedeni, IPv4 adreslerinin yakın gelecekte yetersiz kalacak olmasıdır. Buna ek olarak, IPv6 ile gelen yenilikler ve geliştirmeler aşağıdadır:

Başlık formatının basitleştirilmesi : IPv6'da paket başlığı IPv4'e göre basitleştirilmiştir. IPv6, IPv4'e göre 4 kat fazla adres bitine sahip olmasına rağmen toplam başlık uzunluğu kıyaslandığında IPv4'e göre 2 kat artış vardır. IPv4'te başlık alanı 20 oktet iken, IPv6'da bu alan 40 oktettir. IPv4'teki bazı başlık alanları çıkarılmış, bazıları ise "uzatma başlık" alanında konumlandırılmıştır.

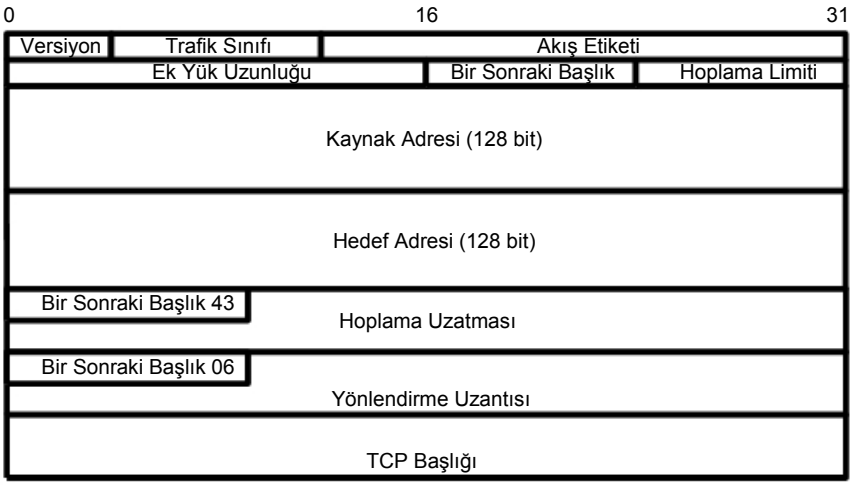
Uzatma başlık kavramının oluşumu : IPv6 ile birlikte uzatma başlık (extension header) kavramı oluşturulmuştur. IPv6'da birçok özellik, bu başlık kısımlarında yerleştirilir. Bu sayede gereksiz başlık kullanım oranı minimize edilmesi amaçlanmıştır.

Doğrulama ve gizlilik : IPv6'daki uygulamaların tümünde paketi alan uç, gönderen ucu doğrular. Birçok durumda da paket içeriği şifrelenerek gönderilir.

Mobilite desteği : IP mobilitesi, IPv4'e göre daha basit ve daha efektif olarak sağlanır. UMTS sisteminde IP mobilitesinin uygulanması, 3GPP tarafından çalışmaları yürütülen ve henüz yaygınlaşmamış bir standardizasyondur.

QoS yeteneğinin gelişmesi : UMTS sistemindeki trafik sınıflandırmasına benzer bir sınıflandırma, IPv6 ile birlikte oluşturulmuştur. Uç biriminin isteği doğrultusunda, faklı türde hizmet alınması istenen bir uygulamaya ilişkin trafik akımına ait paketler etiketlenerek faklı şekilde hizmet sunulabilme (hizmet gereksinimi göz ününde bulundurularak) olanağı tanınır. Örnek olarak UMTS şebeke içerisinde, VoIP trafiğine farklı şekilde hizmet sunulabilir.

Ipv6 paket başlığı Şekil 3.4'te verilmiştir. Başlık bölümleri aşağıda kısa açıklamalar ile birlikte belirtilmiştir.



Şekil 3.4 : IPv6 Başlık Formatı

Versiyon : IPV6 için versiyon numarası 6'dır.

Trafik sınıfı : 8 bitlik bu bölüm, IP paketlerini oluşturan veya yönlendiren şebeke elemanlarının bu paketleri önceliklendirmeleri veya trafik sınıflarına ayrımaları amacıyla kullanılır. IPv4'teki eşdeğeri TOS (hizmet tipi) baytıdır. IPv4'teki faklılaştırılmış hizmetler de bu mantığa göre çalışır.

Akış etiketi : Bu bölüm 20 bitten oluşan bir etiket alanıdır. Yenilik ve geliştirme kısmında belirtilen "QoS yeteneğinin gelişmesi" özelliği, bu bölüm ile birlikte sağlanmaktadır. IPv6 şebeke elemanları, başlıktaki bu kısımda belirli bir trafik akımını etiketleyerek, o paketlere faklı tip hizmet sunulması sağlanabilir. Örnek olarak, bir VoIP oturumuna ilişkin paketler, kendine özgü gereksinimlere sahip olması nedeniyle farklı akış etiketine sahip olabilir. Böylece, operatörler çeşitli uygulamalar için faklı tip çözümler sunulabilme olanağına kavuşur.

Ek yük uzunluğu : 16 bitlik bu alan bir tamsayı ile ifade edilir ve IPv6 paket ek yükünün uzunluğunu belirtir.

Bir sonraki başlık : "Uzatma başlık" kavramına bağlı olarak kullanılan ve 78 bit uzunluğundaki bu alan, IPv6 başlığını takiben gelen uzatma başlığının tipini belirler.

Hoplama limiti : IP paketi her yönlendiriciden geçtiğinde bu değer 1 azaltılır ve sıfıra ulaştığında paket atılır.

Kaynak adresi : Paketi oluşturan ucun 128 bitlik adresini temsil eder.

Hedef adresi : Paketin gideceği uca ait 128 bitlik adresi temsil eder.

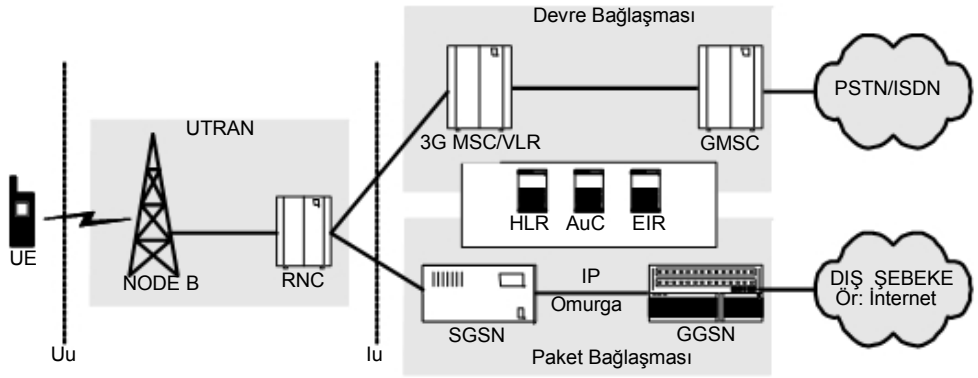
4. UMTS SÜRÜM 99 (R99)

4.1. UMTS R99 Genel Şebeke Yapısı

UMTS R99 sistemi içerisinde IP'nin rolü sadece paket bağlaşmalı (PS) trafiğin taşınmasıyla sınırlıdır. PS trafik şebeke katmanında tamamen IP altyapısı ile taşınmamaktadır. IP, UMTS çekirdek şebekesinde temel olarak 2 alanda kullanılmaktadır. Birincisi mobil ekipman ile diğer IP şebekeleri (ör. İnternet) arasında taşıyıcı mekanizma olarak kullanılması, diğeri ise UMTS çekirdek şebeke elemanları arasında GTP (GPRS tünelleme protokolü) oluşturmak için kullanılmasıdır. Bu yapının en önemli avantajı mobil operatör şebekesini diğer IP şebekelerinden izole etmesidir. Bu sayede mobil kullanıcıların ve harici IP şebekelerin saldırıları kontrol edilebilmiş ve şebeke korunmuş olur.

IP, R99'da UMTS'te radyo erişim şebekesinde (UTRAN) kullanılmamakta; genel olarak şebeke katmanında ATM tercih edilmektedir. ATM adaptasyon katmanı-AAL2 kullanıcı verisini, AAL5 katmanı ise işaretleşme verisini iletmek için kullanılır.

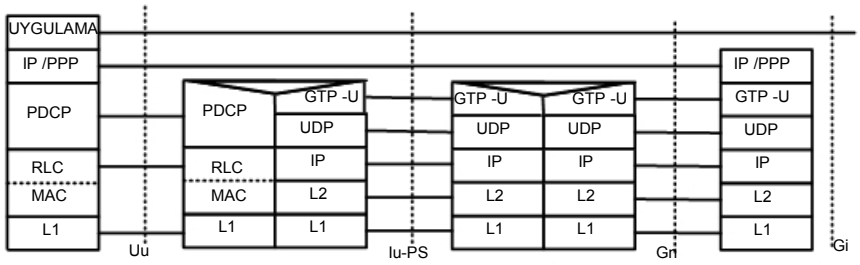
IP; SGSN ile GGSN arasındaki şebeke omurga yapısını, RNC ile SGSN arasındaki Iu-PS arabağdaşımını oluşturur. Şekil 4.1'de UMTS R99 şebeke yapısı verilmiştir.



Şekil 4.1 : UMTS R99 Genel Şebeke Yapısı

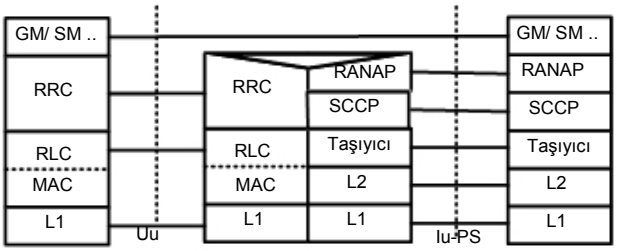
Buna göre CS ve PS trafik için ayrı ayrı şebeke elemanları görev yapmaktadır. UTRAN ile UMTS çekirdek şebeke arasındaki bağlantıyı sağlayan Iu arabağdaşımı iki çeşittir. CS trafiği taşımak için Iu-CS arabağdaşımı, PS trafiği taşımak için Iu-PS arabağdaşımı kullanılır.

Şekil 4.2'de katmanlı yapıda IP'nin kullanıcı düzleminde nasıl kullanıldığına ilişkin şekil verilmiştir.



Şekil 4.2 : GPRS Şebekesinde Kullanıcı Düzleminde IP Protokol Yığını

Şekil 4.3'te ise radyo erişim şebeke uygulama katmanında (RANAP) Iu-PS işaretleşme işaretlerinin iletimine ilişkin katmanlı yapı verilmiştir.



Şekil 4.3 : Iu-PS İşaretleşme İşaretlerinin İletimine İlişkin Protokol Yığını

Bu yapıya göre, şebeke katmanında IP tabanlı veya ATM tabanlı olarak iletim yapılabilir. R99'da ATM, mobil operatörler tarafından daha çok tercih edilen bir yapıdır.

UMTS'te işaretleşme protokolü olarak SS7 kullanıldığı için SS7 işaretleri MTP protokolü (MTP1, MTP2 ve MTP3) ile iletilir. SS7 işaretlerinin IP şebekesi üzerinden taşınabilmesi için 2 protokol geliştirilmiştir. Bunlar SCTP ve M3UA protokolleridir. SS7 ve IP'nin adresleme yapısı tamamen farklıdır. MTP3 adaptasyon katmanı (M3UA), SS7 mesajlarının IP şebekesi üzerinde yönlendirilmesini sağlar.

Aynı zamanda, SS7 kod noktalarının IP adreslerine dönüşümünü gerçekleştirerek IP uç noktalarının SS7 şebeke elemanı gibi fark edilmesini sağlar.

SCTP ise TCP'nin yerini alan bir protokol durumundadır ve SS7 işaretleşmesi için daha uygun bir ortam sunar. SCTP ayrıca her bağlantıya birden çok IP uç noktasının tahsis edilmesini sağlayabildiği için ekstra güvenilirlik sunar. TCP'nin saldırılara karşı savunmasız olmasına karşın SCTP bu saldırılara karşı bağlantıyı korur. Veri hizmeti anlamında bir SCTP bağlantısı üzerinden belirli sayıda veri akışı birbirlerinden bağımsız olarak sağlanabilir. Veri akışı sırasında bir paketin kaybolması nedeniyle o paketi tekrar beklemek gerekmez ve her paket ayrı ve sırasız şekilde iletilebilir. SS7 işaretlerinin IP tabanlı iletimi 6. bölümde (UMTS R5) SIGTRAN (işaretleşme iletimi) başlığı altında daha ayrıntılı incelenecektir.

4.2. PDP Bağlantı Kurulumu

İki mobil terminal arasında veya mobil terminal ile dış şebeke (IP) arasında veri paketlerinin iletilmesi amacıyla oluşturulan protokole, Paket Veri Protokolü (PDP) denir. Paketler karşılıklı iletilmeden önce PDP Bağlantısı kurulması gerekir. Bir PDP Bağlantısı, içeriğinde birçok parametre barındıran bir bütündür. Bunlar; QoS parametreleri, adres bilgileri, sıra numaraları ve bu bağlantıya ait kimlik bilgisidir. PDP Bağlantısı MS ile SGSN ve SGSN ile GGSN arasında kurulur.

Kullanıcı verisine ilişkin paketlerin GPRS şebekesi üzerinden taşınabilmesi için 3 işlemin gerçekleştirilmesi gerekir. İlk aşamada, MS SGSN'e kendi isteği ile bağlanır (attach). İkinci aşamada PDP Bağlantısı kurulur. Son aşamada ise düğümler arasında iletimin sağlanması için GTP kullanılarak paketler kapsüllenir.

Bu iletişimde farklı bit hızları ve geciklemeler yaşanabilir. Veri iletiminde kalite, kullanıcının önceden tanımlanmış QoS profiline göre sağlanır. QoS profili ile ilgili 4 parametre vardır:

Öncelik: Veri iletiminin taahhüt edilme önceliğini temsil eder. Yüksek, orta ve düşük olmak üzere 3 sınıf vardır.

Güvenilirlik: Hizmet veri biriminin (SDU) kayıp olasılığıdır.

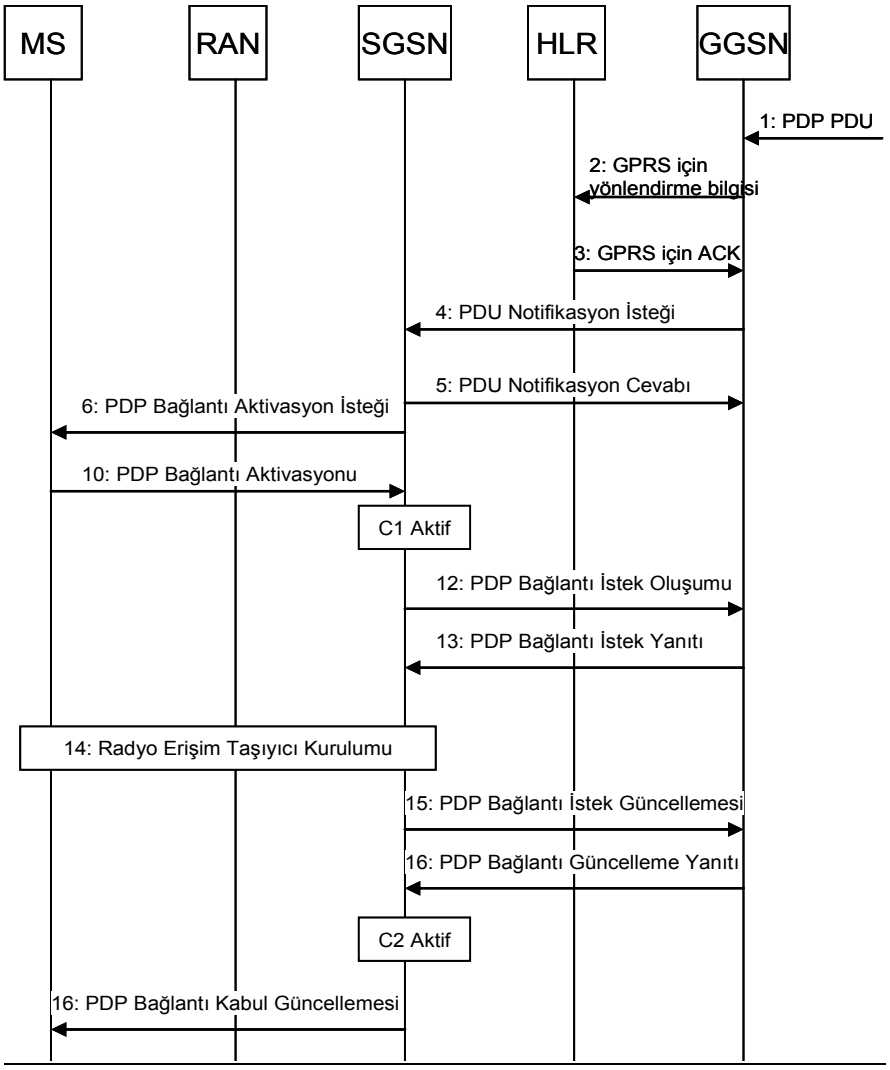
Gecikme: GPRS şebekesi boyunca paketin ortalama gecikmesi

Hız: Ortalama ve maksimum bit hızlarını temsil eder.

Şekil 4.4'te PDP Bağlantı aktivasyonuna ilişkin süreç adım adım verilmiştir.

Dış IP şebekesinden gelen ve MS'te sonlanacak PDP Bağlantı kurulumu bu örnekte incelenmiştir.

1. Dış IP şebekesinden ilk PDU GGSN'e, başka bir deyişle UMTS şebekesine giriş yapar.



Şekil 4.4 : PDP Bağlantı Aktivasyonu

2-3. GGSN, HLR'dan MS'in lokasyonunu sorgular.

4-5. GGSN, SGSN'e bir PDU göndereceği bilgisini verir.

6. SGSN MS'ten PDP Bağlantı aktivasyonu yapmasını ister.

1 ile 6 no'lu arasındaki adımlar, sadece MS'te sonlanacak bir bağlantı durumunda geçerlidir. 10 ile 18 no'lu adımlar arasındaki süreç ise MS'te sonlanan veya MS tarafından başlatılan bağlantı isteklerinde geçerlidir.

10. MS, PDP Bağlantısı kurulum isteğini SGSN'e iletir.

11. MS – SGSN bağlantısı (C1) aktif hale gelir.

12-13. SGSN ile GGSN arasında kurulacak PDP Bağlantı aktivasyonu isteği GGSN'e iletilir.

14-16. Radyo erişim taşıyıcısı (RAB) kurulur ve ihtiyaç olursa PDP Bağlantısı güncellenir.

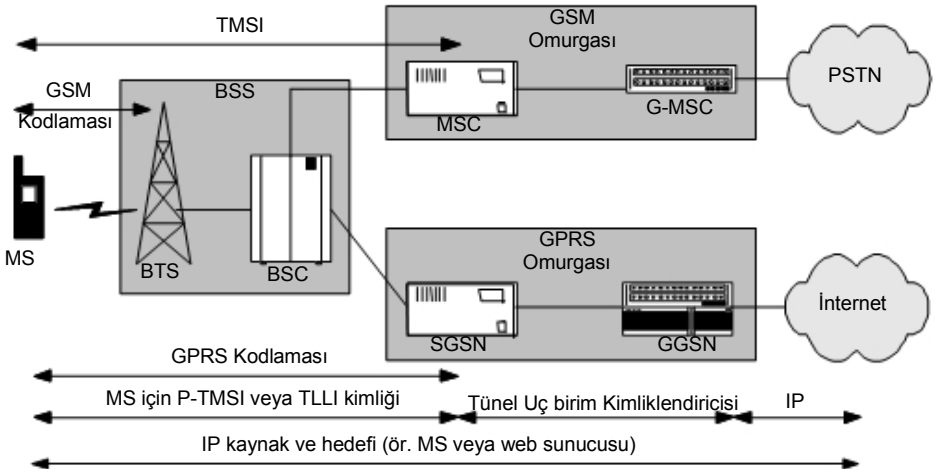
17,18. İkinci PDP Bağlantısı kurulur ve MS bu konuda bilgilendirilir.

4.3. GTP (GPRS Tünelleme Protokolü)

SGSN ile GGSN genellikle aynı lokasyonda bulunur. Bu iki birimin arasında kısa mesafe olması durumunda Ethernet kablosu ile bağlamak mümkündür. SGSN ile GGSN arasındaki mesafe uzak ise, kiralık hatlar veya ATM şebekesi (veri bağlantı katmanı) üzerinden erişim sağlanır. Bir üst katman olan şebeke katmanında IP geçerlidir. İletim katmanında ise UDP protokolü kullanılır. GTP için bu protokol gereklidir. UDP bağlantı yönelimli olmayan bir protokol olduğundan, TCP'ye göre daha hızlı bağlantı kurulmasına olanak tanır. Çekirdek şebekenin güvenilir ve elverişli boyutlandırılması varsıyımı altında UDP kullanılır. GTP versiyon 1'de UMTS çekirdek şebekede IP dışında paketlerin de iletimini sağlayan PPP PDP Bağlantı desketlenmektedir. İlk spesifikasyonda (R97) X.25 protokolüne ait PDP Bağlantı desteklenmekteydi. Fakat bu durumda UDP yerine TCP kullanılması gerekir (paket sıralama-consistency nedeniyle). GTP Versiyon 1'de UDP kullanıldığından X.25 desteği verilmemektedir. GTP V1'de kullanıcı verisinin hedef uç biriminde atanacak port numarası (GTP-U) 2152/UDP Portu, kontrol verisi için ise (GTP-C) 2123/UDP portudur. Kaynak port numarası ise dinamik olarak atanır. GGSN hem 2G hem de 3G GPRS şebekesi ile uyumlu olmak zorunda olduğundan her portu dinlemekle yükümlüdür.

Dünyada GSM sistemlerinde kullanılan her mobil cihazın farklı bir kimlik numarası (IMEI) vardır. Her cihazın kullanıcısı ise IMSI ile kimliklendirilir (SIM kartta

bulunur). Aynı SIM kart, farklı bir UE'ye takılırsa IMSI transfer edilmiş olur. Ücretlendirme ve telefon numarası SIM kart ile eşleştirilir. Mobil cihaz şebekeye bağlanmak istediğinde, IMSI hava arabağdaşımından çekirdek şebekeye ulaşır ve kimlik kontrolü yapılır. Bir kez bu kontrol yapıldıktan sonra geçici kimlik olan TMSI kullanılmaya başlanır. Bunun nedeni, IMSI'nin devamlı hava arabağdaşımında iletilmesi ile bu numaranın güvenilirliğinin tehlikeye atılmasını önlemektir. GPRS çekirdek şebekesinde ise paket TMSI (P-TMSI) kullanılır. Şekil 4.5'te GSM ve GPRS sistemlerinde, IP paketlerinin alt katmanlardaki iletimi için gerekli olan şifreleme ve kimliklendiriciler gösterilmiştir.



Şekil 4.5 : IP Paketlerinin UMTS Sistemi'nde İletimi İçin Gerekli Şifre ve Kimliklendiriciler

Bir GPRS bağlantısında MS, dış dünyadaki bir IP şebekesine bağlanabilmek için bir IP adresine gereksinim duyar. Bu adres şebeke katmanında kullanılmakta olup mobil cihaz için ESI (End system identifier) olarak kullanılmaz. GPRS şebekesi için ESI IMSI'dir. Sabit IP şebekelerinde ESI'nın karşılığı dünyada tek olan MAC adresidir. Bu adres genellikle şebeke donanım arabağdaşımlarında kayıtlıdır. GPRS şebekesinde ise cihazın IP ile MAC adresleri arasında bir bağlantı gereklidir. Bu bağlantı adres çözümleme protokolü (ARP) olarak da bilinen dinamik adresleme protokolü ile sağlanır. Benzer şekilde, GPRS şebekesinde IP adresi ile TEID (veya TMSI veya TLLI) arasında bağlantı gereklidir. GPRS'te ARP'nin eşleniği, IP adresinin GGSN'deki TEID içerisinde adreslenmesidir. Örneğin bir IP şebekesinden GGSN'e gelen IP adresi, GGSN'de TEID ile öncelikle eşleştirilir (bu işlem ARP'de

adres aramaya eşdeğer), GGSN bu işlem sonrasında paketi SGSN'in IP adresine bağlı olarak yönlendirir. SGSN'e paket geldikten sonra TEID, P_TMSI veya TLLI ile eşleştirilir ve ilgili BSS'e yönlendirilir.

GTP 2 ana bölümden oluşur. GTP-C, GTP tünellerinin yaratılması, değiştirilmesi ve silinmesinden sorumlu kontrol işaretlerini, GTP-U ise kullanıcı verisini taşır. Her ikisinin de başlık kısmı minimum 8 byte'dan oluşmak üzere değişkendir. E, S ve PN bitleri, ek alanları belirtir. Şekil 4.6'da GTP başlığı verilmiştir. Versiyon numarası, bu başlığın versiyonunu belirler. R99'da geçerli olan versiyon 1'dir.

Şekil 4.6 : GTP Başlık Formatı

Protokol tipi (PT) biti bu paketin GTP veya GTP^ olduğunu belirtir. GTP^ ücretlendirme için kullanılır. Diğer bitler uzatma (E), sıra numarası (S) ve N_PDU numarasıdır (PN). Mesaj tipi bölümü, iletilecek mesajın tipini belirlemek amacıyla kullanılır. Örneğin PDP bağlantı kurulum isteği, PDP bağlantı silinmesi isteği vs.

4.4. Virtüel Yönlendirici Redondans Protokolü(VRRP)

IP şebeke elemanları her ne kadar güvenilir ve sağlam olsalar da, hatalara karşı güvenli iletişim anlamında geleneksel devre bağlaşmalı şebeke elemanlarına kıyasla daha savunmasız ve az güvenilirdir. Bu problemin üstesinden gelebilmek amacıyla çoğu redondansa dayanan çalışmalar yapılmıştır. Bu yapıya göre yazılım veya donanım olarak her eleman şebekede yedekli olarak kullanılmış ve biri arızalandığında diğeri devreye girmiştir.

IP şebekesinde kilit öneme sahip yönlendiricilerin yedeklenmesi en önemli güvenlik önlemlerinden biridir. Şebeke içi yönlendiricilerin arızalanması, o yönlendirici üzerinden geçecek bağlantıların kopması anlamına gelir. Bir UMTS çekirdek şebekede GGSN'in arızalanması durumunda, şebekenin dış IP şebekeler ile bağlantı sağlayamayacağı açıktır.

IP şebekelerde yaygın olarak kullanılan sistem, yönlendirme işleminin dinamik olarak yapılmasıdır. Bu sayede bir yönlendiricide oluşabilecek arıza durumunda paketler tekrar yönlendirilerek farklı yollardan hedeflenen uç birine ulaşırlar. Bu sistem çekirdek şebekede uygulanması kolay bir yöntemdir fakat bazı sorunlara sebep olur:

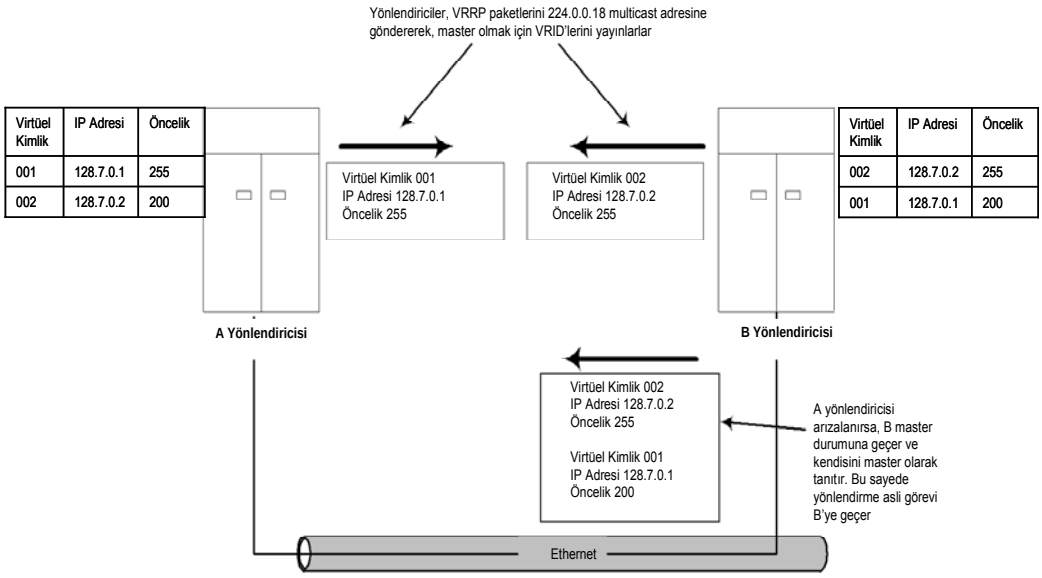
- Sunucular genellikle dış dünyaya tek bir geçitten ulaşırlar. Bu geçit arızalandığında farklı bir geçite paketleri yönlendirebilmek için tekrar konfigüre edilmeleri gerekir.
- Yeni bir yolun kurulması yönlendirme protokolüne bağlı olarak belirli bir zaman alır.
- Birçok şebeke yapısında, diğer şebeke domenlerine ulaşmak için sabit yönlendirme kullanırlar. Bu durumda tekrar yönlendirme mümkün olmaz.

IP şebekelerde redondans protokolü VRRP olarak adlandırılmıştır (RFC 2338). Bu mekanizma ile bir yönlendirici arıza durumunda bir veya daha çok alternatif yönlendirici ile yedeklenebilir. Bir yönlendirici (yedek) diğerinin görevini devraldığında, sadece aynı IP adresini değil ek olarak aynı MAC adresini de alır. Bu durum, diğer IP şebeke elemanlarının bu konfigürasyon değişikliğini bilmeden işlevlerine devam edeceği anlamına gelir. VRRP dizaynı sayesinde çok kısa bir sürede yedekleme işlemi gerçekleştirilir. Protokol şu şekilde işler:

Her fiziksel yönlendirici VRRP koşturarak belirli sayıda virtüel yönlendirici (şebekedeki bir grup sunucu için varsayılan yönlendirici olarak) için sağlayacağı servisleri belirler. Her virtüel yönlendirici bir virtüel yönlendirici kimliğine (VRID) ve bir veya daha fazla (MAC adresine bağlı olarak) IP adresine sahip olur. Her virtüel yönlendirici fiziksel yönlendirici içerisinde 0 ile 255 arasında önceliklendirilir. 255'ten az öncelik verilmiş ise geriye kalan virtüel yönlendiriciler yedekleme amacıyla kullanılır.Her yönlendirici o anki virtüel yönlendiricilerini komşu yönlendiricilere VRRP aracılığıyla iletir ve komşularını günceller. Eğer bir

yönlendirici, virtüel yönlendirici master'ından güncelleme bilgisini belirli bir sürede alamazsa, master'ın yedeği olarak master'lık görevini üstlenir ve komşularına güncelleme bilgisini göndermeye devam eder. Bu durum, Şekil 4.7'da görülmektedir.

A Yönlendiricisi, virtüel yönlendirici numarası 1 ve IP adresi 1238.7.0.1 olan bir master yönlendirici olarak konfigüre edilsin. Yedekleme olarak da virtüel yönlendirici numarası 2, IP adresi 128.7.0.2 ve önceliği 200 olan konfigürasyon verilsin. B yönlendiricisinde ise bu konfigürayonun tam tersi olsun (master'a 2 no'lu, yedeklemeye 1 no'lu virtüel devreler tahsis edilsin). A ve B yönlendiricileri bitişik yönlendiriciler olsun.



Şekil 4.7 : VRRP Uygulama Örneği

Normal işleyişte, her yönlendirici VRRP paketlerini diğer yönlendiricilere çok yönlü (multicast) adres olan 224.0.0.18'e göndererek kendi virtüel paketlerini belirtirler. A yönlendiricisinin arızalanması veya servis dışı kalması halinde, B yönlendiricisi A yönlendiricisinin VRRP bilgisini alamaz ve belirli bir süre sonra B yönlendiricisi 1 no'lu virtüel yönlendiricinin master'ı durumuna geçer. A yönlendiricisi tekrar servis vermeye başlarsa, 1 no'lu virtüel yönlendiricinin yüksek öncelikli VRRP'ni yayar ve bunu farkeden B, master'lık görevini A'ya bırakır.

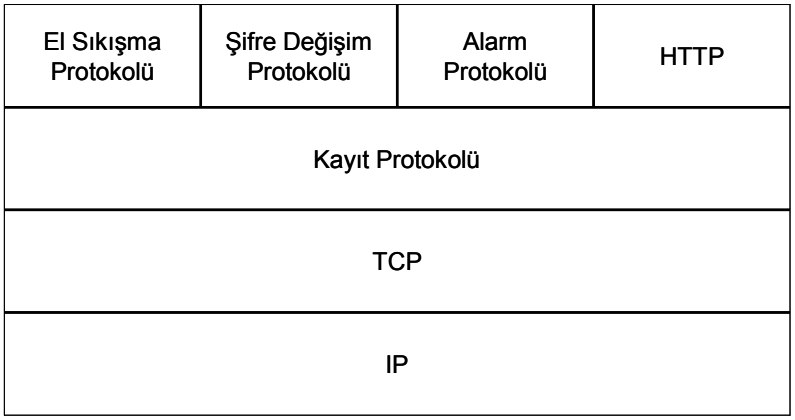
4.5 IP Şebeke Güvenliği

IP şebekelerin uygulama alanları, yazılımsal ve teknolojik gelişmelerle birlikte, giderek genişlemektedir. Bu uygulamalar şebeke içerisinde güvenlik önlemlerinin

alınmasını zorunlu kılmıştır. İnternet bankacılığı, e-posta, e-ticaret gibi birçok uygulama IP şebekeler üzerinden yapılmaktadır. Mobil terminaller üzerinden bankacılık işlemlerinin yapılabilmesi ve mobil imza, İnternet uygulamalarından bazılarıdır. UMTS şebekesindeki veri hizmetleri de IP şebeke üzerinden dış şebekelere bağlantı sağlanarak yürütüldüğünden, UMTS'te IP güvenliği çok önemlidir. Bu bağlamda kullanılan 2 temel protokol bulunmaktadır. Bunlar İletim Katmanı Güvenliği (TLS, Transport Layer Security) ve IP Güvenliği (IPSec) protokolleridir. IPSec daha çok VPN için kullanılmaktadır. Bunun nedeni IPSec'in VPN'lere İnternet'te ilettikleri mesajları kodladıkları için özel şebeke gibi kullanma imkanı sağlamasıdır.

4.5.1. TLS – İletim Katmanı Güvenliği

TLS, Netscape tarafından geliştirilen güvenli soket katmanı (SSL, Secure Socket Layer) V 3.0 üzerine oturtulmuş yeni bir açık kodlu protokoldür. TLS, IETF tarafından standartize edilmiştir. TLS'in temel mantığı web sunucusu ile kullanıcı arasında hassas verinin (ör. Kredi kartı numarası) HTTP protokolü aracılığıyla iletilmesini güvenli şekilde sağlamaktır. Bağlantıyı sağlamak için 80 no'lu HTTP portu yerine 443 no'lu port kullanılır. Şekil 4.8'de TLS protokol yığını gösterilmiştir.



Şekil 4.8 : TLS Paket Formatı

Uçtan uca (ör. MS ile dış IP şebeke sunucusu) güvenli bir bağlantı sağlamak için TCP'yi ve desteklemek için de yığında belirtilen 4 protokol uygulanır. Bunlar el sıkışma (handshake), kayıt, şifre değiştirme ve alarm protokolleridir. Kayıt protokolü kodlama ve doğrulama işlemleri ile gizlilik ve entegrasyonu sağlar. Burada kullanılan şifreler ise oturum başladığında el sıkışma protokolü ile belirlenir. İletilecek veri öncelikle maksimum boyutu 16 kB olan bloklara ayrılır ve

muhtemelen sıkıştırılır. Sonrasında mesaj doğrulama kodu (MAC), bu veriye ilişkin olarak paylaşılan doğrulama şifreleri ile hesaplanır. MAC'ı da içeren kayıt başlığı, protokol yığınına eklenerek sıkıştırılmış veri hakkında bilgi içerir. Şifre değiştirme protokol bölümü 1 bayt'dır ve güncelleme durumunda kullanılır.

Alarm protokolü, mevcut bağlantıda bir hata veya arıza durumunda alarm mesajı üretir. Yanlış bir MAC alınması, formata uygun olmayan mesajlar alınması alarm üretilmesine örnek olabilir. 1. seviye alarmlar sadece uyarı niteliğindedir. 2. seviye alarmlar ise hayati hatalardır ve bağlantının kesilmesiyle sonuçlanır. Alarm mesajları da kullanıcı verisi gibi sıkıştırılır ve kodlanır. El sıkışma protokolünün fonksiyonları; kullanıcı ile sunucu arasında sayısal sertifikalar sayesinde çift yönlü doğrulama mekanizması oluşturmak, kullanılacak kodlama ve doğrulama algoritmalarında ve şifrelerinde uzlaşmaktır. Güvenli bir oturumun kurulmasında 4 faz vardır:

1. fazda kullanıcı ve sunucu birimler birbirlerinin güvenlik geleneğini sorgular ve anlaşır. Bu fazda iletilen ilk mesaj, kullanıcı TLS versiyon bilgisini, oturum tanımlayıcısını, desteklediği kodlama, doğrulama ve sıkıştırma algoritmalarını içerir. Sunucu bu mesaja server_hello mesajı ile karşılık verir. Server_hello mesajı, kullanıcının desteklediği özelliklere göre içeriği aynı kalacak şekilde gönderilir.

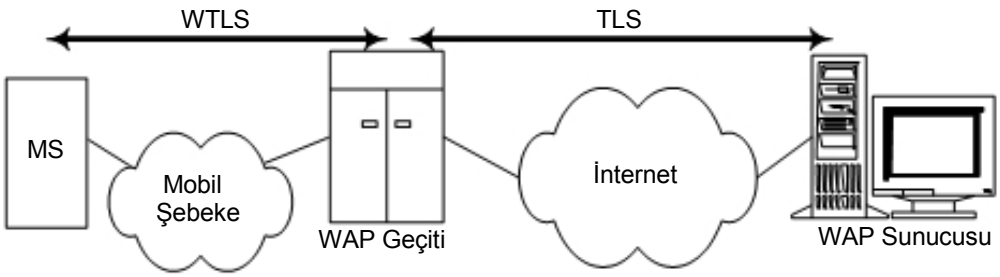
2. fazda sunucu doğrulama ve karşılıklı şifre aktarımı gerçekleşir. Öncelikle sunucu kendi sertifikasını (bazı firmaların yayınladığı sayısal sertifikalar) kullanıcıya gönderir. Gerekli olursa şifre değiş tokuş mekanizmasına bağlı olarak server_key_exchange mesajı iletilir. Sunucu opsiyonel olarak kullanıcıya certificate_request mesajı ileterek onun geçerli sertifikasını isteyebilir. Sunucu da bu fazı server_hello_done mesajı ile kapatır.

3. fazda kullanıcı, sunucudan aldığı sertifikadan emin olduktan sonra kendi sertifikasını sertifika mesajı ile gönderir. Sonrasında client_key_exchange mesajını sunucu ile şifre değiş tokuş mesajına içerik anlamında bağlı olarak gönderir.

Son fazda ise kullanıcı ile sunucu arasında change_cipher_spec mesajı ve finished sonlanma mesajı karşılıklı iletilerek güvenli oturum kurulur. Bu işlem sonunda veri akışı başlar.

4.5.2 WAP TLS

Bu protokol WAP cihazlarının WAP geçitlerine güvenli erşimini sağlamak için geliştirilmiştir. Şekil 4.9'da WTLS'in kullanım aralığı belirtilmiştir.

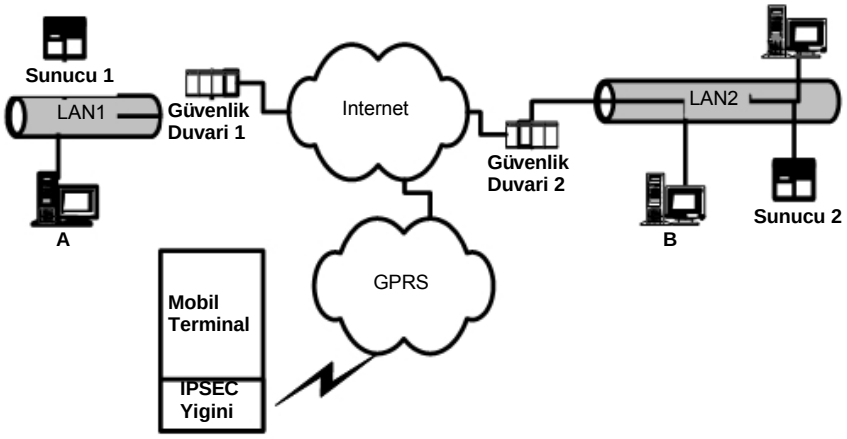


Şekil 4.9 : WTLS'in Kullanım Alanı

MS ile WAP geçiti arasındaki veri transferi, WTLS ile güvence altına alınır. TLS ise WAP geçiti ile WAP sunucusu arasındaki bağlantının güvenliğini sağlar. WAP sunucusunu doğrulamak ve doğru sayısal sertifikaya sahip olduğundan emin olmak WAP geçit düğümünün sorumluluğundadır. WTLS, gönderilen ve alınan mesajlar anlamında TLS ile aynı özelliklere sahiptir fakat TLS kadar güvenli değildir. Bunun nedeni bazı WAP terminallerinin sınırlı işlem yapabilme yeteniğidir. Bu sebeple WAP geçiti zayıf kodlama yapma ya da kullanıcıya hiç kodlama yapmama imkanı da sunar. Ek olarak WTLS'in konfigürasyonu, WAP geçitlerine yapılabilecek saldırılara karşı zayıftır. Bunun nedeni verinin basit yazı olması ve kodlama tekniğinin WAP geçitlerinde değişime uğramasıdır. WAP 2.0 versiyonunda bu güvenlik için yeni bir model geliştirilmiş ve modelde WAP iletim protokolleri, standart IP protokolleri (HTTP, TCP, IP) ile değiştirilmiştir.

4.5.3 IPSec Protokolü

Şekil 4.10'da 2 farklı şebeke İnternet ile birbirine bağlıdır. Şebeke 1'den Şebeke 2'ye gönderilen veri önce güvenlik duvarı 1'de kodlanır ve güvenlik duvarı 2'de kodu çözülür. Arada İnternet bağlantısı (kamu şebekesi) olmasına rağmen kodlama ve kod çözme işlemleri oturuma özel olduğundan bu bağlantıya VPN denir.



Şekil 4.10 : Basit VPN Örneği

Bu bağlantının farkı, kullanılan kodlama ve kod çözme eşleştirmesinden kaynaklanmaktadır. VPN çözümü aynı zamanda mobil operatörler tarafından da GGSN ile kullanıcının bağlı olduğu intranet arasında güvenli bağlantı sağlamak amacıyla kullanılır. Bu özellik mobil operatöre kendi GPRS şebekesini, daha önce anlaştığı sabit hatlı bir şebekenin ilave mobil şebekesi gibi kullandırmaya olanak tanır. VPN'e ek olarak, HLR ve GGSN'deki erişim noktalarına, bu bağlantıyı kullanma hakkına sahip kullanıcıların kayıtları yapılarak, sadece onlara erişim hakkı tanıma olanağı vardır. Bu kullanıcı genellikle GPRS bağlantı özelliğine sahip bir modem görevi gören bir dizüstü bilgisayardır. Fakat bu özellik, GPRS terminallerinin daha güçlü, IP uygulamalarını daha geniş çapta destekleyen bir birim olmalarını gerektirir. Programlanabilir ve Java kullanılabilen GPRS terminalleri mobil hizmetlerin bu amaçla kullanılabilmesi açısından uygulanabilirliğini artırır. IPSec, IP katmanında kodlama yapılabilmesine olanak tanıyan protokole verilen addır. IPSec sadece VPN çözümü değil, uçtan uca trafiğin kodlanması ve doğrulanması işlemlerine de olanak sağlar. Hem IPv4, hemde IPv6'yı destekler. Başlıca fonksiyonları; doğrulama, entegrasyon, gizlilik, tekrarları engellemek ve sıkıştırma yapmaktır. IPSec, IP paketlerinde güvenliği sağladığından, tüm IP uygulamalarını doğal olarak destekler. IPSec'de 2 alt protokol tanımlanmıştır. Bunlar doğrulama başlığı (AH) ve kapsülleme güvenlik ek yüküdür (ESP). IPSec hizmetleri güvenlik birliği (SA) olarak adlandırılan bir mekanizmaya dayanmaktadır. SA, akan trafiğe güvenlik hizmetleri sağlayan tek yönlü bir "bağlantı" olarak tanımlanır. IPSec'de çift yönlü bağlantılar kurulduğundan her yöne 1'er adet olmak üzere 2 SA gereklidir. Bir SA içerisinde; SPI (Güvenlik Parametre İndeksi) olarak adlandırılan

ve şifreleme, doğrulama ve kodlama algoritmalarını içeren bir birim, hedef IP adresi ve güvenlik protokolü (AH veya ESP) tanımlayıcısı bulunur. AH, RFC 2402 spesifikasyonunda tanımlanmış olup veri entegrasyonu, kaynak adres doğrulaması, tekrarlamayı önleme ve başlıktaki bazı parçaları doğrulama hizmeti sunar. AH, üst katman protokolleri ve bir kısım IP başlığı için doğrulama hizmeti sunar. Tüm IP başlığına bu hizmeti sunamaz. Nedeni bazı kısımların yönlendirme sırasında değişebilmesi ve tekrar yönlendirilebilmesidir.

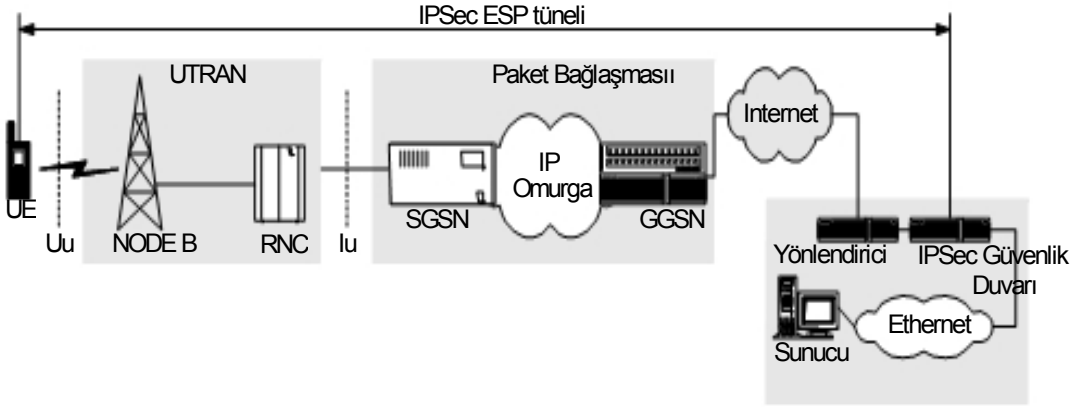
ESP, RFC 2406 spesifikasyonunda tanımlanmış olup kodlama sayesinde gizlilik hizmeti sunar. ESP de AH gibi doğrulama sağlar fakat IP başlığı ESP kullanılarak kodlanmadıysa, IP başlığına doğrulama hizmeti sunmaz. AH ve ESP her ikisi de 2 modda çalışır. Bunlar iletim modu ve tünel modudur. İletim modunda koruma üst katman protokolleri için, tünel modunda ise koruma tünellerin IP paketleri için yapılır.

1. senaryo (AH kullanımı): LAN içerisinde bulunan kullanıcı diğer kullanıcıya bir paket göndermeden önce sayısal imza ile paketleri imzalar. Alıcı uç imzayı kontrol eder ve ya kabul ya da reddeder. İnternet şebekesinde paket değişikliğe uğrarsa, sayısal imza paket içeriğiyle uyuşmaz. Paketler İnternet şebekesinde kodlanmadan iletilir.

2. senaryo (ESP kullanımı): Kaynak uç paketleri güvenli LAN içerisinde kodlar ve gönderir. Farklı bir kullanıcı paketi izleyebilir fakat dekod edemeyeceği için içeriğini okuyamaz. Alıcı uçta doğru dekod algoritması olduğu için mesaj dekod edilebilir.

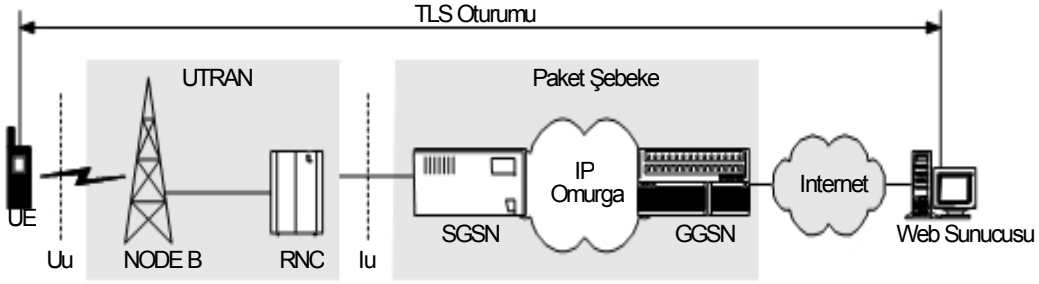
Tünel Modda SA, iki kullanıcı ve 2 geçit birimi arasında veya bir kullanıcı ile bir geçit birimi arasında kurulabilir. Güvenli geçit, güvenli LAN'dan bilgiyi alır. Bu paket aynı hedef uca gidecek diğer bir IP paketi içerisine kapsüllenir. Bu örnekte hedef uç diğer güvenli geçit birimidir. Hedef uç, paketi aldığında dekapsüle eder. İnternet içerisindeki yolculuğu süresince orjinal paket güvende olur. AH kullanılıyorsa hedef uç imza uyumsuzluklarını kontrol eder, ESP kullanılıyor ise kod çözme işlemi yapılır. Eğer güvenli geçitler veri kodlaması yaptılar ise kurulan tünel ile şebeke arasında VPN hizmeti verilir. Hedef uç bir kullanıcı ise, VPN ile güvenli uzaktan erişim sağlanmış olur. Tünel modunda iki tür IP başlığı vardır. Dış IP başlığı IPSec'in işleyeceği hedef ucu belirtir. İç IP başlığı ise paketin son hedef ucunu gösterir. Güvenlik protokol başlığı dış IP'den sonra, iç IP başlığından önce

konumlandırılır. AH kullanılıyorsa dış IP başlığının bir kısmı ve iç IP başlığının tamamı korunur. ESP'de ise dış IP başlığına dokunulmaz, iç IP başlığı doğrulanır ve kodlanır. GPRS şebekesi, UE'den dış IP şebeke uç birimine veya özel IP şebekesine uçtan uca IP iletimi sağlar. Bu özellik sayısal imza ve kodlamanın uçtan uca yapılabilmesi ve gizlilik, doğrulama gibi güvenlik hizmetlerinin uçtan uca verilebilmesini sağlar. Güvenli şebekelerde de istenen, uçtan uca bağlantı hizmeti sunulabilmesidir. GPRS, UMTS sistemine ilişkin güvenlik mekanizmalarıyla (LLC protokolleri) mobil cihazdan SGSN'e kadar olan iletimde güvenliği sağlar. Fakat sade yazı (plain text) olan bu bilginin GPRS çekirdek şebekede (SGSN-GGSN) ve GGSN ile İnternet üzerinde güvenliği sağlamaya yetmez. Bu nedenle, Şekil 4.11'de de belirtildiği gibi bir VPN hizmetinin UE'ye güvenli olarak sağlanabilmesi için uçtan uca kullanılan IPSec ESP tüneli verilmiştir.



Şekil 4.11 : IPSec ESP Tüneli

Kullanıcı verisi, firma güvenlik duvarı ile UE arasında kodlanır ve bu şekilde iletilir. Şekil 4.12'de ise UE'nin dış şebekeye bağlı bir sunucuya TLS ile uçtan uca güvenli bağlantı kurulması örneği verilmiştir.



Şekil 4.12 : UE-WEB Sunucusu Arasında TLS Kurulumu

Karşılıklı şifrelerin değiş tokuşundan sonra şifreleme işlemi ile bilgi korunur ve iletilir.

4.5.4 RADIUS - Uzaktan Doğrulama Çevrim Kullanıcı Hizmeti

Şebeke işleticileri, yetkisi olmayan kişilerin şebekeye erişimini önlemek isterler. Bu amaçla; yetkilendirme, tanımlama ve ücretlendirme (AAA) işlemlerini yapabilmek için IETF alt grubu olan AAA çalışma grubu tarafından RFC 2865 spesifikasyonunda belirtildiği şekilde bir protokol (RADIUS) geliştirilmiştir. Bu protokol, şebeke erişim sunucusundan yetkilendirme sunucusuna erişimi düzenler. UMTS şebekesi düşünüldüğünde GGSN, MS adına şebeke erişim sunucusu olarak davranır (NAS-RADIUS kullanıcısı) ve RADIUS sunucusu sadece bu bilgileri içeren bir veritabanı görevi görür. Görevleri; yetkilendirme, tanımlama, kullanıcı konfigürasyonu tanımlama ve ücretlendirmedir. Bir NAS kullanıcısı şebekeye erişmek istediğinde erişim istek mesajı oluşturur ve NAS aracılığıyla RADIUS sunucusuna iletir. Bu mesaj içeriğinde kullanıcı adı, şifresi, kullanılacak hizmet tipi belirtilmiştir. Mesajı alan sunucu gerekli yetkilendirme ve tanımlama işlemlerini kontrol eder ve erişim kabul mesajı iletir. Mesajda, abonenin kullanacağı IP adresi, sıkıştırma tekniği ve giriş yapılacak kullanıcı adresi bulunur. Ücretlendirme protokolü ise RFC 2866 spesifikasyonunda belirtilmiştir. Bir kullanıcı NAS'a bağlandığında NAS, RADIUS sunucusuna "accounting" istek mesajı gönderir. Bu mesaj oturum numarası (kimliği), kullanıcı adı ve NAS'ın IP adresini içerir. Bu şekilde her farklı oturum için farklı ücretlendirme yapılabilir. Oturum bittiğinde ise oturumu durdurma isteği gönderilir (NAS tarafından). Bu mesajda kullanıcı istatistikleri vardır ve ücretlendirme amacıyla kullanılır.

4.6. IP Tabanlı QoS Mekanizmaları

QoS, bir şebekede farklı tipten servisler veya kullanıcılara önceden üzerinde uzlaşılmış seviyede ve maliyet açısından efektif hizmetler sunma kabiliyeti olarak tanımlanabilir. QoS'un ana hedefi, son kullanıcının aldığı hizmetin belirli bir kaliteye sahip olmasıdır. Kullanıcıların "kalite" anlayışı alınan hizmete bağlı olarak değişkenlik gösterir.

Hizmet kalitesi ve kapasite arasında bir denge söz konusudur. Kapasiteden ödün verildiğinde kalitede artış sağlanması, kaliteden ödün verildiğinde ise kapasitede artış sağlanması UMTS şebekelerinde geçerli bir kavramdır.

IETF, IP tabanlı QoS mekanizmaları ile ilgili çeşitli tavsiyeler yayınlamıştır. Faklılaştırılmış Hizmetler (Diffserv), Entegre Hizmetler (Intserv) ve Çok-Protokollü Etiket Bağlaşması (MPLS) bu tavsiyelerden en yaygın kullanılanlarıdır. Çekirdek şebeke geçit birimleri, QoS anlamında büyük öneme sahiptir. QoS gereksinimlerinin diğer şebekelerden UMTS'e aktarımı geçit düğümleri ile yapılmaktadır.

4.6.1 Veri Hizmet Sınıfladırması

Veri hizmetlerinin sınıflandırılması, hangi uygulamaya nasıl hizmet sağlanması gerektiği konusunda önemli bir yere sahiptir. UMTS operatörü tarafından kullanıcı ile önceden yapılan anlaşmaya uygun olarak verilen kriterlere uygun hizmetler sunularak, memnun abone sayısı artırılabilir.

Temel hizmet sınıfları, Tablo 4.1'de verilen kriterlere göre şu şekilde belirlenebilir:

Tablo 4.1: Belirli Kriterlere Göre Farklı Hizmet Sınıfları

Hizmet	Güvenilirlik	Gecikme	Bit Hızı Garantisi
E-posta	Yüksek	Yüksek	Yok
Faks	Düşük	Yüksek	Yok
Web / Wap gezinme	Yüksek	Orta	Yok
Ses / Video Akımı	Düşük	Orta	Var
Ses / Video Konferansı	Düşük	Düşük	Var

Güvenilirlik ve gecikmelere karşı duyarlılık, bu sınıflandırmanın oluşumunda önemli iki etkendir:

Güvenilirlik: İletişimde yaşanan paket kayıpları, güvenilirliğin belirlenmesinde en önemli etkendir. Bazı uygulamalar paket kayıplarına karşı çok hassas değil iken (Ör: Ses trafiği - Kullanıcının kötü yönde algısı oluşmadan belirli bir kayıp ile iletişim

sürdürülebilir), bazıları ise herhangi bir kayıp veya hataya çok duyarlıdır. Örneğin bir e-postanın hatalı veya kayıplı iletilmesi kabul edilemez.

Gecikmelere Karşı Duyarlılık: Gerçek zamanlı uygulamalar, uç birimler arasındaki iletişimin paket gecikmelerine karşı duyarlı olduğu uygulamalardır. IP tabanlı uygulamalar düşünüldüğünde; video konferans, VoIP, Hücresel Sistemlerde Bas-Konuş (PoC) örnek olarak verilebilir. Bu uygulamalar için garanti edilmesi gereken sabit bit hızları, kullanılan kodeke bağlı olarak çeşitlilik göstermektedir. IP Tabanlı QoS mekanizmalarından UMTS çekirdek şebekede kullanılan iki ana yöntem entegre hizmetler ve farklılaştırılmış hizmetlerdir.

4.6.2. Intserv - Entegre Hizmetler

Intserv, çalışma mantığı olarak datagram ve devre bağlaşmalı şebekelerin avantajlarını birleştirerek bunu paket bağlaşmalı şebekede uygulamaktır. Bu amaçla bir şebeke hizmetinin ses, video, gerçek zamanlı ve gerçek zamanlı olmayan veri trafiğini taşıma kabiliyetine sahip olması öngörülmüştür. İki tip hizmet belirlenmiştir:

Kontrollü Yük Modeli: Bu modelde yüklü olmayan bir şebekede bir paketin iletim başarımının aynı şekilde yüklü bir trafikte de sağlanması esas alınır. Şebeke, QoS açısından şu kriterleri sağlamalıdır:

- İletilen paketlerin büyük çoğunluğu şebeke üzerinden hedeflenen uca iletilmelidir.
- İletilen paketlerin büyük bir yüzdesi, minimum iletim gecikmesinden daha az bir gecikme ile alıcı uca iletilmelidir. Minimum iletim gecikmesi, her yönlendiricide harcanan toplam işlem zamanını belirtir. Bu modelin amacı, şebekedeki yükün artması durumunda dahi sunulan hizmeti garanti etmektir.

Garantili Hizmet: Bu modelde ise daha önceden belirlenmiş uçtan uca maksimum kuyruk gecikmesi esas alınır. Minimum veya ortalama iletim gecikmesi kontrol edilmez. Sadece maksimum kuyrukta bekleme süresi sınırlandırılır. Bu nedenle jitter (minimum ve maksimum gecikme varyansları arasındaki fark) da kontrol edilmez.

4.6.3. RSVP – Kaynak Rezervasyon Protokolü

Bahsedilen her iki model için gerekli bant genişliğini veya buffer boşluğunu sağlamak amacıyla kabul kontrolü ve kaynak rezervasyonu gibi işlemlere ihtiyaç duyulur. Bu işlemler için IETF tarafından oluşturulan (RFC 2210) kaynak rezervasyon protokolü (RSVP) kullanılır.

RSVP bir kontrol protokolüdür ve her veri akışı için şebekede abonenin kullanacağı uygulamaya uygun bir QoS isteğinde bulunmasını sağlar. OSI yapısı baz alındığında, RSVP iletim katmanında yer alır ve kullanıcı verisi trafiğini taşımadığından dolayı işaretleşme protokolü olarak adlandırılır.

RSVP, genellikle gecikmelere karşı duyarlı trafiğin IP şebeke üzerinden akışını sağlamakta kullanılır. Örneğin bir host, gerçek zamanlı bir video oturumu başlatmak istediğinde, RSVP kullanarak şebekeden bu isteğin karşılanmasını talep edebilir. Şebekenin bir kısmı RSVP'yi desteklemiyorsa, herhangi bir rezervasyon işlemi yapılmaz. Bu durumda, RSVP şebekenin bu bölümünde paketleri tüneller ve bu işlemi RSVP destekleyen yönlendiriciye kadar sürdürür. RSVP'de rezervasyon işlemi tek yönlü yapıldığından, full dupleks bir iletişimde iki ayrı rezervasyon kurulum işlemi yapılmalıdır. RSVP tek yönlü ve çok yönlü trafiği destekleme özelliğine sahiptir.

RSVP destekleyen bir şebeke elemanının bazı özelliklere sahip olması gereklidir. Denetim kontrolü, kabul kontrolü, paket sınıflandırma yeteneği, paket zamanlaması bu özelliklerdir. Denetim kontrolü, istek yapan kullanıcının rezervasyon yapma yetkisini doğrulamak için; kabul kontrolü ise kaynakların istenen QoS'u sağlayacak niteliğe sahip olup olmadığını kontrol etmek için kullanılır. Bu iki aşamadan geçilememesi durumunda, kaynak uca olumsuz yanıt verilir. Paket sınıflandırması, QoS talep edilen veri akışına ilişkin paketlerin o akışa ait olup olmadıklarını kontrol etmek ve doğru paketlerin işaretlenmesini; paket zamanlayıcısı ise, her veri akışı için gereken QoS'a ulaşmak ve paketlerin iletimini sağlamak için kullanılır.

Rezervasyon iki tip mesaj paketi ile yapılır. Bunlar yol (path) ve rezervasyon (resv) mesajlarıdır. Yol mesajı, kaynak uçtan alıcı uca doğru gönderilir ve içeriğinde veri akışına ilişkin olarak; gönderilecek veri formatı, kaynak adresi, kaynak port numarası ve trafik karakteristiği bulunur. Bu mesaj, kaynak ile hedef uç arasında bir yol kurulması için kullanılır. Bu mesaj, RSVP destekleyen bir yönlendiriciye geldiğinde,

ileri yöndeki adres ve veri akışı hakkındaki bilgiler kaydedilir. Bu bilgiler hedef uçtan resv mesajı geldiğinde kullanılır. Alıcı uç mesajı aldıktan sonra veri akımını alabilmek için o yol üzerinde görevli yönlendiricilere resv mesajı göndererek alacağı veri için rezervasyon isteği yapar. Bu istek yönlendirici tarafından kontrol edilir ve doğrulanırsa kaynak rezervasyonu yapılır.

RSVP 3 tip trafiği destekler:

- En iyi performans (Best Effort): Bu tip trafik geleneksel IP trafiğidir. Örnek olarak e-posta transferi verilebilir.
- Hıza duyarlı trafik: Bu tip trafik, hıza duyarlı hizmetler için kullanılır. Örnek olarak video konferans verilebilir.
- Gecikmeye duyarlı trafik: Değişken hızda fakat aşırı gecikme olmaması gereken uygulamalarda kullanılır. Örnek olarak bir MPEG-2 videosunun bir uctan diğer uca iletimi verilebilir.

RSVP, çok yaygın olarak kullanılan bir protokol değildir. Büyük çaplı şebekeler (Ör: UMTS şebekeleri) için çok elverişli olmaz. Bunun sebebi, her veri akışı için birçok işlem yapılması gerekliliği ve işaretleşmenin yoğun şekilde uygulanması nedeniyle şebekeye ek yük getirmesidir.

UMTS şebekesi içerisinde kullanılmasa da bir UE ile dış IP şebeke kullanıcısı arasında uçtan uca QoS sağlamak amacıyla kullanılabilir. Örneğin bir UE, dış IP şebeke kullanıcısı ile bir oturum başlatmak istesin. Öncelikle UE ile SGSN üzerinden GGSN ile PDP Bağlantı aktivasyonu yapılır. Daha sonra UE, uçtan uca QoS için RSVP rezervasyon sürecini istek yaparak başlatır. UE isteğini GGSN'e gönderir ve GGSN de dış IP şebekesinde rezervasyon işlemini yapar (RSVP yolu kurarak). Sonrasında UE alıcı konumunda olacağından, aşağı yönde rezervasyon işlemi de yapılır (Yol bu kez dış IP şebeke üzerinden kurulur). Bu yol talebi üzerine PDP Bağlantı, trafik karakteristiğine göre PDP içeriğini değiştirir ve UMTS çekirdek şebekede ilgili rezervasyonu da yaparak dış IP şebekeye onay mesajı verir.

RSVP mesajlarının hepsi, UMTS şebekesi boyunca tünellenerek iletilir. Başka bir deyişle, GGSN ve UE dışındaki tüm UMTS şebeke elemanları mesajın içeriğinin farkında olmaz.

4.6.4 Diffserv - Farklılaştırılmış Hizmetler

Diffserv, IP tabanlı şebekelerde QoS'u sağlamak için uygulanan yöntemlerden biridir. Bu modelde farklı tipten uygulamaları farklı sınıflara ayırma mantığı benimsenmiştir. Diffserv Kod Noktaları (DSCP) adı verilen sınıflar, farklı tip hizmetleri seviyelere bölmek için kullanılır. Her IP paket başlığında DSCP alanı vardır ve bu işlev için ayrılmıştır. IPv4 başlığında bu bilgi, hizmet tipi (TOS, Type of Service) alanında, IPv6 başlığında ise Trafik Sınıfı (TC) oktetindedir. Diffserv QoS mekanizması, şebeke uç yönlendiricilerinde (Edge Router) bulunur. Bir Diffserv şebekesinde aynı hizmet sınıfı ile işaretli tüm paketler, şebekedeki tüm yönlendiricilerde aynı seviyede hizmet alırlar. Buna, Her Adımda Davranış (PHB, Per-Hop-Behaviour) denir. PHB'de 3 farklı hizmet sınıfı tanımlanmıştır:

Hızlandırılmış Yönlendirme (EF): EF, ATM'deki CBR hizmeti ile benzerlik gösterir. Amacı, paketlerin sorunsuz ulaşımını sağlamak, gecikme ve jitter'ı minimize etmek, küçük oranda paket kaybı ile iletimi tamamlamaktır. Bu sınırlar çerçevesinde iletilen trafik, önceden belirlenen limiti aşmamalıdır. Aştığı taktirde paketler atılır. EF, tek bir kod noktasına sahiptir ve genellikle gerçek zamanlı veri akışı için kullanılır.

Emin Olunan Yönlendirme (AF): AF, kendi içerisinde 4 farklı sınıftan oluşan bir yapıya sahiptir. Bu sınıf farkları, sağlanması gereken minimum elverişli bant genişliği tahsisine dayanır. Her sınıfa belirli oranda bant genişliği tahsis edilmiş olsa da yığılma anında yığılma kontrolüne maruz kalabilir ve paketlerin bir kısmı bu nedenle atılabilir. 4 sınıf kendi içerisinde ayrıca 3 atılma (drop) sınıfına ayrılmıştır. Yüksek öncelikli atılma durumu, yığılma anında bu paketlerin öncelikli atılacağını belirtir.

En iyi performans (Best Effort): Hiçbir öncelik mekanizması geçerli değildir. Tüm paketler aynı işleme tabi tutulur.

Bir Diffserv şebekesinde PHB, şebekeye paket ilk geldiğinde önceden belirlenmiş olan denetim kriterine göre sınıflandırılır. Burada IP paket başlığındaki DSCP doldurulur ve ilgili yönlendiriciye iletilir. Diffserv şebekesinden çıkan paket ise tam tersi işlem yapılarak bu sınıflandırma kaldırılır. Sonuç olarak Diffserv'de yönlendiricilerin, veri akışları ile ilgili durum bilgisini depolamaları gerekmez. Şebekeye girişte gerekli işaretleme (mark) yapılmış olur.

Tablo 4.2'de, UMTS QoS sınıflarının Diffserv modelinde hangi sınıflara karşı düştüğü ve DSCP'lerinin neler olduğuna ilişkin bilgi verilmiştir.

Tablo 4.2 : UMTS QoS Sınıflarının Diffserv Hizmet Seviyelerindeki Karşılıkları

UMTS Trafik Sınıfı	Diffserv Hizmet Seviyesi	DSCP
Karşılıklı Görüşme	EF PHB	101110
Veri Akımı	AF PHB Sınıf 1	001010
İnteraktif	AF PHB Sınıf 2	010010
İnteraktif	AF PHB Sınıf 3	011010
Arka plan	BE	000000

AF sınıfındaki DSCP'ler, en düşük atılma önceliğine sahip olan sınıflardır. Veri akımı sınıfına giren trafik, önceden belirlenen eşik değeri aşarsa, sınıfı değişmeksizin bir işaret ile işaretlenerek yüksek öncelikli atılma durumuna geçer. İnteraktif olan ve AF PHB Sınıf 2'ye ait bir trafik için de aynı olay geçerlidir. AF PHB Sınıf 3'e ait bir trafik ise eşik değeri aştığında, ya aynı sınıf içerisinde yüksek öncelikli atılma durumuna geçer, ya da BE sınıfına atanır.

Diffserv'in en avantajlı yönü, Intserv'e göre çok daha az işaretleşme yükü getirmesidir. Tüm işaretleşme host (dış şebekedeki) ile UMTS çekirdek şebeke uç birimleri (GGSN) arasında gerçekleşir. Bu nedenle GGSN'lerin Diffserv sistemini desteklemeleri gerekir.

Diffserv, UMTS şebekesinde IP tabanlı iletimde QoS'u sağlamak için ideal bir yöntemdir. Nedenleri;

- Diffserv uygulaması GGSN'ler ve SGSN'lerin kontolündedir.
- Diffserv'de işaretleşme az olduğu için şebekeye ek trafik yükü getirmez.
- Diffserv, GGSN ve SGSN'lerin üzerinden yönetilen ve yönlendirilen bir sistem olması nedeniyle daha ölçeklenebilirdir.
- UMTS'te dış şebekeler ile iletişim geçit düğümleri üzerinden yürütüldüğünden, Diffserv uygulanabilirliği daha basit hale gelir.

Intserv, temel anlamda her veri akışı için ayrı bir QoS tanımlaması yapar. Diffserv'de ise sadece şebekeye gelen trafik belirli hizmet sınıflarına ayrılır ve ilgili

hizmet sınıfı için belirlenen QoS uygulanır. Bu açıdan değerlendirildiğinde, UMTS şebekesi için Diffserv kullanılması daha uygundur.

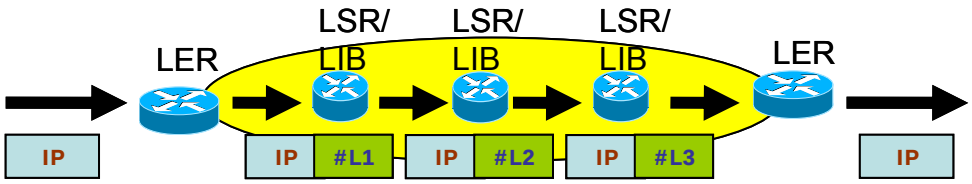
4.6.5. MPLS ile IP Şebekesi'nde QoS

Çok-Protokollü Etiket Bağlaşması (MPLS), bir şebeke içerisinde MPLS domeni boyunca yönlendiricilerin paketleri hızlı ve etkin yönlendirmelerini sağlayan bir protokoldür. MPLS, OSI katmanlı mimarisinde veri bağlantı katmanı ile şebeke katmanı arasında bulunmaktadır. MPLS'in oluşum nedeni, paketlerin şebeke içerisinde hızlı yönlendirilmelerini sağlamaktır. Buna ek olarak, hizmet çeşitliliği yaratma anlamında da kullanılmıştır. Günümüzde şebeke ve trafik yönetimi mekanizması olarak kulanılabilmektedir.

MPLS domenini oluşturan birimler aşağıdadır:

- Etiket Sınır Yönlendiricisi (LER): MPLS domeninin sınırlarını belirleyen şebeke elemanıdır. Diğer domenlerle MPLS domeni arasında arabağdaşım işlevi görür.
- Etiket Bağlaşma Yönlendiricisi (LSR): MPLS fonksiyonlarını yürütebilme yeteneğine sahip yönlendiricilere verilen addır.
- Etiket Bilgi Tabanı (LIB): MPLS'te kullanılan etiketleri içeren bir tür veritabanıdır. Her yönlendiricide bir LIB bulunur.

İleri yönde eşdeğer sınıf (FEC), aynı doğrultuda yönlendirilecek ve dolayısıyla aynı etikete sahip olacak bir grup paketi ifade eder.



Şekil 4.13 : MPLS Genel Yapısı

MPLS'in temel mantığı; yönlendirilecek IP paketlerinin 2. ve 3. katmanlar arasında sabit uzunluklu etiketler ile etiketlenmeleridir. Bu etiketlerin içeriğinde;

- MPLS şebekesinde paketin yönlendirilmesini sağlayacak adres bilgisi
- Paketin QoS kategorisi

bulunur. MPLS paketleri, trafik mühendisliği ve QoS seviyelerine göre önceden belirlenmiş güzergahlar üzerinden hedef uca iletilir.

MPLS'te Yönlendirme: MPLS domeninde yönlendirme işlemi aşağıda adım adım verilmiştir:

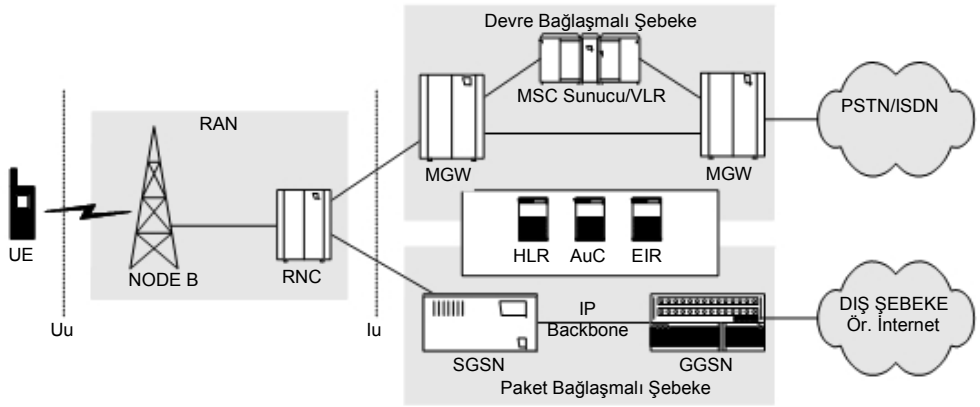
- IP paketi MPLS domenine LER ile giriş yapar.
- LER, paketin hedef adresini alır ve kendi LIB'inde o adrese karşı düşen etiketi belirleyerek IP paketlerinin önüne bu etiketi ekler.
- MPLS paketi (Etiketlenmiş IP paketi) etiket doğrultusunda bir sonraki LSR'ye yönlendirilir.
- LSR bu paketi kendi LIB'inde inceler, kıyaslar ve hangi arabağdaşımdan hangi LSR'ye yönlendirileceğini belirler. Gelen paketin etiketinden farklı bir etiket ile paketi etiketler ve ilgili LSR'ye iletir.
- Bir önceki işlem, paketin hedef uç tarafındaki LER'e ulaşmasına kadar tekrarlanır.
- Hedef uç tarafındaki LER'e ulaşan MPLS paketinin etiketi çıkarılır ve IP paketi, IP domeninde ilgili uca normal koşullardaki şekilde iletilir.

MPLS çalışma mantığında, IP paket başlığı yerine daha kısa etiketler vasıtasıyla yönlendirme işlemi yapılır. Bu sayede daha az işlem süresi ile daha hızlı yönlendirme ve iletim sağlanır. Etiketleme ile trafik ve öncelik sınıflandırması yapmak mümkün olur. VoIP gibi ekyükü küçük boyuta sahip uygulamalara ilişkin paketler, MPLS ile şebeke içerisinde daha hızlı ve etkin iletilir.

5. UMTS SÜRÜM 4 (R4)

5.1. UMTS R4 Genel Şebeke Yapısı

UMTS R4 versiyonu, çekirdek şebeke altyapısında CS domeninde radikal değişiklikler yapılması ile 3GPP standartlarına göre oluşturulmuş bir yapıdır. UMTS R4'ün ana özelliği, CS şebekede işaretleşmenin ve veri trafiğinin ayrı altyapılar üzerinden taşınmasına olanak sağlanmasıdır. R99 ile olan temel fark CS şebeke altyapısında görülmektedir. PS şebekede herhangi bir değişiklik söz konusu değildir. Bu sayede taşıyıcıdan bağımsız bir CS şebekesi sağlanmış olur. Şebeke katmanının yapısı farklı olabilmektedir (Ör: IP veya ATM). 3GPP standardında da belirtildiği üzere "Taşıyıcıdan Bağımsız CS Çekirdek Şebeke" mimarisi kabul edilmiştir. Günümüzde mobil operatörler genellikle ATM yapısı kullanılmaktadır. Fakat yapılan araştırmalarda, ATM tabanlı çekirdek şebeke yapısından IP tabanlı yapıya yönelme görülmektedir. Bu bölümde şebeke katmanı IP tabanlı olarak kabul edilecek ve bu durum üzerinde yoğunlaşılacaktır. UMTS R4'e ilişkin çekirdek şebeke altyapısı Şekil 5.1'de verilmiştir.



Şekil 5.1 : UMTS R4 Genel Şebeke Yapısı

Bu yapıda kullanıcı trafiği, Medya Geçitleri (MGW, Media Gateway) ile çekirdek şebeke içerisinde iletilir. MGW temel olarak trafiğin yönlendirilmesinden ve UMTS çekirdek şebekede CS formatındaki veri ile PSTN-ISDN harici şebekelerden gelen CS formatındaki verinin karşılıklı çevirisinden sorumludur. MGW'ler MSC

Sunucuları tarafından kontrol edilirler. MSC Sunucuları tarafından MGW'lere iletilen kontrol komutları sayesinde bu mekanizma işler. UMTS çekirdek şebekede CS domenindeki bu yapısal değişiklik, uç birimlerinde (mobil cihazlar) herhangi bir değişikliği zorunlu kılmaz. Bunun nedeni UMTS R4'te UTRAN'da IP tabanlı sistemin kullanılmamasıdır (ATM tabanlı yapı kullanılmaktadır).

5.2. Çekirdek Şebekede Softswitch Mimarisi

R4'te CS domeninde işaretleşme işaretlerinin ve kullanıcı trafiğinin farklı şebeke elemanları tarafından işlenmesi softswitch mimarisi olarak adlandırılır. Bu yapı, şebekenin ölçeklendirilmesinde önemli bir avantaj sağlar. Veri trafiğinin arttığı ve kapasite ihtiyacının ortaya çıktığı durumda, şebekeye sadece MGW'ler eklemek yeterli olacaktır. Bir diğer durumda ise çağırma kontrolü kapasitesi yetersiz kalabilir ve bu durumda MSC Sunucularının sayısı artırılarak ihtiyaç karşılanabilir. GSM, GSM'in üst versiyonları (GPRS, EDGE) ve R99'da çağırma kontrolü ve veri trafiği aynı şebeke elemanı tarafından (MSC ve Geçit MSC) yapılır.

5.2.1. MSC Sunucusu

R4 ile UMTS çekirdek şebekesine yeni eklenen bu eleman, mobil terminal tarafından başlatılan veya bitirilen çağırmalarda, çağırma kontrolü, mobil terminalin şebekeye kaydının ilgili yerde tutulması (mobilite yönetimi) gibi başlıca fonksiyonları yürütür. Ek olarak;

- Doğrulama fonksiyonlarını yürütür.
- Mobil terminal tarafından başlatılan çağırmanın hedef noktaya yönlendirilmesinden sorumludur.
- Mobil terminal tarafından sonlandırılan çağırmanın paging ile yönlendirilmesinden sorumludur.

MSC Sunucusu, çekirdek şebeke ile RNC arasındaki işaretleşmeyi Iu arabağdaşımında sonlandırır. Çekirdek şebekede taşıyıcıların (bearer) kurulmasını MGW'leri kontrol ederek gözetir.

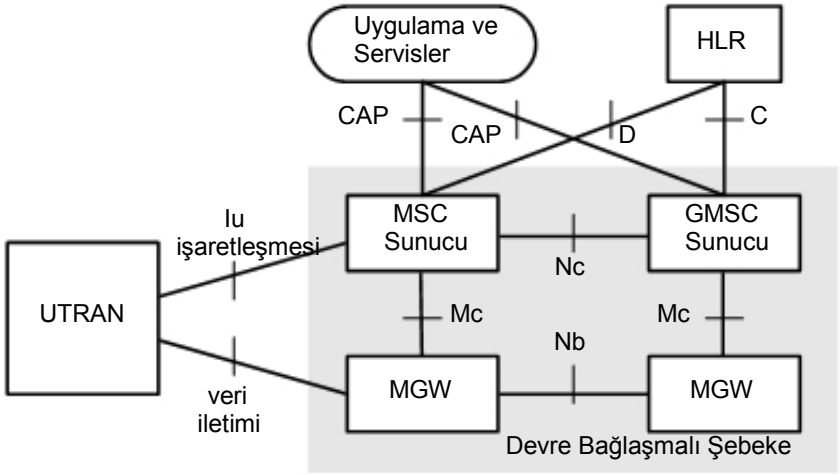
5.2.2. Medya Geçiti

R4 ile çekirdek şebekeye yeni eklenen bu eleman, aşağıdaki fonksiyonları yürütür:

- CS ve PS şebekelerden gelen taşıyıcı kanalın sonlandırılması
- CS devreler için eko olumuşumunu engellemek
- Kodek türleri arasında dönüşüm yapabilmek
- Farklı tip şebekelerden gelen ve bu şebekelere giden trafiği uygun formata dönüştürmek

Her MGW bir veya daha fazla MSC Sunucusu tarafından kontrol edilebilir.

Geçit MSC Sunucusu: GMSC Sunucusu, GSM'deki GMSC'ler ile aynı çağırma kontrol özelliklerine sahip bir elemandır. HLR ile devamlı iletişim halinde olarak hem diğer operatörlerden gelen çağırmaların uygun MSC Sunucusuna, hem de MS'ten PSTN'e iletilecek çağırmaların yönledirilmesini sağlar. Şekil 5.2.'de CS çekirdek şebeke yapısı verilmiştir. Bu yapıda 3 farklı arabağdaşım bulunmaktadır. Bunlar Mc, Nc ve Nb'dir.



Şekil 5.2 : CS Çekirdek Şebeke Yapısı ve Arabağdaşımlar

Mc arabağdaşımı, MSC Sunucuları ile MGW'ler arasında kontrol işaretlerinin iletimini ve MGW'lerden de MSC Sunuculara olay geri dönüşlerinin iletimini sağlar. Örneğin, bir MGW PSTN'den DTMF işareti alırsa, öncelikle MSC Sunucusuna bilgi vermesi gerekir. Bu arabağdaşımda kullanılan protokol MEGACO (Media Geçit

Kontrol) olarak adlandırılır ve ITU Tavsiyelerinde (H.248) belirtilmiştir. Protokol, bu bölümün son kısmında ayrıntılı olarak incelenecektir.

Nc arabağdaşımı, iki MSC Sunucusu arasındaki iletişimi sağlar. Bu arabağdaşım çekirdek şebekeye gelen MGW'yi kontrol eden MSC Sunucusundan, şebekeden çıkan MGW'yi kontrol eden MSC Sunucusuna gerekli işaretleşme işaretlerinin akışını sağlar. Bu arabağdaşımda kullanılan protokol "taşıyıcıdan bağımsız çağırma kontrol" protokolü olarak adlandırılır ve bu bölüm içerisinde ayrıntılı olarak incelenecektir.

Nb arabağdaşımı MGW'ler arasındaki bağlantıyı oluşturan arabağdaşımdır. Kullanıcı verisi bu arabağdaşımdan akar. "Kullanıcı protokolü" olarak adlandırılan ve 29.415 ile 25.415'te belirtilen protokol geçerlidir. Bu arabağdaşım, Iu arabağdaşımı ile aynı özelliklere sahiptir. Önceden tanımlanmış SDU boyutuna göre Transparan ve Destek modu olmak üzere 2 modu destekler. Destek modunda, MGW'ler arasında ve MGW-RNC arasında akan trafik zaman yönünden katı kurallara göre iletilir. Şebeke katmanında IP veya ATM olabilir. IP tabanlı yapıda iletim katmanında gerçek zamanlı iletim protokolü, ATM tabanlı yapıda ise ATM adaptasyon katmanı (AAL2) uygulanır. UTRAN içerisinde IP tabanlı yapı kullanılmadığından AAL2 katmanı geçerlidir.

CN-CS arasında 3GPP'nin önerdiği bir iletim katman yapısı olmamasına rağmen IP kullanılması birçok avantajı beraberinde getirebilmektedir. Özellikle VoIP çağırmalarında daha az ölçüde işaretleşme gerçekleştirilebilir. IP kullanımı 2. katmanda daha geniş bir şebeke teknolojisine imkan sağlayabilir. Örnek olarak 10 gigabit Ethernet, "ATM üzerinde IP" verilebilir. Bu durum bütçe, QoS ve bant genişliği anlamında esnek bir yapıya olanak tanır.

RAN ve PSTN ile olan bağlantılar haricinde, CS çekirdek şebekenin HLR ve kullanıcı uygulamalarını içeren sunuculara arabağdaşım ihtiyacı vardır. CS çekirdek şebeke ile HLR arasında geleneksel 2 tip arabağdaşım bulunmaktadır. D arabağdaşımı, VLR ile HLR arasında VLR'ın mobil terminal ile ilgili güncel bilgileri HLR'a göndermesini sağlar. C arabağdaşımı ise GMSC tarafından mobil terminalde sonlandırılacak bir çağırmanın hangi MSC'ye yönlendirileceğini sağlamak amacıyla kullanılır. Bu arabağdaşımlarda kullanılan protokol mobil uygulama kısım (MAP, mobile application part) protokolüdür.

5.3. VoIP – IP Üzerinden Ses İletimi

IP tabanlı şebeke üzerinden gerçek zamanlı ses trafiğinin taşınması protokolü (VoIP), UMTS R4'ü R3'ten ayıran en önemli özelliklerden biridir. VoIP'in UMTS R4'te çekirdek şebekede büyük önemi vardır. VoIP'in başlıca avantajları; ek maliyete gerek olmadan mevcut IP şebeke altyapısını kullanması, IP şebekenin özelliğinden dolayı şebeke elemanlarının düşük maliyetli olması, veri hizmetlerinin ses hizmetleri ile entegre şekilde tek şebeke üzerinden sağlanmasıdır. Buna karşın ATM ile IP kıyaslandığında, IP şebekenin gerçek zamanlı hizmetlerin sunulması için tasarlanmamış olması, kalite kriterlerinin henüz olgunluğa erişmemiş olması başlıca dezavantajlarıdır. Bu nedenle IP şebekede kaliteyi artırıcı birtakım protokoller yapılandırılmıştır (Diffserv, RSVP, RTP, MPLS gibi). UMTS şebekede gerçek zamanlı bir telefon görüşmesinde çağırma kontrol işlemleri SS7 protokolleri ile bir devre bağlaşmalı yol tahsis edilerek yürütülür. Fakat IP şebekede bunun bir karşılığı yoktur. Çünkü IP domeninde sadece IP paketlerinin varacağı adres ve yönlendirme ile ilgili içerik vardır. Bu nedenle çağırma kontrolü için 2 ana yöntem belirlenmiştir.

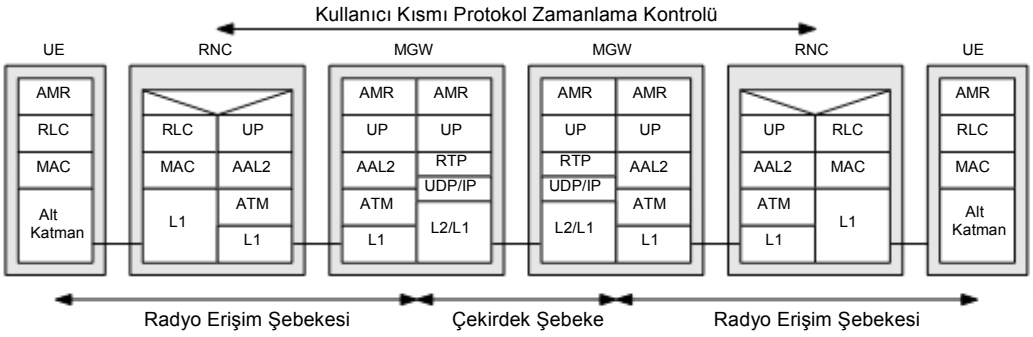
1. yöntem: SS7 uygulama protokolünü modifiye etmeden IP şebeke içerisinde tünelleyerek iletmek. Bu amaçla geliştirilen protokol Akım Kontrol İletim Protokolüdür (SCTP). SCTP, iletim katmanında TCP veya UDP yerine kullanılır. Bu yapı SIGTRAN olarak adlandırılır.

2. yöntem: Çağırma kontrol protokolünün tamamen değiştirilerek IP için optimize edilmiş yeni bir protokol oluşturulmasıdır. H.323, oturum başlatma protokolü (SIP) ve Taşıyıcıdan Bağımsız Çağrı Kontrol Protokolü (BICC) gibi protokol ve tavsiyeler IP şebeke için optimize edilmiştir. Bazı şebekeler SS7 işaretleşmesini, bazıları SIGTRAN'ı, bazıları ise H323, SIP veya BICC'yi kullandığı için bu protokollerin karşılıklı çalışabilmesi gereklidir. Arabağdaşımlarda bu protokollere geçiş sağlanmalıdır. Şekil 5.9'da UMTS R4'teki şebeke elemanları arasındaki arabağdaşımlar ve geçerli olan protokoller ayrıntılı olarak verilmiştir. Ses verisi IP paketleri içerisine konulmadan önce sırayla örneklenmeli, kuantalanmalı, kodlanmalı, gerekirse sıkıştırılmalı ve kriptolanmalıdır.

5.3.1. RTP

UMTS R4 çekirdek şebekede Nb arabağdaşımında kullanılan RTP, UDP üzerinden çalışan bir protokoldür. RFC 1889 spesifikasyonunda belirtilmiştir. Protokolün amacı, IP şebeke üzerinden uçtan uca gerçek zamanlı ses ve video iletimi sağlamaktır. 3GPP'nin TS 29.414 tavsiyesinde R4'te şebeke katmanı olarak IP kullanılması durumunda MGW'ler arasında CS domenindeki paketlerin iletimi için RTP kullanılacağı belirtilmiştir.

Nb Arabağdaşımında RTP Kullanımı: R4'te kullanıcı düzleminde (UP, user plane) Nb arabağdaşımında çekirdek şebeke ve radyo erişim şebekesinde, elemanlar arasındaki iletim ve protokol yığını Şekil 5.3'te verilmiştir.



Şekil 5.3 : UMTS Şebekesinde Kullanıcı Düzleminde RTP Protokol Yığını

Burada UP destek modunda çalışır ve çerçeveleme ile zamanlama fonksiyonlarını Nb ve Iu arabağdaşımlarında yürütür. Bu nedenle Nb arabağdaşımında RTP'nin zamanlama ile ilgili bir fonksiyonu yoktur ve RTP başlığındaki bu bilgi gereksizdir. RTCP 29.414 tavsiyelerinde de bu durum belirtilmiştir. Fakat R5'te RTP uçtan uca bağlantıda zamanlama fonksiyonunu da yürütür. Bunun nedeni UP'nin transparan modda çalışmasıdır. Şekil 5.4'de RTP başlığı verilmiştir.

Şekil 5.4 : RTP Başlık Formatı

5.4. Taşıyıcıdan Bağımsız Çağırma Kontrol Protokolü (BICC)

Bu alt bölümde, Taşıyıcıdan Bağımsız Çağırma Kabul Kontrol Protokolü ayrıntılı olarak incelenmiş, son kısımda ise bir çağırmaya ilişkin örnek verilmiştir.

5.4.1. BICC'nin Genel Özellikleri

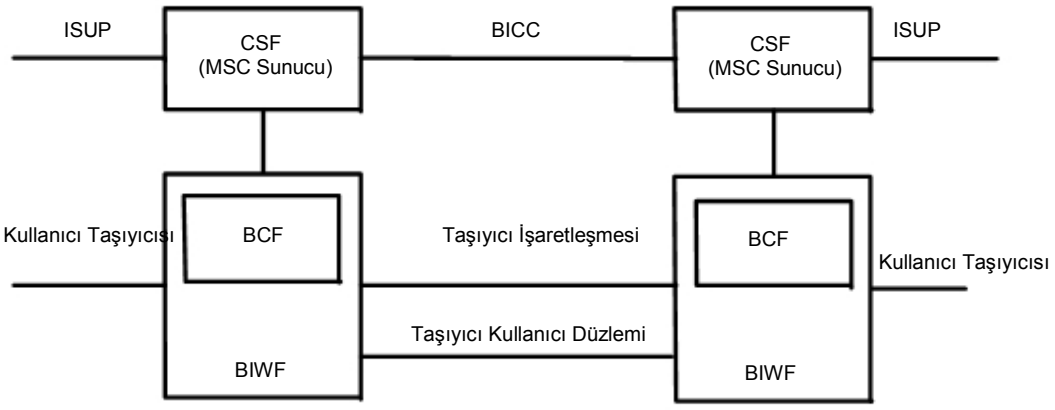
UTRAN'da başlatılan bir çağırmanın, bir PSTN aboneye ulaştırılması ya da tam tersi bir çağırmanın kurulması için UMTS R4 IP çekirdek şebekesinde, çağırma başlatılmadan önce bazı çağırma-kontrol mekanizmaları uygulanır. PSTN tarafında bu kontrol, büyük ölçüde ISUP (ISDN kullanıcı bölümü) ile yürütülür. UMTS çekirdek şebeke tarafında ise farklı alternatifler uygulanabilmektedir. Bir yaklaşım, oturum başlatma protokolü (SIP) kullanarak bütün PSTN hizmetlerini emüle etmektir. Fakat, hizmetlerin kompleks olduğu durumlarda, emülasyonda birebir doğru sonuç vermemesi nedeniyle problemler yaşanabilmektedir. ITU-T'nin bakış açısı, ISUP ile %100 uyumlu bir protokol oluşturmak için her bir hizmetin ayrı ayrı emüle edilmesi gerektiğidir. Bu durum, 2 PSTN abonesinin IP şebeke üzerinden iletişim kurup bu iletişimin nasıl sağlandığını bilmemeleri durumuna eşdeğerdir. BICC, bu amaçla oluşturulmuş bir protokol olup aşağıdaki özelliklere sahiptir:

- ISUP protokolü üzerine kurulmuş bir protokoldür ve onunla tamamen uyumlu çalışır
- Ses/veri çağırma kontrolü yapabilme yeteneğine sahiptir
- Şebeke katmanından (Ör: ATM, IP) bağımsız olarak çalışır

BICC, taşıyıcıdan bağımsız bir yapıya sahip olduğu için, ayrı bir taşıyıcı oluşturma mekanizmasına ihtiyaç duyar. ITU-T'nin IP ve ATM şebekelerde BICC kullanımına ilişkin tavsiyeleri vardır. Fakat BICC'nin temel amacı ATM'yi geçici kullanım amacıyla tutarak, IP tabanlı şebekeye geçişi kolaylaştırmaktır.

BICC protokolü, ilk olarak sadece ATM'yi destekleyen yetenek seti (CS) 1 ile oluşturulmuştur. CS 1, AAL2 işaretleşmesine ilişkin bir spesifikasyondur. CS 1, ATM virtüel devrelerindeki AAL2 virtüel bağlantısına ilişkin kurulum, sürdürülebilirlik ve versiyon bilgilerini içeren bir yapıdadır. Bu sayede geleneksel TDM tabanlı iletimin yerine ATM tabanlı iletimi geçerli kılmak mümkün olur. AAL1-AAL2 ATM adaptasyon katmanları ile gerçek zamanlı çağırmalar kontrol edilerek iletilir. CS 1, orjinal ISUP'un değiştirilmiş hali olarak görülmektedir.

Sonrasında, BICC CS 2, Q.1902.X tavsiyeleri ile oluşturulmuştur. Bu versiyon, tüm ISUP ilave hizmetlerini karşılamakla birlikte, IP tabanlı şebekeleri de destekleme özelliğine sahiptir. Taşıyıcıların IP tabanlı şebekelerde kurulmasına olanak tanımak amacıyla, BICC IP Taşıyıcı Kontrol Protokolü Q.1970 tavsiyeleri ile geliştirilmiştir. Şekil 5.5'te BICC'nin basitleştirilmiş yapısı gösterilmiştir.



Şekil 5.5 : BICC Genel Yapısı

BICC protokolünde de MEGACO gibi kontrol ve veri trafiği ayrıştırılmış ve farklı birimler tarafından fonksiyonların yürütülmesi sağlanmıştır. Çağırma Hizmet Fonksiyonu (CSF), MSCS'te bulunur ve şu fonksiyonları yürütür:

- Çağırma kontrol
- ISUP şebekesine arabağdaşım oluşturmak
- Taşıyıcı şebekeye arabağdaşım oluşturarak ve BICC kullanarak istekleri iletmek
- Taşıyıcı kontrol fonksiyonuna (BCF) arabağdaşım oluşturarak taşıyıcıların IP şebekede kurulmasını sağlamak

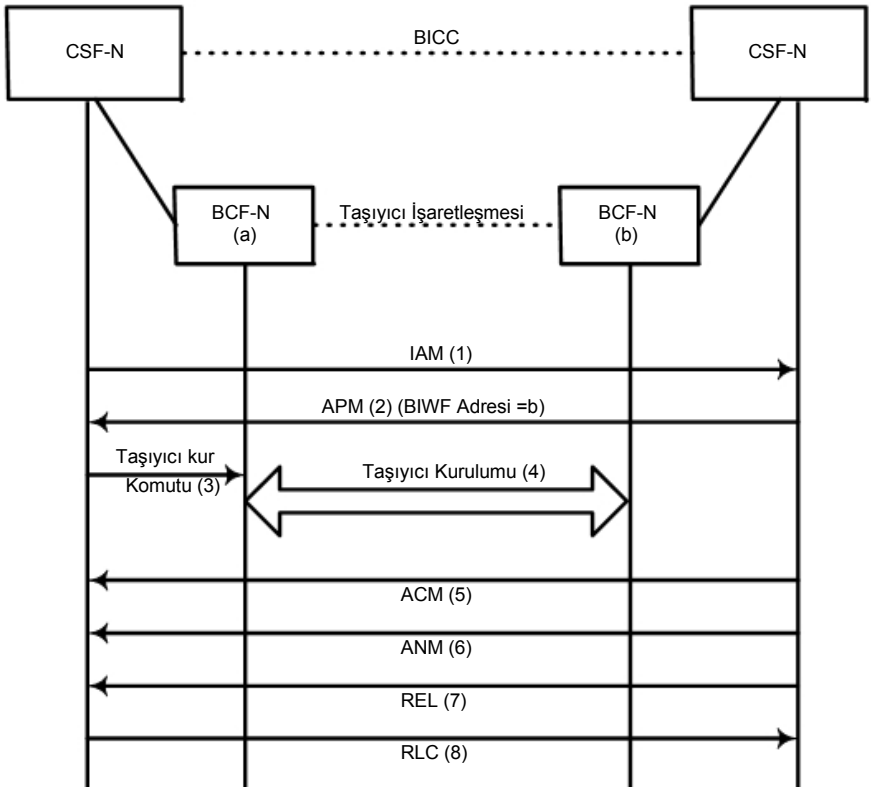
Taşıyıcı Eş Çalışma Fonksiyonu (BIWF, UMTS'te MGW'ye denktir), 2 farklı şebeke arasında çeviri görevini yürütür. UMTS R4'te, MGW, TDM'den IP'ye ve tam tersi dönüşümü sağlar. Bunun yanında kullanıcı düzlemine arabağdaşım oluşturmak, Kodek dönüşümü yapmak, taşıyıcı oluşturmak ve çözmek diğer fonksiyonlarıdır. BCF, BICC taşıyıcı kontrol protokolü sayesinde yeni taşıyıcı oluşumu için gerekli işaretleşmeyi sağlar. CSF'in görevi, BCF'i kontrol etmektir.

5.4.2. İleri ve Geri Yönde Taşıyıcı Kurulumu

İleri yönde taşıyıcı kurulumunda, taşıyıcı kurulum kontrolü, çağırma kurulumundaki ilk aşama olan "İlk Adres Mesajı" (IAM) ile aynı (ileri) yönde yapılır. IAM'a ters yönde de taşıyıcı kurulumu yapılabilir. Bu özellik, tek bir MSCS ile şebeke kaynaklarının kontrol edilebilmesini sağlar.

Şekil 5.6'da ileri yönde çağırma kurulum aşamaları verilmiştir. Burada CSF-N'ler MSCS'leri, BCF-N'ler ise MGW'leri temsil eder.

IAM mesajı çağırma kurulumunu başlatan mesajdır. İçeriğinde, hedef ucun numarası vardır ve hedef uca hizmet veren MSCS'e (PSTN'e bağlı olan) gönderilir. Sonrasında, IAM'a ters yönde BICC kullanıcıları arasında (MSCS'ler) BICC olmayan genel amaçlı mesaj (APM) iletilir. Bu mesaj, taşıyıcı bilgisini, uzak uçtaki MGW'nin medya özelliklerini, IP adresini ve RTP port numarasını içerir. Bu mesajı alan lokal MSCS, kendine bağlı MGW'e, uzak uç MGW aracılığıyla taşıyıcı kurulum isteğini iletir (MEGACO protokolü ile). Taşıyıcı, RTP protokolüne göre iki MGW arasında kurulduktan sonra, ACM mesajı ters yönde iletilir ve bu aşamada hedef uç telefonu çalmaya başlar. Hedef uç telefonu açarsa, ANM mesajı ters yönde iletilir, zil sesi hattan kesilir ve medya akışı çift yönlü başlatılır.



Şekil 5.6 : BICC'de İleri Yönde Çağırma Kurulumu

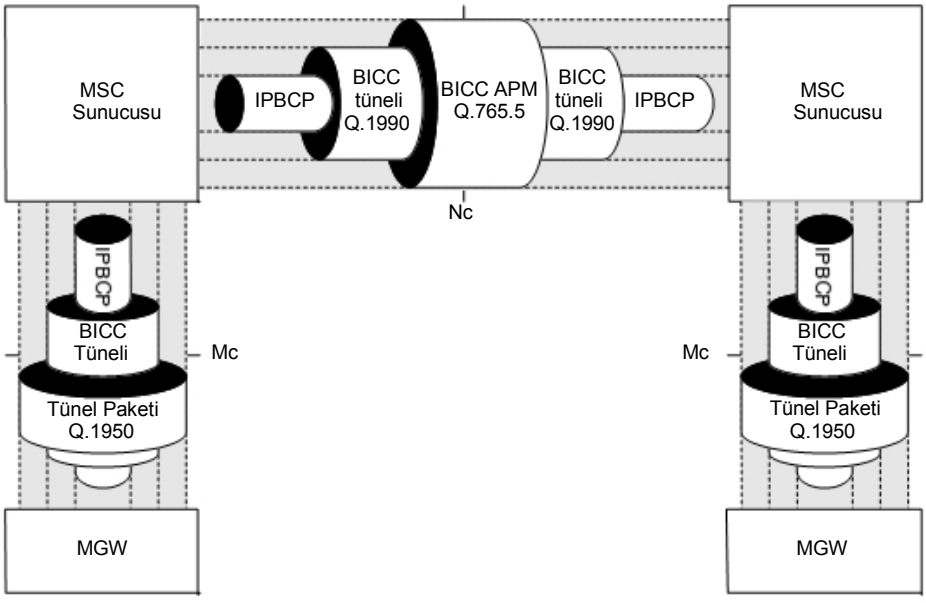
5.4.3. BICC IP Taşıyıcı Kontrol Protokolü (IPBCP)

IPBCP; IP şebeke birimlerine, aralarında taşıyıcı kurulumu için gerekli olan IP adreslerinin, RTP port numaralarının ve medya karakteristiklerinin karşılıklı görüşülmesini sağlayan kontrol protokolüdür. Bu içerikleri, 6. bölümde incelenecek oturum açıklama protokolünü kullanarak düzenler. IPBCP aşağıdaki mesajları destekler:

- İstek: Taşıyıcı kurulması isteği veya medya taşıyıcısının modifikasyonu
- Kabul: Taşıyıcı kurulması kabulü veya medya taşıyıcısının modifikasyonu
- Tanımlayamama: Diğer uçtan gelen isteğin formatının anlaşılamaması
- Red: Taşıyıcı kurulumu veya modifikasyonunun kabul edilmemesi

Genellikle taşıyıcı kurulumu talep eden uç, hedef uca istek mesajı gönderir. Belirli bir süre kabul veya red cevabı bekler. Bu süre zarfında herhangi bir yanıt alamazsa, tekrar istek mesajı gönderir.

IPBCP Tünellemesi: IPBCP mesajları Nb arabağdaşımı ile MGW'ler arasında doğrudan atanmış (dedicated) bir bağlantı üzerinden gitmesi yerine Nc ve Mc arabağdaşımları üzerinden tünellenerek iletilir. IPBCP mesajları BICC Tünelleme Protokolü (Q.1990) içerisinde kapsüllenir. BICC taşıyıcı kontrol tünelleme mesajı ise BICC APM mesajı veya BICC mesajları (Ör: IAM) içerisinde kapsüllenerek iletilir. Bu durum Şekil 5.7'de gösterilmiştir.



Şekil 5.7 : BICC'de IPBCP Tünellemesi

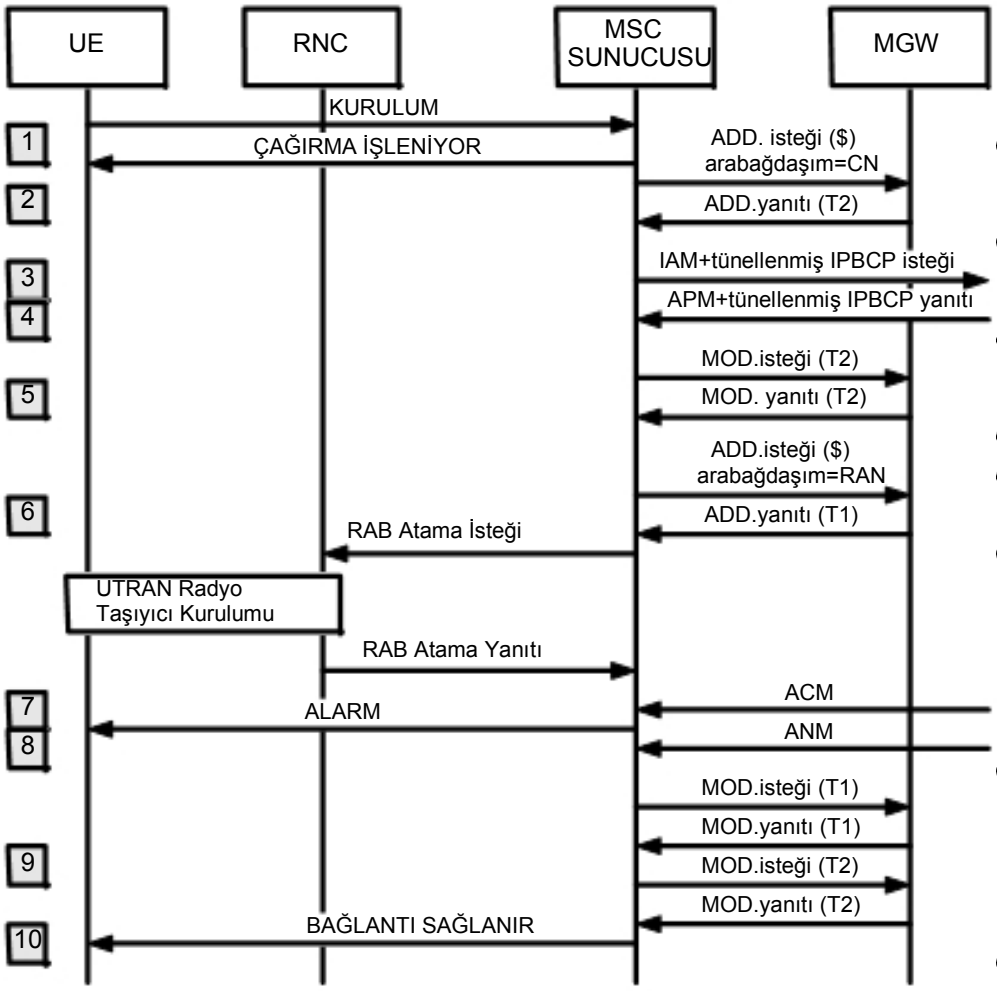
Tünellemenin 2 ana avantajı vardır. Birincisi, 2 MGW arasında bir TCP bağlantı kurulmasını beklemeden zaman tasarrufu sağlamaktır. İkinci avantajı ise BICC çağırma kontrol mesajları içerisinde enkapsüle edilerek iletilmeleridir.

5.4.4. UMTS R4'te BICC Çağırma Örneğine İlişkin Akış

Şekil 5.8'de UMTS R4'te mobil tarafından başlatılan ve PSTN abonesinde biten bir çağırmada BICC protokolünün nasıl işlediği aktarılmıştır.

1. Çağırma, mobil terminalden MSCS'e istek mesajı gönderilerek başlar

2. MSCS, kendine bağlı lokal MGW'ye taşıyıcı oluşturması amacıyla "add" mesajı gönderir. MGW de yeni bağlantı (context) ve sonlanma (termination) bilgilerini içeren bir yanıt verir.



Şekil 5.8 : UMTS R4'te BICC Çağırma Örneğine İlişkin Akış

3. MSCS, IAM mesajı üretir ve hedef uç numarasını sınayarak doğru uç MSCS'ine gönderilmesini sağlar. IAM mesajı ayrıca IPBCP isteğini de içerir.

4. MSCS, "add" komutu ile, kendine bağlı MGW'ye taşıyıcı kurmasını iletir. Bir önceki mesajda tünellenmiş IPBCP mesajını da alan uç MGW, kendi sonlanmasını hazırlar ve uç MSCS üzerinden APM mesajı içerisinde tünelleyerek lokal MSCS'e iletir.

5. Lokal MSCS, IPBCP yanıtını lokal MGW'ye Mod. isteği ile gönderir. Bu sayede iki MGW arasında taşıyıcı kurulmuş olur.

6. Lokal MSCS, radyo erişim tarafı için bir taşıyıcı hazırlar. "Add" komutu ile Iu arabağdaşımında bir sonlanma oluşturur. Bu komuta yanıt olarak sonlanmaya ilişkin IP adresi ve RTP port numarası MSCS'e iletilir. Daha sonra MSCS, RAN üzerinden UE ile RAB kurar (RNC'ye RAB erişim isteği ile). RNC, RAB erişim isteğine RAB erişim yanıtı ile yanıt verir ve taşıyıcı kurulur.

7. ACM mesajı hedef ucun bağlı olduğu MSCS'ten lokal MSCS'e iletilir ve MSCS de bunu UE'ye alarm mesajı olarak iletir. Bu aşamada hedef uç cihazında zil çalar ve MS'ye çalıyor sesi dinletilir.

8. Hedef uç telefonu açtığında, lokal MSCS'e ANM mesajı gönderir.

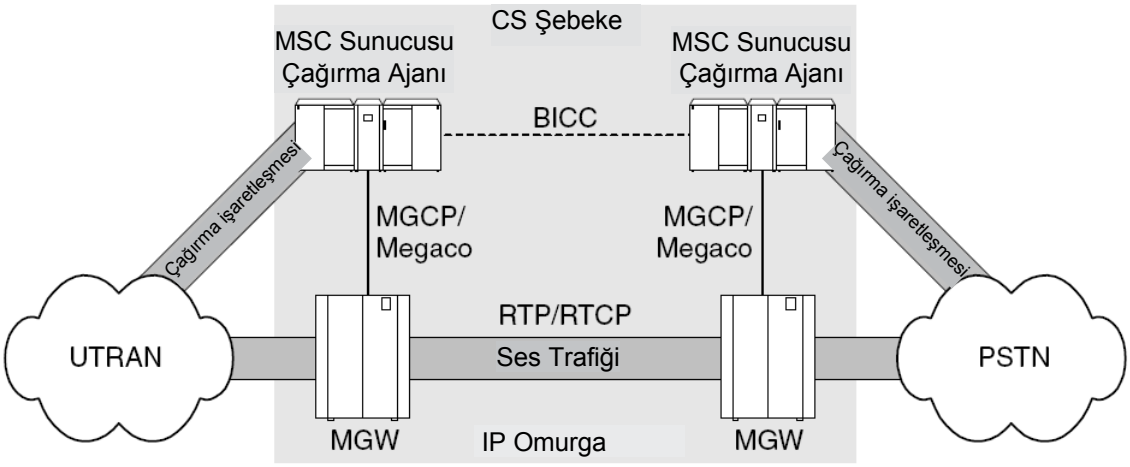
9. Çağırmanın yanıtlanması sırasında lokal MSCS, MGW'den çağırma yolunu izlemesini ister. Ses iletişimi için "ses işleyiş fonksiyonunu aktive et", veri iletişim için ise " eş işleyiş fonksiyonunu aktive et" istekleri ve cevapları, uçlar arasında karşılıklı iletilir.

10. UE'ye "bağlandı" mesajı iletilir ve bağlantı kurulur.

Kodlama tekniğine göre MGW'ler kod dönüştürme yeteneğine sahip olmalıdır. Klasik bir yöntem, iki MGW arasında PCM olarak şekilde dönüşüm yapmaktır. Bunun nedeni, her MGW'nin mutlaka PCM'i desteklemesi gerekliliğidir. Bu şekilde çekirdek şebeke içerisinde karşılıklı (MGW'ler arasında) kodlama aynı olur.

5.5. MEGACO – Medya Geçit Kontrol Protokolü

Medya geçitleri kontrol protokolleri (MEGACO), kontrol işaretlerinin ve kullanıcı verisinin farklı şekillerde işlenmesi ve iletimini sağlar. Şekil 5.9'da UMTS R4'teki MGW ve MSC Sunucu yapısı verilmiştir.



Şekil 5.9 : UMTS R4 MGW-MSC Sunucusu'na ilişkin Yapı

MGW kontrol protokolleri basit geçit kontrol protokolleri (SGCP) ile Bell Araştırma Merkezi'nde başlamıştır. Bu protokol UDP üzerinde çalışır ve sadece ses trafiği için geçerlidir. 1999'da IPDC ve SGCP birleştirilerek MGCP geliştirilmiştir. MGCP bu iki protokolü değiştirmiş ve uygulama alanlarını genişletmiştir. UMTS R4 için MGCP'nin yerini MEGACO protokolü almıştır.

MEGACO, MGCP'ye göre bazı geliştirmeler ve değişiklikler gösterilmiştir. ITU-T ile IETF'nin ortak ürünü olan MEGACO daha çok multimedya ve telekonferans ile ilgili düzenlemelere ağırlık vermiştir. Softswitch cihazı olarak MEGACO'da geçen MGW kontrolörü, UMTS R4'te MSC Sunucusudur. 3G sistemler için bu protokol genişletilmiş halde TS 29.232 tavsiyesinde belirtilmiştir.

MEGACO'da 2 soyut kavram tanımlanmıştır. Bunlar son ve bağlantı kavramlarıdır. Son, bir medyanın kaynağını temsil eder (Ör. Modem). Her sonlanma ise, fiziksel bir kaynağı temsil eder (Ör. TDM devresindeki bir zaman dilimi). Bağlantı ise bir son'un bağlanırlık özelliğini temsil eder. Bağlanırlığa sahip olan sonlar, aralarında veri alışverişi yapabilirler. Her son, tek olan bir sonlanma kimliği ile temsil edilir.

5.5.1 Olaylar ve İşaretler

Olaylar son'lar tarafından üretilir ve MGW'ler tarafından fark edilir. Sonrasında MSC sunucusuna bilgi iletilir. Olaya örnek olarak mikrotelefonun (ahize) kaldırılması veya numara çevrilmesi verilebilir. MSCS önceden belirlenen olaylar için MGW'ye modify mesajı iletir. Olay olduğunda, MGW notify mesajı ile karşılık verir. İşaretler ise hat durumunu (Ör. Meşgul tonu, telefonun zil sesi çalması) belirtir

ve MGW'deki son'lara uygulanır. MSCS modify mesajını kullanarak bu işaretlerin MGW son'larına uygulanmasını sağlar. Tüm olay ve işaretler paketler halinde gruplanmıştır. Bunlardan bazıları Tablo 5.1'de verilmiştir.

Bir son, paketin özellik ve ihtiyaçlarına göre bazı özellikleri karşılar. Örneğin MGW'ye bağlı bir analog hat DTMF ton farkındalığı, çağırma ilerliyor tonu üreteci paketlerini destekler.

Tablo 5.1 : MEGACO Paketleri

Paket İsmi	Paket Kimliği	Bilgi
Analog Hat Denetimi	Al	Ahize kaldırma, bırakma, Zil sesi'nin hatta uygulanması
DTMF Ton Farkedilmesi	Dd	Telefonda sayılara basınca rakamların fark edilmesi
RTP Paketi	Rtp	RTP bağlantısı ile ilgili bilgiler içerir. Ör: Gönderilen ve alınan bayt miktarı, ortalama jitter

5.5.2. MEGACO Komutları ve Açıklayıcıları

MEGACO'da Tablo 5.2'de verilen 8 farklı komut tanımlanmıştır. Bu komutlara ilişkin parametreler açıklayıcı olarak tanımlanır.

Bu durumda MGW'in bir sayı seçerek bunu MSCS'e iletmesi gerekir. Bu durum yeni bir bağlantı veya son oluşturulurken kullanılır. Tüm sonları ilgilendiren bir komutta son ID'si ROOT olarak düzenlenir.

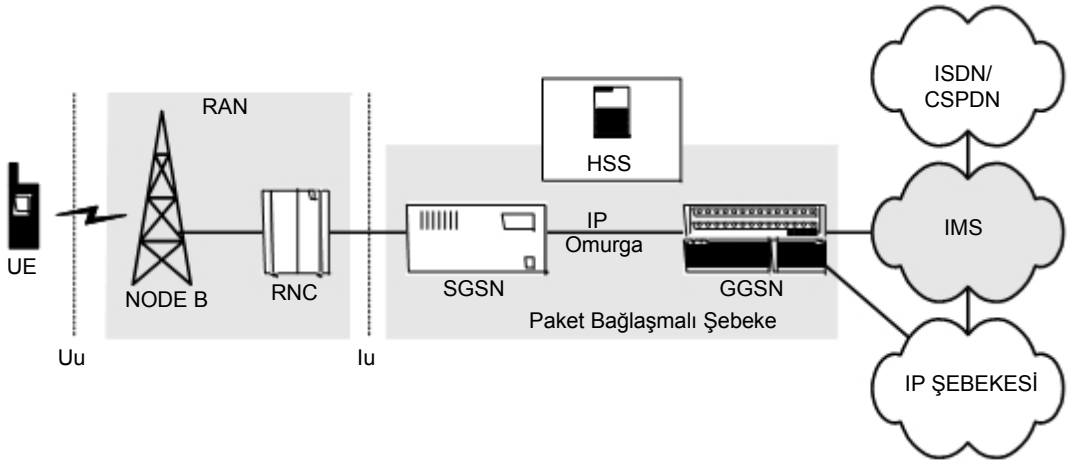
Tablo 5.2 : MEGACO Komutları

Komut	Kaynak	Amaç
Hizmet Değişimi	Medya Geçiti	MGW'nin hizmete gireceğini veya hizmet dışı kalacağını belirtir
Hizmet Değişimi	Medya Geçit Kontrolörü	MGW'ye hizmet dışı kalacağını veya hizmete gireceğini emreder
Yetenek Hesabı	Medya Geçit Kontrolörü	MGW'ye "son" ile ilgili tüm bilgileri (Ör: Kodek yapısı, veri hızı, vs.) iletir
Değişiklik	Medya Geçit Kontrolörü	Bir son'a ilişkin özellikleri değiştirme komutudur
Bildiri	Medya Geçit Kontrolörü	MGW'de olan her olay için MGW kontrolörünü bilgilendiren komuttur
Ekleme	Medya Geçit Kontrolörü	Bağlantıya bir son eklemek için kullanılır
Çıkarma	Medya Geçit Kontrolörü	Bağlantıdan bir son çıkarmak için kullanılır
Taşıma	Medya Geçit Kontrolörü	Bir son'u bir bağlantıdan diğerine taşımak için kullanılır

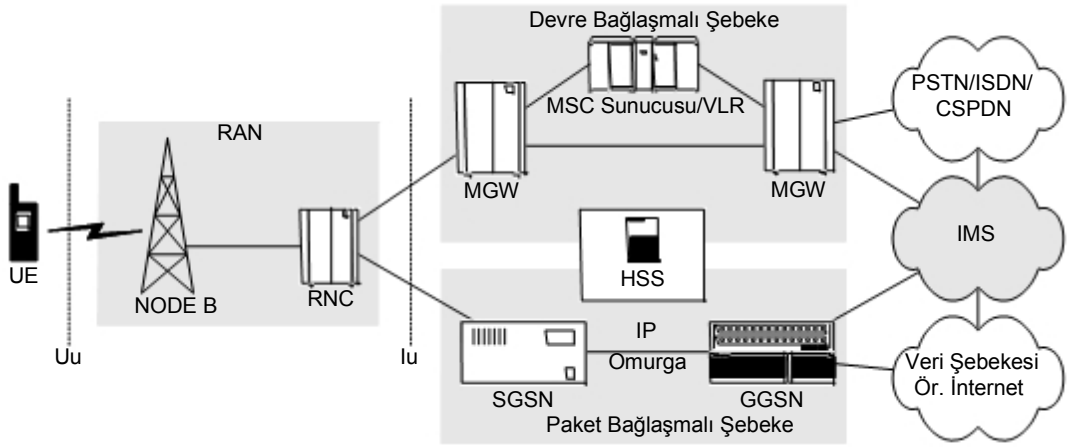
6. UMTS SÜRÜM 5 (R5)

6.1. UMTS R5 Genel Şebeke Yapısı

3GPP tarafından R4'ün bir üst sürümü olarak oluşturulan R5, UMTS çekirdek şebekede tamamen IP tabanlı yapı üzerinden paket bağlaşmalı olarak uçtan uca iletim sağlar. TÜM-IP yapısına geçişte önemli aşamalardan biri olan R5'te paketler, radyo erişim şebekesi de dahil olmak üzere GPRS çekirdek şebekesi ve IMS üzerinden tamamen IP tabanlı olarak uçtan uca iletilebilir. R5, R4'ün bir üst sürümü olduğundan, mevcut kullanılan ATM tabanlı mobil şebekenin sağladığı QoS, güvenlik vs. gibi hizmetlerin IP tabanlı şebekede de sağlanması gereklidir. Radyo erişim şebekesinde (UTRAN) de ATM'den IP'ye geçiş UMTS şebekesi için önemli bir yeniliktir. R5'te uçtan uca IP tabanlı şebeke kurgulanmış olsa da mevcut durumda kullanılan ATM tabanlı şebeke ve hizmetler de R5'te sağlanır. Geçişin tamamlandığı düşünüldüğünde, CS domeni tamamen PS domene geçecek ve IP QoS mekanizmaları ile gerçek zamanlı ses, video ve ilgili hizmetler GPRS ve IMS şebekeleri üzerinden iletilebilecektir. R4'ten R5'e aşamalı geçişi ve R5 UMTS şebekesine ilişkin yapı Şekil 6.1 ve Şekil 6.2'de verilmiştir.



Şekil 6.1 : UMTS R5 Genel Şebeke Yapısı



Şekil 6.2 : UMTS R4'ten R5'e Geçiş

6.2. IMS - IP Mulimedya Alt Sistemi

3GPP tarafından R5'te tanımlanmış olan IP Multimedya Altsistemi (IMS), 3G şebeke bağlamında bir grup şebeke elemanından oluşan; ses, video, yazı ve bunların kombinasyonu olan multimedya servisleri olarak adlandırılan hizmetleri PS domeni üzerinden sunan sisteme verilen addır. IMS, UMTS ile birlikte mobil terminallere uçtan uca IP tabanlı şebeke üzerinden bu şebekeye uygun uygulamaların erişimini sağlar. IMS, mobil şebekeler ile dış dünyadaki IP ve PSTN şebekelerin birbirlerine efektif şekilde bağlanmalarını da temin eder. Bu alt bölümde, IMS ayrıntılı olarak incelenmiş, çeşitli örnekler verilmiştir.

6.2.1 IMS Genel Özellikleri

Teknolojik gelişmeler ışığında, şebekelerin ve servislerin çeşitliliği göz önüne alındığında, tek bir şebeke ve tek bir mimari yapı üzerinden tüm trafiğin ve servislerin sağlanması fikri bir gereksinim olarak karşımızdadır. IP'nin iletişimdeki rolünün giderek yaygınlaşması, TÜM-IP (ALL-IP) modelinin oluşumuna zemin hazırlamıştır. TÜM-IP şebekenin oluşumundaki en önemli faktör budur. Bu yapılanmanın birden bire oluşması beklenemez. TÜM-IP yapısına aşamalı olarak geçiş benimsenmiştir. Mobil şebekeler ile sabit şebekeleri ortak bir yapıda buluşturmak (Fixed-Mobile Convergence) TÜM-IP yapısının temelini teşkil eder. Geleneksel devre bağlaşmalı mobil şebekelerin sunduğu hizmeti aynı kalitede sağlamak, ek olarak birtakım faklı hizmetleri de aynı zamanda sunmak gereklidir.

IMS, bu anlamda mobil şebekeler ile gerçek zamanlı ses hizmetinin yanında multimedya hizmetlerini de sunar. IMS'in kullanıcılara sağladığı hizmetler;

- Gerçek zamanlı ses, video ve multimedya iletişimi
- Ses ve video konferans
- Video, ses ve multimedya içeriklerinin uç birimlerine yüklenebilmesi (download)
- Multimedya mesajlaşması

IMS'in oluşumunda rol alan ve gelecekte yaşayacağı değişimlere yön veren ihtiyaçlar aşağıda verilmiştir:

Esnek Erişim: IMS bir çekirdek şebeke standardı olduğundan dolayı IP bağlantı özelliği olan herhangi bir erişim şebekesi vasıtasıyla IMS hizmetlerini alacak uygun terminallere hizmet verebilmelidir. Örneğin UTRAN, Iu-PS arabağdaşımı ile bu erişimi sağlar. R5'te GPRS çekirdek şebekesine has bazı özellikler bu kavramı sınırlandırmıştır.

Dolaşım(Roaming): IMS kullanıcıları farklı operatörler arasında dolaşım yapabilmelidir. Lokal şebekede sağlanan tüm hizmetlerin dolaşım yapılan şebekelerde de sağlanması gerekir.

Kullanıcı odaklı hizmet ihtiyacı: Kullanıcı erişim kontrolü, kullanıcı yeteneği ve kapasitesinin pazarlığı, kalite pazarlığı gibi kavramlar IMS oturum oluşumunda ele alınır.

Gizlilik, güvenlik ve denetim: Güvenlik ve gizlilik anlamında IMS sistemi en az mevcut GPRS sistemi kadar güvenli ve gizli olmalıdır. IMS ile UMTS çekirdek şebekesi arasında operatöre yetkilendirme ve taşıyıcı kontrol mekanizmaları anlamında esneklik sağlanmalıdır.

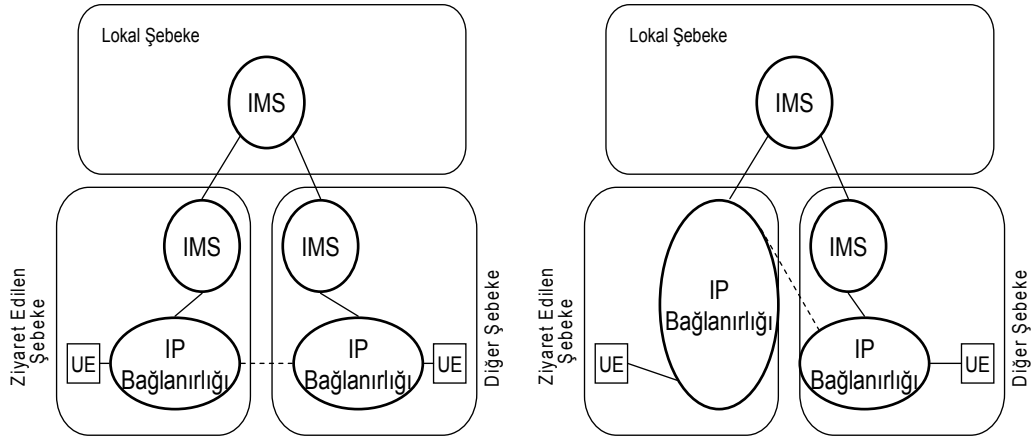
Standartizasyon: IMS'te hizmetler sınırlandırılmamalıdır. Çeşitli hizmetlere olanak sağlayan yetenek ve kapasiteye dayalı olarak, operatörlere farklı ve çeşitli hizmetler sunulmasına olanak tanınmalıdır.

Diğer şebekelerle uyumlu çalışma: 3 alt başlık bu konu bağlamında değerlendirilebilir. İlk olarak; IMS sistemi dış CS şebekeler (PSTN, ISDN) ile uyumlu çalışır ve mobil operatörler ile dış CS şebekeler arasında köprü görevi görür.

İkincisi, dış IP şebekeler ile mobil kullanıcılar arasında özellikle operatör dışındaki IP uygulamalarının MS'ler tarafından kullanılabileceği bir şebeke altyapısı oluşturmaktır. Son olarak gelecek nesil dış şebekeler ile mobil şebekelerin uyumlu şekilde çalışmalarına zemin hazırlamaktır.

IMS Oturumu: Bir IMS oturumunda kullanıcılar IP tabanlı tüm servisleri eş zamanlı veya ayrı ayrı kullabilirler. Ses, video, yazı, resim gibi içerikleri aynı anda aynı oturum içerisinde kullanabilirler. Oturum sırasında yeni bir servisi oturuma dahil edebilir veya çıkartabilirler.

IP Bağlantılı Olma: IMS'in ihtiyaç duyduğu en önemli özellik IP bağlanırlığıdır. Bu nedenle IP adresleri konusunda sıkıntı olmayan IPv6 IMS için kabul edilen versiyondur. Geçmiş ile uyumluluk anlamında IPv4'ü de destekleyen bir yapı kabul edilmiştir ve bunu destekleyen spesifikasyonlar 3GPP'nin TR 23.981 tavsiyesinde belirtilmiştir. Şekil 6.3'te kullanıcının dolaşım yaptığındaki 2 farklı durum belirtilmiştir.



Şekil 6.3 : IMS ile Dolaşım (Roaming) Arasındaki İlişki

İlk durumda her şebekenin IMS sistemi vardır. Gelecek bölümlerdeki incelemelerde bu durum ayrıntılı olarak ele alınacaktır. Dış şebeke ile lokal şebeke arasında sadece IP bağlantı özelliği olsa bile, IMS servisleri lokal şebeke üzerinden sağlanabilir. Teknoloji henüz geniş çapta bu uygulamaya elverişli olmasa dahi teoride uygulanmasına engel teşkil eden bir durum yoktur.

IMS Servisleri için QoS anlamında Emin Olmak: İnternette paketlerin gecikme süreleri, kaybolmaları veya atılmaları mümkün iken IMS ile bu konu asgariye indirilmiştir. Şebekeler IMS ile birlikte düşünüldüğünde, erişim ve iletim olarak

uçtan uca QoS sağlanır. UE, oturum kurulum sürecinde QoS gereksinimlerini, kendi yeteneklerini ortaya koyarak pazarlık yapılır. Pazarlık yapılan bazı parametreler şunlardır:

- Medya tipi
- Medya tip bit hızı, paket boyutu, iletileceği frekans
- Medya tipi için kullanılacak RTP ek yükü
- Bant genişliği adaptasyonu

Bu parametreler ile ilgili olarak mobil operatörlerin hizmet seviyesi anlaşması yaparak ilgili QoS'u sağlayabilecekleri konusunda fikir birliğine varmaları gerekir.

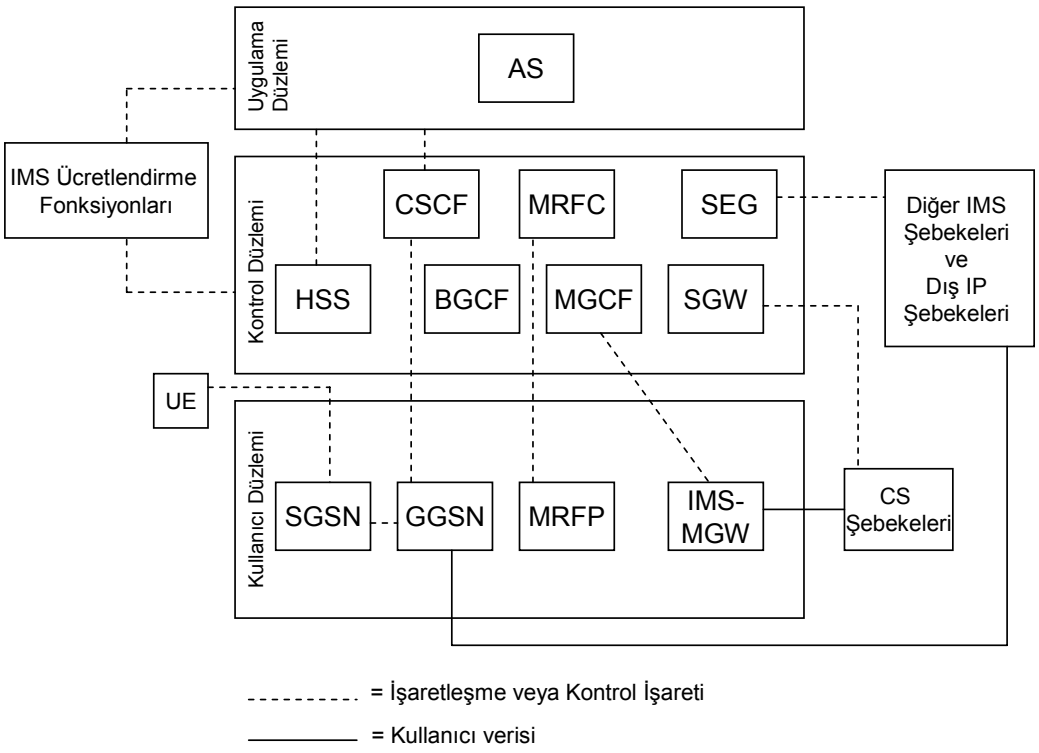
IMS'te Ücretlendirme: Operatörler için büyük önem taşıyan bu özellik, IMS'in sunduğu farklı ücretlendirme modelleri ile kullanılabilir. Operatörler iletim katmanında akan trafik ve trafiğin niteliği (hizmet türü ve içeriği) ücretlendirmede önemli rol oynar. Online ve offline ücretlendirme yapılabilir. Bu sayede ön ödemeli veya faturalı aboneler için farklı ücretlendirme mümkündür.

6.2.2. UMTS R5 Şebeke Yapısı (Düzlem Bazında) ve IMS Şebeke Elemanları

IMS oluşumunda katmanlı yapı göz önünde bulundurularak bu yapıya uygun bir şebeke alt sistemi geliştirilmiştir. Şekil 6.4'te bu yapı ve IMS şebeke elemanları gösterilmiştir.

Bir sonraki bölümde bu elemanlar ve arabağdaşımlar ayrıntılı incelenecektir. Katmanlı yapı sayesinde kontrol işaretleri ile kullanıcıya sunulan hizmete ilişkin taşıyıcılar ve uygulamalar farklı katmanlarda iletilir.

- IMS elemanları fonksiyonlarına göre 4 ana kategoride sınıflandırılabilir:
- Oturum Yönetim ve Yönlendirme Ailesi (CSCF)
- Lokal Abone Sunucusu (HSS)
- Hizmet Fonksiyonları (Uygulama Sunucusu, MRFC, MRFP)
- Uyumlu Çalışma Fonksiyonları (BGCF, MGCF, IMS-MGW, SGW)



Şekil 6.4 : UMTS R5'in Düzlem Bazında Yapısı

6.2.2.1. Çağırma Oturum Kontrol Fonksiyonu (CSCF)

3 tip CSCF vardır. Bunlar Proxy-CSCF (P-CSCF), Hizmet Veren CSCF (S-CSCF) ve Sorgulayıcı (Interrogating) CSCF'tir (I-CSCF). Her CSCF'in kendine özgü görevleri vardır. Bu bölüm içerisinde her üçü de incelenecektir. CSCF'lerin benzer özellikleri; kayıt, oturum kurulumu ve SIP yönlendirilmesinde görev almalarıdır. Ek olarak, ücretlendirme anlamında CSCF'lerden gelen tüm bilgiler offline ücretlendirme fonksiyonuna dahildir. Her 3 fonksiyon da kullanıcı adına oturumu sonlandırabilir, SDP'nin içeriğini kontrol edebilir ve kullanıcı için bu SDP'nin medya tipi ve kodekler anlamında uyumlu olup olmadığını kontrol edebilir.

P-CSCF: Proxy çağrı oturum kontrol fonksiyonu (P-CSCF), kullanıcının IMS ile ilk iletişime geçtiği (bir çeşit geçit olarak kabul edilebilir) birimdir. IMS'ten UE'ye iletilecek SIP işaretleşme işaretleri mutlaka P-CSCF üzerinden iletilir. P-CSCF'e atanmış 4 ana görev vardır. Bunlar; SIP şıkıştırması, IPSec güvenliği sağlanması, Denetim Karar Fonksiyonu ve Acil Oturum Fark Edilmesi ile bire bir iletişimde olmaktır. SIP Protokolü, yazı (text) tabanlı işaretleşme protokolü olması nedeniyle birçok başlık ve başlık parametleri içerir. Uzatma ve güvenlik ile ilgili bilgiler, ikili kodlama kullanan protokollere göre yazı tabanlı sistemlerde paket boyutu büyür. Bu

nedenle P-CSCF, SIP sıkıştırması yaparak bu sorunu giderir. P-CSCF, güvenlik birliğini (SA) sürdürmek ve SIP işaretleşmesinin korunmasından da sorumludur. Bu güvenlik SIP kaydı sırasında UE ve P-CSCF arasındaki IPSec pazarlığı ile sağlanır. UMTS R5'te Denetim Karar Fonksiyonu (PDF), P-CSCF ile birlikte aynı birim içerisinde bulunur. Destek fonksiyonu alt bölümünde PDF incelenmiştir.

I-CSCF: Lokal IMS ile diğer operatörlere ait IMS'ler arasında arabağdaşım olan birimdir. Başlıca görevleri;

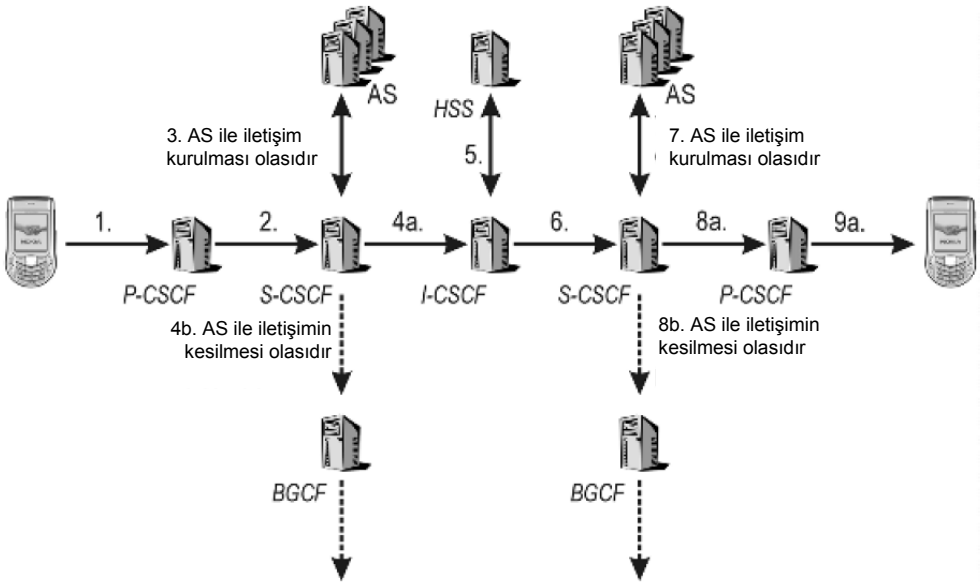
- HSS'ten gelen bilgileri ilgili birimlere yönlendirmek
- Gelen kayıt isteklerinde, S-CSCF'in aboneye atanmasını sağlamak

S-CSCF: Bu birim, IMS'in merkezi birimi olarak tanımlanır. Görevleri;

- Kayıt işlemlerini yürütmek
- Şebeke içerisinde yönlendirme kararlarını vermek
- Oturum durumunun sürdürülebilirliğini sağlamak
- Hizmet profillerini kayıt altına almak

Kullanıcı bir kayıt isteğinde bulunursa, ilgili mesaj S-CSCF'e yönlendirilir ve S-CSCF, HSS'ten doğrulama bilgilerini alır. UE ile ilgili işaretleşmeler sonucunda kayıt işlemini yapar. Bu işlem için gerekli olan kullanıcıya ait hizmet profil bilgilerini de HSS'ten alır. Hizmet profil bilgisi, UE'ye ilişkin hangi tip hizmetleri kullanabileceği ve hangi AS'yi kullanacağına dair bilgileri içeren ve HSS'te tutulan bir kayıttır.

S-CSCF, UE tarafından başlatılan ve UE'de bitirilen tüm oturumlarda yönlendirme kararını veren şebeke elemanıdır. UE'den P-CSCF aracılığıyla S-CSCF'e gelen istekle ilgili olarak öncelikle AS ile kontak kurulmasına gerek olup olmayacağına karar verilir. Olası AS iletişimi sonrasında, S-CSCF ya diğer domenlere (CS veya diğer bir IP şebeke) yönlendirme işlemi ya da IMS çağırmaların da P-CSCF üzerinden GGSN'e ve UE'ye iletim işlemini yapar. Bunun nedeni, P-CSCF'in UMTS şebekesine tek arabağdaşım olması, sıkıştırma ve güvenlik mekanizmalarının P-CSCF tarafından yönetilmesidir (Şekil 6.5).



Şekil 6.5 : CSCF'lerde Yönlendirme

6.2.2.2. HSS

HSS, IMS'e ilişkin ana veritabanını oluşturur. HSS'te operatöre ait kullanıcı kimlikleri, kullanıcı-kullanabileceği hizmet ilişkisi, kullanıcı kayıt bilgileri, erişim parametreleri bulunur. Kullanıcı kimliği özel veya genel kimlikler olmak üzere 2'ye ayrılır. Özel kimlikte, lokal şebeke tarafından kullanılabilen kayıt ve yetkilendirme bilgileri bulunur. Genel kimlikte ise diğer kullanıcıların o kullanıcıya bağlantı kurmak amacıyla istek yapabilmeleri için kullanılan bilgiler bulunur. IMS erişim parametreleri ise oturum kurulumunda gerekli olan kullanıcı doğrulama, dolaşım yetkilendirmesi için kullanılan bilgileri içerir.

HSS içerisinde, UMTS sistemindeki HLR ve CS-PS fonksiyonları için ayrıştırılmış bilgiler de bulunur. UMTS R5'te HLR ve AuC birimleri tek bir birimde (HSS) birleştirilmiştir.

6.2.2.3. Hizmet Fonksiyonları

Multimedya Kaynak fonksiyonu (MRF), iki birimden oluşur. Bunlar MRF kontrol (MRFC) ve MRF işleme (MRFP) birimleridir. R4'teki MSCS – MGW yapısına benzer bir bölünme söz konusudur. Bu birimlerin görevi, ses / video konferansı için medya bilgisini karıştırmak, multimedya duyurularını sağlamak ve medya akımını işlemektir.

Uygulama sunucusu (AS), IMS şebekesi dışında kullanılabilen bir birim olmasına rağmen IMS sistemi içerisinde değerlendirilecektir. AS genel olarak katma değerli hizmetlerin abonelere sunulmasına hizmet eder.

6.2.2.4 Uyumlu Çalışma Fonksiyonları

Burada incelenecek 4 fonksiyon, IMS ile dış CS şebekeler (PSTN, ISDN) arasındaki işaretleşme ve medya akışı için kullanılan birimlerdir.

Breakout Geçit Kontrol Fonksiyonu (BGCF), dış CS şebekede sonlanacak bir çağrının (S-CSCF'ten gelir) doğru MGCF'ye yönlendirilmesinden sorumludur.

Medya geçit kontrol fonksiyonu ve medya geçiti, dış CS şebeke ile IMS arasında bağlantıyı sağlar. MGCF, SIP protokolü ile olan arabağdaşımı kontrol eder. Dış CS şebekeden SGW'ye gelen işaretleşme işaretleri (SS7 veya ISUP), SIGTRAN kullanılarak MGCF'ye iletilir. MGCF, SIP ve ISUP arasında çevirmenlik yapar. Uyumlu çalışma için bu gereklidir.

6.2.2.5 Destek Fonksiyonu

Denetim Karar Fonksiyonu; P-CSCF'ten alınan oturum ve medya ile ilgili bilgilere dayanarak bir denetim kararı vermekle sorumlu birimdir. Oturum kurulumu esnasında, uçtan uca SIP ve SDP mesajları iletilir. Karşılıklı bu mesajlaşma sırasında UE'ler, medya karakteristikleri konusunda pazarlık yapar. Bir UE'den gelen bağlantı isteği olduğunda, bağlantı ile ilgili SDP bilgileri P-CSCF vasıtasıyla PDF'e gelir. PDF, aynı P-CSCF'e bir yetkilendirme mesajı iletir. Bu sayede PDF oturum kurulumu sırasında ilgili SDP parametreleri ile kendi yetkilendirdiği şekilde QoS seçilmesini ve bu şekilde GGSN'e iletimini sağlar. PDP Bağlantı aktivasyonunda, GGSN yetkilendirme bilgisi için P-CSCF üzerinden PDF'i sorgular. Kurulan PDP bağlantısındaki akan medya özellikleriyle kendinde kayıtlı bilgileri karşılaştırır ve kararı GGSN'e iletir.

6.2.3. SIP - Oturum Başlatma Protokolü

Oturum Başlatma Protokolü (SIP), IP tabanlı bir şebeke üzerinden kullanıcılar arasında multimedya oturumlarının kurulmasına zemin hazırlayan bir protokoldür. SIP ile ilgili spesifikasyonlar, IETF tarafından RFC3261 tavsiyelerinde belirtilmiştir. Bu alt bölümde, SIP protokolü ayrıntılı olarak incelenmiştir.

6.2.3.1. SIP Protokolünün Genel Yapısı

IMS içerisinde genel olarak kullanılan protokol SIP'tir. SIP ile desteklenen hizmet türleri şunlardır:

- Multimedya çağırma kurulumu
- Kullanıcı mobilitesi
- Konferans çağırması
- Ek hizmetler (Çağırma yönlendirme, çağrı bekletme vs.)
- Doğrulama ve fiyatlandırma
- Birleşik mesajlaşma (ses / video vs.)
- Anlık mesajlaşma ve bulunma farkındalığı

SIP'in Tüm-IP'ye geçişte sağladığı önemli avantajlar şunlardır:

- Mobil kullanıcı ile sabit kullanıcı arasında uçtan uca SIP işaretleşmesi sağlanması
- İnternet SIP sunucularının mobil kullanıcılara katmadeğerli hizmetleri daha kolay ve esnek şekilde sunması
- SIP'in daha az işaretleşme yükü gerektirmesi
- Basit bir yapıya sahip olması

SIP ile UMTS operatörleri kendi abonelerine İnternetteki hizmetleri daha esnek ve kolay şekilde sunabilecektir. Örneğin, bir UMTS operatörüne bağlı bir abone, İnternete bağlı bir bilgisayarın sürdürdüğü bir video oturumuna katılabilecektir.

BICC, mevcut PSTN şebekeler ile mobil şebekelerin uyumlu çalışmasında önemli bir protokol olmasına karşın, sesin IP üzerinden taşınmasında önemli olan multimedya veya ekstra hizmetleri sunmaz. SIP ile zenginleştirilmiş gerçek zamanlı olan-olmayan hizmetler birarada eş zamanlı sunulabilir.

6.2.3.2. SIP Adreslemesi

SIP adreslemesi, SIP kullanıcılarının bağlantı kurulumunda tanınması ve yerinin belirlenmesi amacıyla kullanılır ve SIP uniform kaynak belirteci (URI) ile belirtilir. 2 tip URI vardır. Birincisi, e-mail formundadır. Ör: ahmet.erten@xtel.com.

Diğeri ise kullanıcı kısmında telefon numarası yazan ve önünde "+" belirteci ile belirtilmiş formattaki URI'dir. Ör: +5658447654421@gw.com;user=phone

İlk format İnternet'e bağlanma durumunda kullanılır. 2.cisi ise belirtilen telefon numarasını temsil eder ve kullanıcı bir PSTN geçitine mutlaka bağlanmalıdır. UMTS şebeke abonesi, SIP ile ilgili kimliği (Ör: SIP adresi) İnternet Multimedya Sistem Abone Kimlik Modülü (ISIM) içerisinde barındırır. Bu bilgi, UMTS operatörüne ait SIM kartı içerisindedir. ISIM uygulaması olmayan UE'lerde SIP adresi;

sip: IMSI numarası@MNC.MCC.IMSI.3ggpnetwork.org

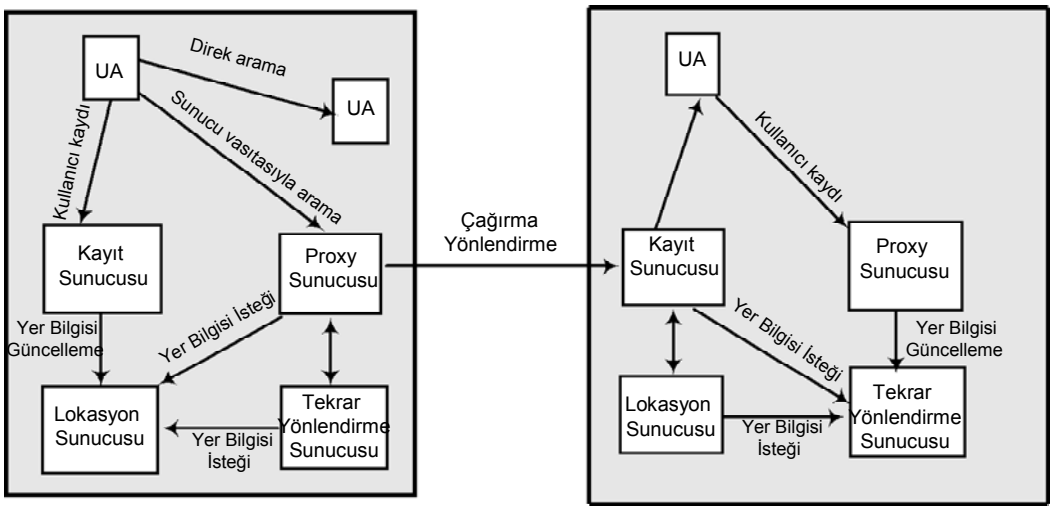
olarak geçerlidir. MNC ve MCC, IMSI'deki kodlardır ve bunlar sayesinde hangi ülkede hangi operatöre ait olduğunu belirler. Bu tipteki SIP adresi, sadece IMS içerisinde (S-CSCF ile HLR arasında) kullanılır. Dış şebekeler için güvenlik nedeniyle kullanılmaz.

6.2.3.3. SIP Elemanları

SIP içerisindeki birimler temel olarak kullanıcı ajanları (UA) ve sunuculardan oluşur. Şekil 6.6.'da bir SIP şebekesine ilişkin temel elemanlar verilmiştir. SIP sunucuları, çağrı kurulumunda ve mobilite yönetiminde görev alırlar. Fakat kullanıcılar sunucular olmadan da (direk birbirleri ile) bu işlemleri yapabilir. Proxy ve tekrar yönlendirme sunucuları bir önceki durumlarını hafızalarında tutmazlar.

UA, bir SIP kullanıcısı adına çağırmaları kabul eden veya reddeden birimdir. SIP kullanıcısı, bir kişi veya sunucu üzerindeki bir uygulama olabilir. UA, SIP çağırma işaretleşmelerini sonlandırır ve SIP şebekesine bir nevi arabağdaşım teşkil eder. UA'lar kullanıcı ajan sunucusu (UAS) veya kullanıcı ajan alıcısı (UAC) olarak davranabilirler. UAS'ın görevi, SIP isteklerini karşılamak ve uygun-gerekli yanıtı (kabul, red vea meşgul) vermektir. UMTS şebekesinde UE, UA'ları (UAC, UAS) içerir. UA bir sunucu da olabilir. Örneğin bir uygulama sunucusu istek anında video hizmeti (video on-demand) sunsun. UA, abonelerden gelen istekleri kabul eder, sonrasında medyayı ilgili kullanıcılara iletir.

Proxy sunucusu, SIP ajanı adına istekleri yönlendiren birimdir. SIP Proxy, SIP mesajını doğru yere gitmesi için yönlendirmeden önce tekrar yazabilir. Proxy sunucusu ayrıca doğrulama fonksiyonlarından ve kamusal şebekeler ile özel iç şebeke arasında kontrolör görevi görür.



Şekil 6.6 : SIP Şebeke Elemanları

Kayıt Sunucusu, SIP ajanına o anda bulunduğu yerin kaydedilmesini sağlar. UMTS şebekesi düşünüldüğünde, bulunulan yerden kasıt PDP Bağlantı kurulumu sırasındaki varış IP adresidir. İçeriğinde, UTRAN hücre adı ile bağlı olduğu P-CSCF'in kimliği bulunur. Kayıt sunucusu, "update" mesajı göndererek UE'nin yeri hakkındaki bilgiyi devamlı güncel tutar.

Tekrar yönlendirme sunucusu, UA isteğine aranan kullanıcının o andaki lokasyon bilgisini ileterek yanıt verir. Bu durumda, UA bu yanıt içeriğindeki lokasyona göre yeni bir çağırma başlatmak zorundadır.

Lokasyon sunucusu, kullanıcıdan mevcut bulunduğu yere ilişkin bilgiyi sağlayan birimdir. Tekrar yönlendirme sunucusu ve proxy sunucusu, abone yeri sorgulama için bu birimi kullanır.

6.2.3.4 SIP Mesajları

SIP protokolü, tüm fonksiyonlarını 6 ana tipteki mesajlar ile yürütür. Bu mesajlara metod denir. SIP mesajları, RFC 3261 tavsiyelerinde belirtilmiştir.

INVITE ve ACK, SIP çağırma kurulumu için kullanılan mesajlardır. INVITE mesajı çağırmayı başlatmak için, ACK mesajı ise çağırma kurulumunda son aşamada diğer ucu bilgilendirme amacıyla kullanılır. BYE mesajı, daha önceden kurulmuş aktif bir çağırmada uç birimlerinden birinin oturumu sonlandırması durumunda kullanılır. CANCEL mesajı, çağırma kurulumu sırasında uçlardan birinin kurulumu başlamadan sonlandırması durmunda kullanılır. Bu mesaj, kişinin telefonu çalarken çağırmayı

reddetmesi durumunda da kullanılır.

REGISTER mesajı, UA tarafından kendi lokasyonunun ve ulaşılabilirliğinin kayıt sunucusuna kaydedilmesini amaçlar. Kayıt işlemi, UA aktif hale geldiğinde (telefon ilk açılıp kendi operatörüne bağlanıldığında) veya farklı bir operatöre geçtiğinde (roaming) yapılır.

OPTIONS mesajı, proxy sunucuların ve aranacak kullanıcıların yeteneklerini ve özelliklerini (Ör: Kodek yapısı) sorgulamak için kullanılır.

INFO mesajı, SIP çağırmalarının durumunu değiştirmeyen uygulama işaretleşme işaretleri için kullanılır. Örnek olarak DTMF sayılarının iletilmesi verilebilir.

PRACK (Geçici bilgilendirme) mesajı, çağırma kurulumu sırasında geçici bilgilendirmeler yapmak amacıyla kullanılan mesaj türüdür. Bu mesaj, UMTS'te daha sonra incelenecek olan yanıt mesajlarının iletildiğinden emin olunması için iletilir (Ör: Zil sesi 180-RINGING; aranan kişinin telefonunun çaldığına ilişkin mesajı arayana iletir).

UPDATE mesajı, çağırma kurulumu tamamlanmadan kullanıcıya çağırma ile ilgili değişiklik yapma olanağı tanır. Genellikle bir oturum için üzerinde anlaşılan QoS parametrelerinin belirteci olarak kullanılır.

REFER mesajı, UA'nın 3. parti bir kullanıcı ile oturum kurulumu için kullanılır. Bu sayede çağırma yönlendirme, konferans v.b. ek hizmetlerin sağlanması olanaklı olur.

SUBSCRIBE ve NOTIFY mesajları, olayların not edilmesi için kullanılır. Bir "olay"a örnek olarak meşgul olan bir abonenin çağırma bittikten sonra ulaşılabilir hale gelmesi, yeni bir e-postanın kullanıcıya gelmesi verilebilir.

MESSAGE mesajı, anlık mesajlaşma için kullanılır. Oturum kurulumuna gerek olmadan bir UA'dan diğer UA'ya kısa mesaj iletimi sağlar.

6.2.3.5. SIP Yanıtları

SIP cihazları; kendilerine gelen istek mesajlarına 6 sınıflandırmada yanıt verirler.

1xx, geçici ve bilgilendirme amaçlı yanıtları temsil eder. Örneğin 180 RINGING yanıtı, kaynak UA'ya, hedef UA'daki cihazın zilinin çaldığı bilgisini iletir. 100 TRYING yanıtı ise sunucunun aranan uç ile iletişime geçme denemesi yaptığını belirtir.

2xx-6xx arasındaki kodlar ise son yanıt kodları olup hareketin (transaction) biteceğini belirtir. 2xx yanıtı komutun başarılı olduğunu gösterir. 3xx yanıtı, hedef ucun farklı bir lokasyon üzerinden tekrar bağlanmasını denemesi gerektiği zaman kullanılır. 4xx, 5xx ve 6xx, çeşitli hata durumlarını göstermek amacıyla kullanılır.

6.2.3.6. SIP'te Hareket Yürütülmesi

Her SIP Hareketi; bir istek mesajından, bir ya da daha çok geçici bilgi ve bir ya da daha çok son yanıtlardan oluşur. SIP protokolü, hem TCP'yi hem de UDP'yi kullanabilme özelliğine sahip olduğundan, mesajların kaybolmaması için bir güvenlik mekanizması olması gerekir. SIP'in özellikle UDP üzerinde uygulanması durumunda, kaynak uç önceden belirlenen süre bitiminde yanıt mesajı alamazsa aynı mesajı tekrar gönderir. INVITE mesajı dışındaki tüm mesajlar, son yanıt alınana kadar tekrar gönderilir. INVITE mesajında ise ilk bilgilendirme yanıtı alındığında, tekrar gönderim durdurulur. Hareket, son ACK mesajı ile tamamlanır. UA bir mesaj aldığında, kaynak uca bilgilendirme amacıyla PRACK mesajı gönderir. Buna karşılık olarak 200 OK (hata yok ise) mesajı ters yönde iletilir.

6.2.3.7. SIP Mesaj İletimi

Bütün SIP birimleri, TCP ve UDP protokollerini desteklemelidir. Güvenlik anlamında TCP üzerinde daha once 4. bölümde incelenen TLS kullanılabilir. TCP güvenlik açısından UDP'ye göre avantajlıdır. Fakat bağlantı kurulumu sırasında UDP'ye gore daha fazla işaretleşmeye ihtiyaç duyar. SIP için TCP'nin algoritmalarına gerek yoktur. Bunun nedeni, SIP'in kendi tekrar iletim mekanizmasına sahip olmasıdır. UDP, işaretleşme anlamında ek bir yük getirmez fakat UDP'de yığılma ve akış kontrol mekanizması (TCP'de var) yoktur.

6.2.3.8. SIP Başlıkları

Başlık kısmı, bir SIP isteğinde kullanılması gereken bazı bilgileri içerir. Bu başlıklar her istek mesajında vardır.

Via: SIP sunucusu, kendine gelen mesajı farklı bir birime yönlendirmeden önce Via başlık listesinin başına kendisini kaydeder. Bu bilgi sayesinde yanıt da ters yönde aynı yolu izleyecektir. Her Via başlığı, her hareket için tek olan bir dal parametresi içerir. Bütün dallar, "z9hG4bK" kodu ile başlar ve transaction kimliği olarak kabul edilir.

To ve From: ”To” ve “From” başlıkları, SIP isteğinin kaynağını ve gideceği hedef uç birimini gösterir. SIP Sunucuları arasında mesaj yönlendirilirken bu başlıklar hep sabit kalır.

Çağırma kimliği (ID): Bu değer tek bir tamsayı olarak düzenlenir ve istek ile ona bağlı yanıtın o çağırmaya özel olarak eşlenmesini sağlar.

Max-Yönlendirme: Bu başlık, bir yönlendirme hatası olması durumunda, SIP mesajının şebeke içerisinde devamlı bir döngü yaparak dönüp dolaşmasını engellemek içindir. Her SIP sunucusu mesajı aldığında sayaç 1 azalır. Sıfıra ulaştığında, kaynağa “483 Too Many Hops” mesajı iletir ve kurulumu iptal eder. Varsayılan değer 70’tir.

Cseq: Bir sayı dizisidir ve her yeni SIP isteği yaratıldığında 1 artırılır. İstek ve yanıtların eşleştirilmesinde kullanılır.

İçerik uzunluğu: Bulunduğu istek içerisinde hangi uzunlukta veri olduğunu belirtir.

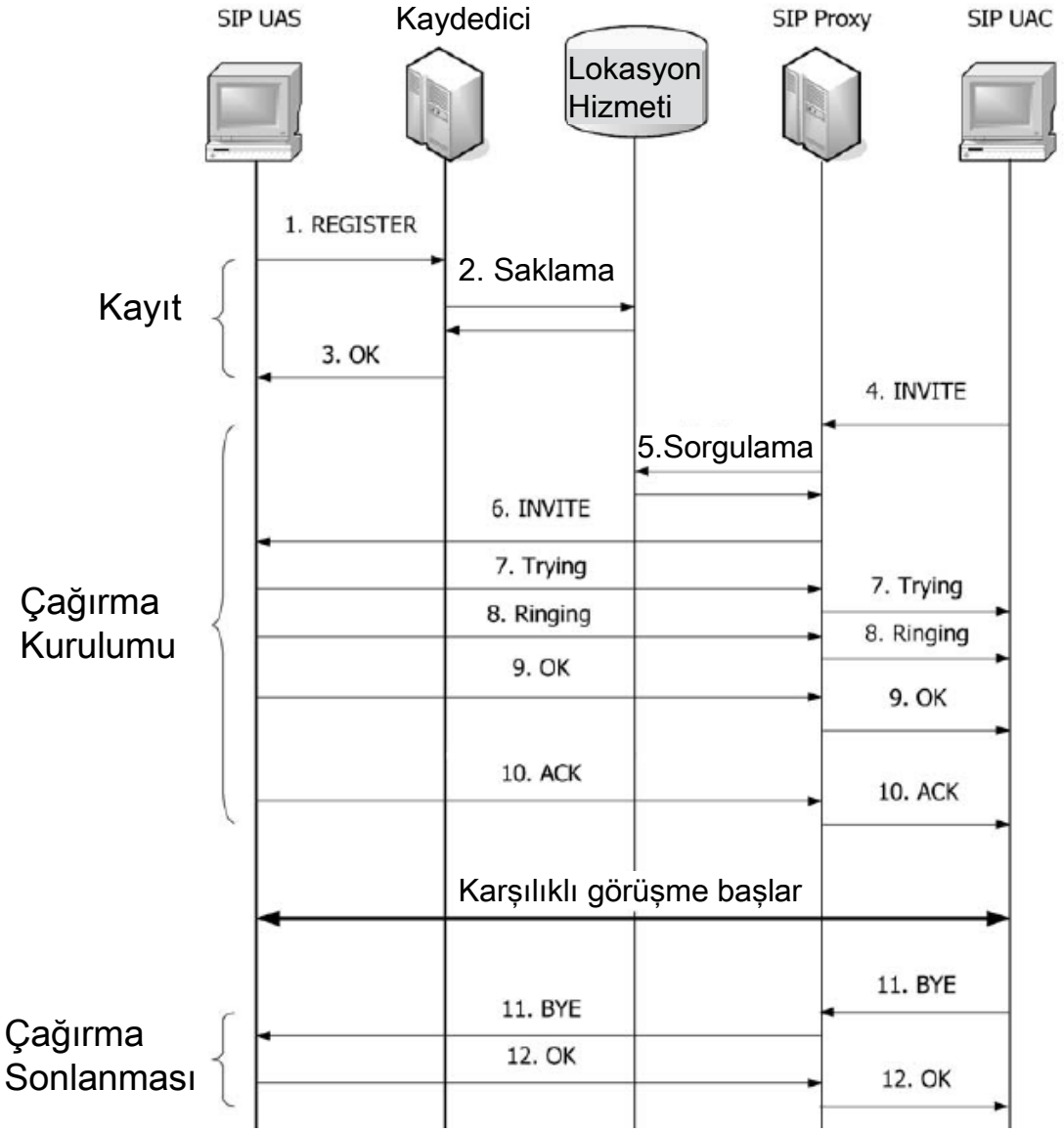
İçerik tipi: UMTS’te bir bağlantı kurulumu sırasında bu bilgi oturuma ilişkin SDP açıklamasıdır. Diğer SIP mesajları için mesajın tipine göre bu parameter değişebilir.

SIP İçeriği : Başlık kısmı boş bir satır ile bitirildikten sonra içerik kısmı başlar. SIP INVITE mesajının içerik kısmı, kurulması istenen oturuma ilişkin bilgileri (medya tipi-ses veya video, istenen veri hızı, RTP oturumu için port numarası) içerir. Bu parametreler 6.2.4 bölümünde incelenen SDP’de açıklandığı şekildedir.

6.2.3.9. SIP’te Kayıt, Çağırma Kurulumu ve Sonlandırılması

Bir SIP şebekesinde, UAC, UAS ve sunucular arasındaki işaretleşme Şekil 6.7’de verilmiştir. Sürece ilişkin tüm adımlar aşağıda açıklanmıştır:

1. Bir SIP UAS’ı aktif hale getirildiğinde, kendine ait SIP URI’sini kaydedici sunucuya REGISTER mesajı ile gönderir.
2. Kaydedici, bu bilgiyi (kullanıcı bilgisini) lokasyon hizmet veritabanına kaydeder.
3. Kaydedici, bir önceki adımı başarıyla tamamladığına dair 200 OK mesajını SIP UAS’a iletir.



Şekil 6.7 : SIP'te Kayıt, Çağırma Kurulumu ve Sonlandırılması

Bir SIP UAC'ın, bir SIP UAS'a çağırma talebi olduğunda aşağıdaki aşamalar gerçekleşir:

4. SIP UAC, bağlı olduğu proxy sunucusuna INVITE istek mesajı gönderir. Bu mesaj içerisinde UAS'ın SIP URI'si ve SIP UAC'a ait RTP bilgisini içeren SDP mesajı bulunur. RTP bilgisinde SIP UAC'a ait IP adresi ve port numarası bulunur.
5. Proxy sunucusu INVITE mesajı içindeki SIP URI'yi çözmek ve SIP UAS'ın kullanıcı bilgilerine ulaşmak amacıyla lokasyon hizmet veritabanından sorgulama yapar.
6. Proxy sunucusu SIP UAS'a INVITE mesajı iletir.

7. SIP UAS, INVITE mesajına karşılık 100 TRYING mesajını proxy sunucusuna çağırma kurulumu devam ediyor anlamında gönderir. Bu mesaj proxy sunucusu aracılığıyla SIP UAC'a iletilir.
8. SIP UAS kullanıcıya zil sesi çaldırır (çağırma geldiğine dair kendi UE'sini uyarmak için) ve aynı zamanda SIP UAC'a, SIP UAS'ın bağlı olduğu kullanıcının zil sesinin çaldığına dair 180 RINGING yanıtını gönderir. SIP UAC da kendi UE'sine karşı zil sesi tonu uyarısı iletir.
9. Aranan UE, çağırmayı kabul ettiği anda SIP UAS, proxy sunucu aracılığıya SIP UAC'a 200 OK yanıtını iletir. Bu mesaj içerisinde SIP UAS'a kullandığı IP adresi ve port numarasını da içeren SDP mesajı da vardır.
10. SIP UAC, OK mesajına karşı mesajı aldığına dair ACK bilgilendirme mesajını iletir ve çağırma kurulumu tamamlanır.

SIP UAS, SIP UAC'a RTP paketlerini INVITE mesajı içeriğine göre gönderir. SIP UAC da SIP UAS'a OK mesajı içeriğine göre RTP paketlerini iletir.

SIP UAC oturumu kapatmak istediğinde;

11. SIP UAC proxy sunucusu üzerinden BYE mesajını SIP UAS'a gönderir.
12. SIP UAS, onay amaçlı OK mesajını SIP UAC'a gönderir ve çağırma bu şekilde sonlandırılır.

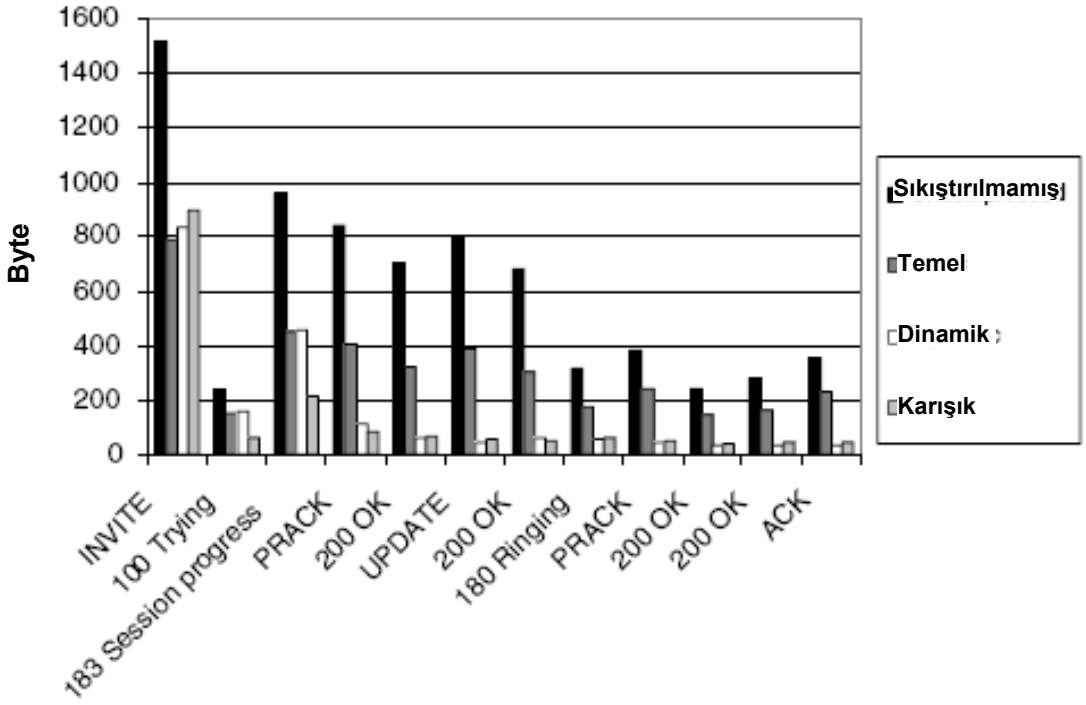
6.2.3.11. SIP Sıkıştırması

UMTS şebekesinde SIP ile IMS çağırma kurulumu, SIP için ayrılan bant genişliğinin az olması durumunda uzun sürebilir. Çağırma kurulum süresini kısaltmak için kullanılan bir yöntem işaretleşme işaretlerinin sıkıştırılması (Sigcomp) yöntemidir. Metin (text) bazlı protokollerde (Ör: SIP) sıkıştırma algoritmaları, RFC 3321 [85] tavsiyelerinde belirtilmiştir.

SigComp'un ana elemanı Genel Dekompressör Virtüel Cihaz'dır (UDVM). Bu birim sıkıştırmanın tersi (açma) için tasarlanmıştır. Sıkıştırılmış SIP mesajını alır, kullandığı algoritmaya göre açma işlemini yapar. Tavsiyelerde sıkıştırma algoritması belirlenmemiştir. UDVM şartlarına uygun sıkıştırma algoritmaları üreticiler tarafından kullanılabilir. SigComp'un en çok kullandığı algoritma, metin işleme sırasında, her tekrarlanan kavram veya sembol dizisi bir kod ile ifade edilir.

Sıkıştırmanın performansı, aynı kavram veya sembol dizisinden hangi oranda tekrarlandığıdır. SIP protokolünde kullanılan mesajlar sınırlı olduğundan ve tekrar tekrar kullanıldığından, bu basit sıkıştırma yöntemi kullanılabilir. Sıkıştırma için kullanılacak referans, sözlük olarak adlandırılır.

SigComp, performansını artırmak için SigComp Genişletilmiş Fonksiyonları (RFC 3485 Tavsiyesinde) kullanılabilir. Şekil 6.8.'de basit, dinamik ve karışık modlarda sıkıştırma yöntemi kullanıldığında, sıkıştırılmamış duruma göre mesaj bazında bayt hacminin ne kadar azaldığı verilmiştir.



Şekil 6.8 : SIP'te Sıkıştırmanın Etkisi

Dinamik sıkıştırma yönteminde, SIP sözlüğü ile birlikte iletilen bilgilendirme mesajları da sıkıştırmaya tabi olur. Karışık sıkıştırmada ise statik sözlük ile iletilen ve alınan bilgilendirme mesajları sıkıştırmaya tabi tutulur.

6.2.4. SDP - Oturum Açıklama Protokolü ve SDP İstek / Yanıt Modeli

Oturum Açıklama Protokolü (SDP), bir uygulama katmanı protokolü olup multimedya oturumlarının içeriğini tanımlamak amacıyla tasarlanmıştır. Bu alt bölümde, SDP ve SDP İstek / Yanıt Modeli incelenmiştir.

6.2.4.1. SDP Genel Özellikleri

SDP yazı tabanlı bir protokoldür. Bir oturumun tanımlanması; arayan ve aranan uç birimlerinin karşılıklı yeteneklerini, destekledikleri medya formatlarını ve mesaj kabul edecekleri adres / port numaralarını içeren bilgilerin iletimi anlamına gelir. Bu yetenekler, oturum kurulurken veya oturum başladıktan sonra iletişim sırasında karşılıklı iletilir. SDP spesifikasyonları, RFC2327 tavsiyesinde belirtilmiştir. SDP mesajları şu yapıya sahiptir:

1 karakterden oluşan ve bayrak (token) adı verilen bir birim, sonrasında gelen " = " işareti ve en sonda ise ilgili parametreleri içeren bir yapı vardır.

Ör: < karakter > = < diğer >

diğer : parametre1, parametre2, ... , parametreN

SDP mesajları, içerik olarak 3 ana sınıfa ayrılır:

- Oturum seviyesi açıklayıcısı: Oturum seviyesindeki parametreleri içerir. Bu parametrelere ilişkin gösterge ve SDP Açıklayıcı isimleri Tablo 6.1'de verilmiştir.
- Zamanlama Açıklayıcısı: Başlama ve bitiş zamanları, tekrarlama zamanlarını temsil eder.
- Medya Trafiği ve Formatı: İletim protokolü, port numarası ve Tablo 6.2'de verilen parametreleri içerir.

Bazı SDP satırları:

- Protokol versiyon satırı (v satırı): SDP protokol versiyonu " 0 (sıfır)" dır. SDP mesajlarının tümünde v = 0 .
- Bağlantı Bilgi Satırı (c satırı): Bu satır hem medya hem de oturum seviyesinde belirtilebilir. Oturum seviyesinde belirtilmemişse, medya seviyesinde mutlaka belirtilmelidir. Ör:

c = < şebeke tipi > < adres tipi > < şebeke adresi >

c = IN IPv4 128.5.6.7

Tablo 6.1 : Oturum Düzeyinde SDP Satırları

Alan	Açıklama	Vekil
v	Protokol versiyonu	m
o	Orijin ve oturum kimliği	m
s	Oturum ismi	m
u	Oturum URI'si	o
i	Oturum bilgisi	o
e	E-posta adresi	o
p	Telefon numarası	o
c	Bağlantı bilgisi	m
b	Bant genişliği bilgisi	m
z	Zaman dilimi doğrulaması	z
k	Şifreleme	o
a	Nitelik satırı	o

Tablo 6.2 : Medya Düzeyinde SDP Satırları

Alan	Açıklama	Vekil
i	Medya başlığı	o
c	Bağlantı bilgisi	o
b	Bant genişliği bilgisi	o
k	Şifreleme	o
a	Medya niteliği	o
m	Medya ve iletim	o

- Medya satırı (m satırı): Bu satır taşıma bilgileri de dahil olmak üzere medya içeriğine ilişkin bilgileri içerir. Ör:

m = < medya > < port > < taşıma > < format listesi (kodek tipi) >

m = video 51372 RTP / AVP 31

- Nitelik satırı (a satırı): Bu satır ise medyanın niteliğini belirtmek amacıyla kullanılır. Ör:

a = < nitelik alanı > [":" < nitelik değeri >]

a = rtpmap : 96 AMR → RTP Dinamik Ek yük tipinin belirlenmesinde kullanılabilir.

6.2.4.2. SDP ile İstek / Yanıt Modeli

SDP Teklif / Yanıt Modeli, iki uç birimi arasında medya özellikleri konusunda pazarlık yapmak ve fikir birliğine varmak amacıyla kullanılır. Örnek olarak hangi tür medya iletileceği, kodek tipi verilebilir. Teklifi yapan uç, ilk SDP teklifinde, kullanmak istediği medya özelliklerini yanıt verecek uca iletir. İçeriğinde, kaynak ucun kullanmak istediği medya tipi, kodek yapısı, yanıt almak istediği IP ve port numaraları bulunur. Hedef uç, bu isteğe kendi seçtiği ve destekleyebildiği özellikler ile yanıt verir. Bu yanıt içerisinde ise, teklif edilen medya türünün kabul edilip edilmediği, desteklenen kodek türü, mesaj alacağı IP adresi ve port numarası bulunur. Bu modelde, teklif eden uç bir teklif mesajı ilettikten sonra, kabul veya red yanıtı alıncaya kadar başka bir teklif yapamaz.

Faklı türden medya akımları için tür sayısı kadar "m" satırı teklif edilir. Desteklenmeyen bir tür için yanıt mesajında o tür satırı için "m = 0" yanıtı verilir. Bu sayede kaynak uç, hedef ucun desteklediği medya tipini öğrenir.

Bu model, oturum kurulumu sırasında oturum niteliğini oluşturmak veya önceden kurulmuş bir oturumun niteğini değiştirmek amacıyla kullanılır.

6.2.5. COPS - Genel Açık Denetim Hizmeti Protokolü

COPS protokolü, IETF tarafından RFC 2748 tavsiyesinde tanımlanmıştır. COPS, IMS sisteminde denetimin genel yönetiminden, uygulanmasından ve konfigürasyonundan sorumludur.

COPS, denetim sunucusu ile kullanıcı arasında denetim bilgisinin karşılıklı iletimi için oluşturulmuş sorgulama-yanıt protokolüdür. Kullanıcı, Denetim Zorlama Noktası (PEP, Policy Enforcement Point), sunucu ise Denetim Karar Noktası (PDP, Policy Decision Point) olarak adlandırılır. Bu sistemde PEP PDP'ye istek, güncelleme ve silme mesajlarını iletir. PDP'de verilen kararlar ise PEP'e yanıt olarak gönderilir. PEP de son aboneye PDP tarafından verilen kararları bildirir. UMTS R5'te PEP, GGSN'de konuşlanmıştır. GGSN, kullanıcı ile IMS sistemi arasındaki bağlantıyı sağlar. PDP ise IMS'teki P-CSCF'te bulunmaktadır. COPS protokolü, PDP ile PEP arasındaki güvenli iletişimi sağlamak amacıyla TCP protokolünü kullanır.

COPS mesajı, COPS başlığı ve hemen sonrasında gelen COPS nesnelerinden oluşur. Şekil 6.9'da COPS başlık formatı verilmiştir.

Şekil 6.9 : COPS Başlık Formatı

Versiyon: COPS versiyonunu belirtir. Varsayılan versiyon 1'dir.

Bayraklar: Belirli mesajları simgelemek için kullanılır. Sık kullanılan bir alan değildir.

OP Kodu : COPS işlemini belirten bölümdür. Örneğin, "1" değerline sahip REQ mesajı, PEP'in PDP'den karar verip kendisine bu kararı iletmesi amacıyla kullanılır.

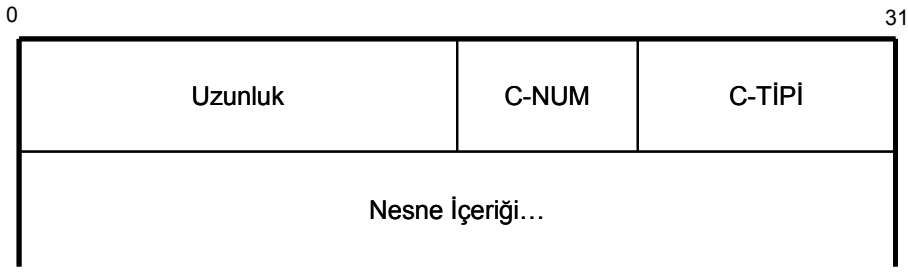
Alıcı (client) tipi : Alıcının ve COPS başlığından sonra gelen nesnelerin tanımlanması amacıyla kullanılır.

Mesaj uzunluğu : Mesajın oktet uzunluğunu belirtir.

COPS standardına özel nesnelerin formatı Şekil 6.10'da verilmiştir:

Uzunluk : Nesnelerin oktet uzunluğunu belirtir.

C-Num : Nesne içeriğindeki bilginin sınıfını belirtir.



Şekil 6.10 : COPS Nesne Formatı

C-Tipi : Nesne içerisindeki bilginin tipi veya versiyonunu göstermek amacıyla kullanılır.

Bir nesneye örnek olarak "karar" verilebilir. C-Num değeri 6 olan bu nesne "karar" olarak adlandırılır. Nesnenin içeriğinde, PDP tarafından verilen denetim kararı vardır.

6.2.6. Diameter

Diameter, RADIUS'un daha gelişmiş halidir. 3GPP, IMS'teki ücretlendirme fonksiyonları anlamında DIAMETER kullanımını tavsiye eder. RADIUS'tan farklı başlıca özelliği IPv6'yı desteklemesidir.

Diameter, temel bir peer-to-peer protokoldür ve AAA uygulamalarının oluşturulmasında kullanılır. Bu temel protokol, iki uç arasında nitelik değer çiftlerinin (AVP) ve ücretlendirme fonksiyonu bilgilerinin karşılıklı iletimini düzenler.

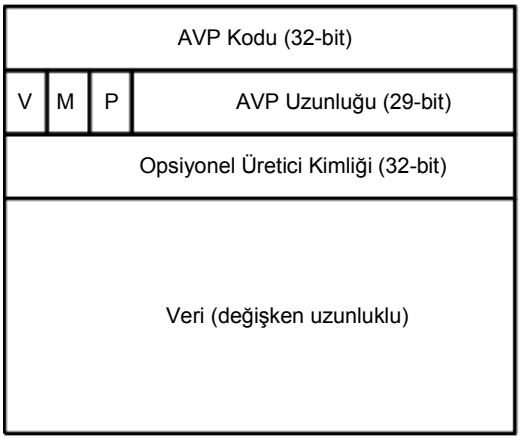
Her AVP, nitelik açıklayıcısı ve ona ilişkin değeri içeren bir veri bütününden oluşur. Şekil 6.11'de AVP formatı verilmiştir.

AVP kodu, üretici kimliği ile birlikte değerlendirilerek tek olan AVP niteliğini oluşturur. Bu sayede üreticiler kendilerine özgü AVP'lerini oluşturma imkanına sahip olurlar. Üretici kimlik bölümü opsiyoneldir.

V biti 1 ise bu opsiyon değerlendirmeye alınır.

M (zorunlu) biti, yapılmış bir istek için AVP'in desteklenmesini zorunlu kılar. Bir uç, M biti 1 olan AVP içerikli bir Diameter mesajı alırsa ve bu AVP'yi tanıyamazsa, isteği reddeder.

P (gizlilik) biti, Diameter mesajının iki uç arasında şifrelenerek iletileceğini gösterir.



Şekil 6.11 : AVP Mesaj Formatı

SIP için kullanılan bazı AVP adları aşağıdadır:

SIP-AOR (Kayıt Adresi) : Kamusal kullanıcı kimliğini temsil eder.

SIP-Server-URI : İlgili S-CSCF'i temsil eder.

SIP-Auth-Data-Item : Doğrulama verisini temsil eder.

Diameter, sonuç olarak IMS'te doğrulama, yetkilendirme ve ücretlendirme bilgilerinin iki şebeke elemanı arasında iletimini düzenleyen bir protokoldür.

6.2.7. IMS'te Kayıt İşlemi

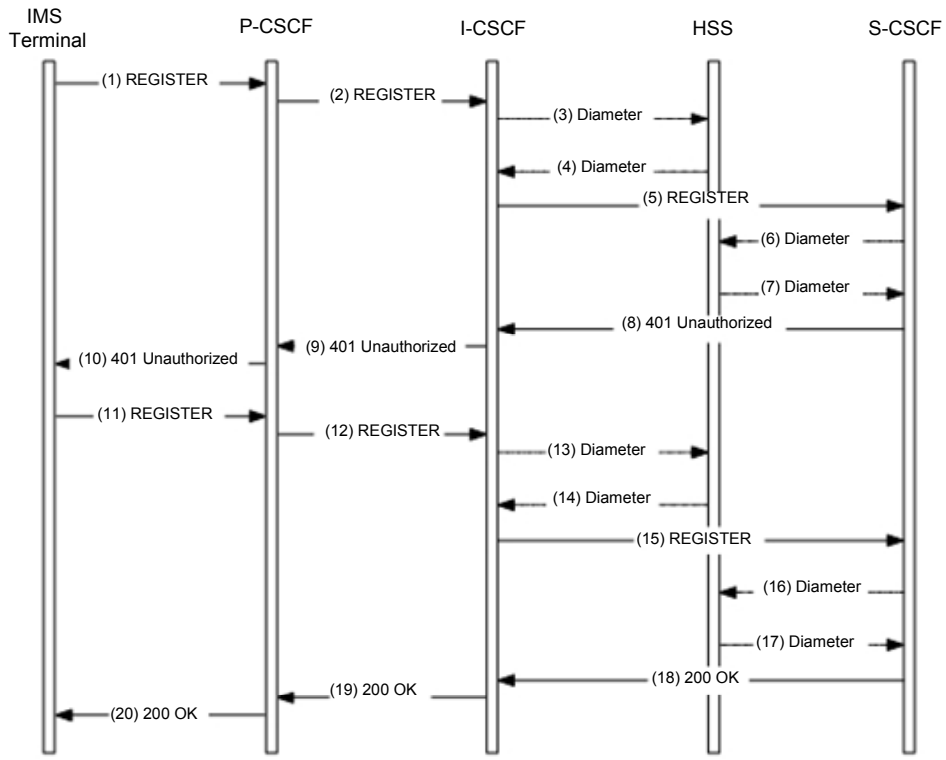
Bir UMTS şebeke abonesi, IMS sisteminden hizmet almadan önce, bağlı bulunduğu S-CSCF'e kaydolmalıdır. Bu sayede dış şebekelere MS tarafından çağırma kurulması istendiğinde veya MS'te sonlandırılan çağırmalarda, S-CSCF'in MS'in adresini bilmesi sağlanır ve çağırmalar sağlıklı iletilmiş olur. Kayıt işlemi sırasında MS'in doğrulama işlemi de yapılır.

Bir kullanıcı IMS'e kaydolduğunda, o kullanıcıya bir S-CSCF atanır. Bu S-CSCF kullanıcının kaydedici sunucusu olur. Kullanıcı S-CSCF'e kaydolduktan sonra, kullanıcının profilini HSS'ten elde eder. Bu sayede kullanıcının kriterlerine göre uygun AS ile iletişime geçer.

IMS kayıt prosedürü aşağıda adım adım verilmiştir:

1. IMS terminali, REGISTER istek mesajını bağlı olduğu P-CSCF'e iletir. Bu istekteki URI, kullanıcının lokal domenindeki kaydedicisinin adresidir. Bu

istek ayrıca kullanıcının kamu ve özel kimliklerini, dış IMS şebekesinin ve lokal şebekenin IP adreslerini de içerir.



Şekil 6.12 : IMS'te Kayıt İşlemi

2. P-CSCF, bu isteğe dış IMS şebekeleri için kullanılacak kimliği de ekleyerek I-CSCF'e gönderir.
3. I-CSCF, isteği S-CSCF'e göndermekle sorumludur. Fakat öncesinde, HSS ile iletişime geçerek kullanıcının IMS'e erişim yetkisinin olup olmadığını kontrol eder. Bu mesajlaşmada I-CSCF, HSS'e kullanıcının kimlik bilgilerini HSS'e gönderir ve daha önceden kullanıcı kayıtlı ise HSS'ten kullanıcının kayıtlı olduğu S-CSCF adresi I-CSCF'e gönderilir. IMS terminali kayıtlı değil ise (bu akış örneğinde kayıtlı değildir) ilgili S-CSCF'e de kayıt isteği I-CSCF tarafından gönderilir.
4. S-CSCF HSS'ten kullanıcı ile ilgili bilgleri alır ve kaydedici olarak davranır. Kullanıcı bilgilerinin doğruluğunu sorgulamak amacıyla 401 UNAUTHORIZED mesajını I-CSCF ve P-CSCF üzerinden IMS terminaline iletir.

5. IMS terminali, kendi kimlik bilgilerini ve ihtiyaç duyulan cevabı (gerekli şifreler) hazırlar ve yeni bir REGISTER mesajı ile S-CSCF'e iletir.
6. S-CSCF, IMS terminalinden gelen bilgiler ile kendinde bulunan abone bilgilerini kontrol eder ve HSS'e bilgilerin doğru olduğunu iletir.
7. S-CSCF aynı zamanda IMS terminaline kayıt işleminin tamamlandığını 200 OK mesajı ile aynı yol üzerinden iletir.

6.2.8. IMS'te Oturum Kurulumu

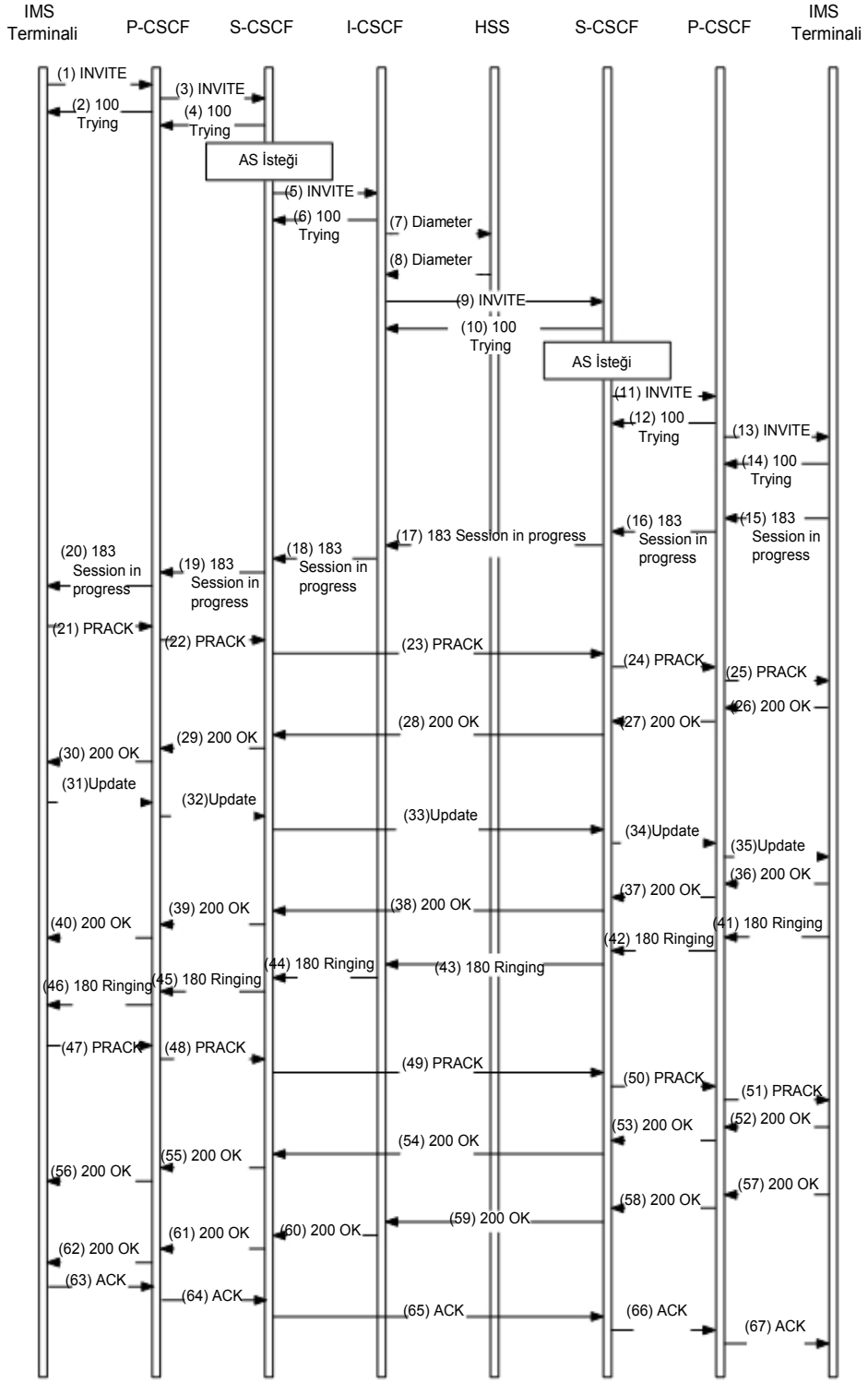
MS, IMS çağırması başlatmadan önce kendi UMTS şebekesi içerisinde IMS mesajlarını iletecek PDP Bağlantı kurulumunu GPRS şebekesinde gerçekleştirir. Bu kurulum sırasında GGSN, P-CSCF'e ait IP adresini (DNS veya farklı bir metodla elde eder) alır ve PDP Bağlantı yanıtında (GGSN'den UE'ye gelen) P-CSCF'e ait IP adresi de bulunur. Bu şekilde UE ile IMS arasındaki arabağdaşım tamamlanmış olur.

Şekil 6.13'te bir MS tarafından başlatılan ve diğer bir operatöre ait MS'te sonlanan bir çağırmanın kurulumu aşamalı olarak aşağıda verilmiştir:

UMTS operatör abonesi, SIP INVITE mesajı oluşturur ve GGSN üzerinden UMTS operatörüne bağlı IMS'teki (lokal IMS) P-CSCF'e iletir. MS'in kayıtlı olduğu S-CSCF'e bu mesaj iletilir. S-CSCF, abonenin hizmet profilini kontrol eder ve kullanıcının filtre kriterinden geçip geçmediğine karar verir ve I-CSCF'e INVITE mesajı gönderir. I-CSCF, HSS'ten aranan kişinin bilgilerini ve bağlı bulunduğu S-CSCF'i sorgular. I-CSCF diğer mobil şebekeye bağlı I-CSCF üzerinden S-CSCF'e SIP INVITE mesajını iletir. S-CSCF aranan kişinin kullanıcı filtre kriterine uygun olup olmadığını kontrol eder ve INVITE mesajını aranan UE'nin bağlı olduğu P-CSCF'e iletir.P-CSCF de GGSN üzerinden GPRS çekirdek şebeke aracılığıyla aranan UE'ye iletir. SIP INVITE mesajını alan UE, desteklediği Kodek tipini belirtir ve ilgili SDP'yi içeren 183 Session In Progress mesajını ters yönde bilgilendirme amacıyla gönderir. Bu sırada aranan MS, kendi erişim şebekesinde ilgili kaynak rezervasyon işlemini gerçekleştirir. Bu mesajı alan kaynak MS de kendi erişim şebekesinde ilgili kaynak rezervasyon işlemlerini yürütür. Bu işlemleri tamamlayan hedef uç, SIP Update mesajını aynı yolla iletir.

SIP update mesajını alan hedef uç, kendi kaynak rezervasyonu işlemlerini tamamladıysa, bu uçta telefon zili çalmaya başlar ve çaldığına dair bilgi RINGING

mesajı ile arayana iletilir. Aranan kişi çağırmayı kabul ettiğinde, arayan kişiye 200 OK mesajı gönderilir ve bilgilendirme amacıyla ACK mesajı ters yönde iletilir.



Şekil 6.13 : IMS'te Oturum Kurulumu

Bu sayede oturum kurulmuş olur. Bilgilendirme amacıyla kullanılan 183 Session In Progress ve 180 RINGING mesajlarının güvenilirliği anlamında ters yönde PRACK mesajı ile yanıt verilir.

Dış şebekeden gelen ve MS tarafından sonlandırılan çağırmalarda, dış IMS şebekelere arabağdaşım olan I-CSCF üzerinden lokal IMS şebekesine mesaj gelir ve MS tarafından başlatılan çağırma süreci ters yönde aynı şekilde yapılır.

6.2.9. IMS Güvenliği

Güvenlik, haberleşme sistemlerinin sağlaması gereken en önemli unsurlardan biridir. Güvenlik denince akla ilk olarak şifreleme gelir. Şifreleme, önemli bir özellik olmasına karşın tek başına yeterli değildir. Entegre koruma, kullanıcı doğrulaması, şifre yönetimi ve güvenlik protokolleri gibi kavramlar da güvenliğin sağlanmasında önemli rol oynarlar.

Operatörlerin kendi şebekelerini ve kullanıcı trafiğini en iyi şekilde korumaları beklenir. Güvenlik anlamında da, diğer alanlarda olduğu gibi standartizasyon vardır. 3GPP modelinde, erişim ve çekirdek şebeke elemanlarının birbirleri ile iletişimlerinde önceden tanımlanmış güvenlik protokollerine göre hareket etmesi ve olası bir saldırının önceden sezilerek tehdit oluşturmasının engellenmesi benimsenmiştir. Bir UMTS şebekesinde radyo erişim şebekesi ve operatör ile dış dünya bağlantısının sağlandığı arabağdaşım en büyük tehlikenin gelebileceği noktalardır. Operatör, çekirdek şebekesi yönünden fiziksel olarak iyi korunmuş bir yapıya sahiptir.

IMS hizmetlerine erişim için öncelikle kayıt işlemi sırasında yapılan yetkilendirme ve doğrulama işlemi IMS Doğrulama ve Şifre İşbirliği (AKA, Authentication and Key Agreement) ile UMTS çekirdek şebekesindeki doğrulama algoritmasına benzer şekilde yapılır. AKA, kullanıcı ile IMS arasında paylaşılan şifreleri de sağlar. IMS ile P-CSCF arasındaki SIP işaretleşmesini korumak için bu şifreler kullanılır. Doğrulama işlemi her zaman MS'in bağlı olduğu lokal IMS şebekesinde yapılır. MS dolaşım yapsa dahi doğrulama işlemleri hep lokal IMS'te gerçekleştirilir. Güvenlik ile ilgili aşağıda bazı kavramlar açıklanmıştır:

Doğrulama işlemi, MS'te bulunan ISIM ile HSS arasında yapılır. UMTS'teki doğrulama algoritmasının aynen uygulanmasına karşın kullanılan kimlik verileri ile gizli şifreler farklıdır. Bu kapsamda aşağıdaki kavramlar tanımlanmıştır:

IM Kamu Kimliği (IMPU): Aboneye çağırmaların yönlendirilmesi amacıyla kullanılan SIP adresidir.

IM Özel Kimliği (IMPI): UMTS şebeke içerisinde kayıt, kabul ve ücretlendirme amacıyla kullanılan kimliktir. SIP çağırmalarının yönlendirilmesinde etkisi yoktur.

IM Hizmet Kimlik Modülü (ISIM): IMS'te yürütülen güvenlik fonksiyonları için kullanılan kimlik bilgilerini taşıyan modüldür.

Özel Şifre: ISIM ile HSS arasında doğrulama işlemi için kullanılan şifre modülüdür.

IMPU, IMPI ve Özel Şifre ISIM içerisinde bulunur ve modifiye edilemezler.

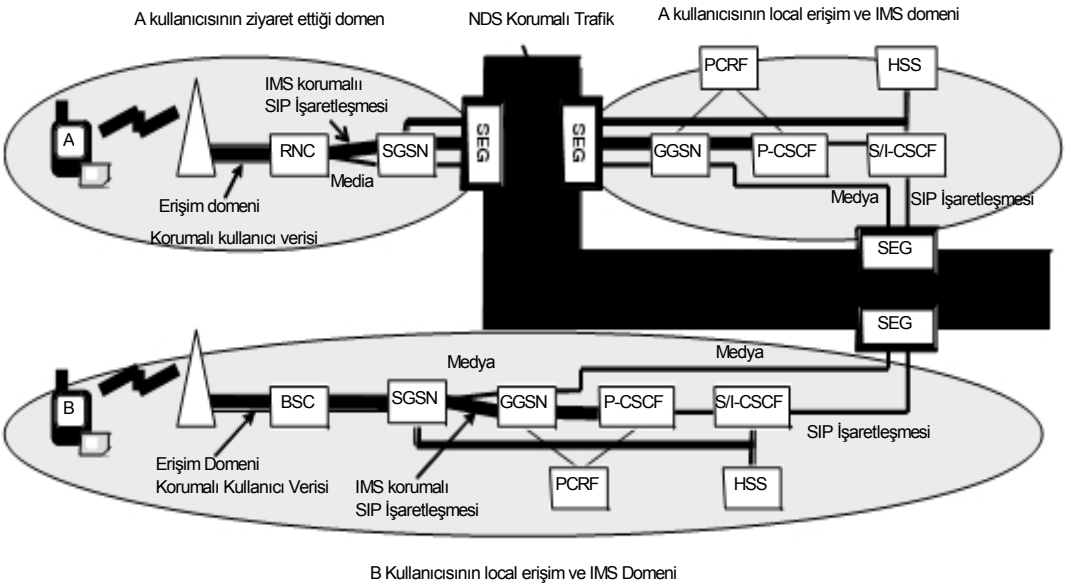
ISIM, IMS şebekesindeki kimliği, USIM ise UMTS şebekedeki (Radyo Erişim) kimliği belirtir. Genel Entegre Devre Kartı (UICC, Universal Integrated Circuit Card) her iki kimliği de barındırır. IMS şebekesinde erişim için ISIM tercih edilir fakat geriye dönük sistemleri desteklemesi amacıyla USIM'in de geçerli olması kararlaştırılmıştır. Şekil 6.14'te UMTS şebekesinde IMS güvenliğinin nasıl sağlandığı belirtilmiştir.

Farklı operatörler arasında SIP işaretleşmesinin yapıldığı birimler Güvenlik Geçitleri (SEG, Security Gateway) olarak adlandırılmıştır. Şebeke elemanları arasındaki bağlantılarda kullanılan genel güvenlik protokolü IPSec'dir. SEG'ler arasındaki güvenlik, tünel modda ESP ile sağlanır. Bunların dışındaki bağlantılarda ise normal modda ESP ile güvenlik sağlanır. IMS ile MS arasnda güvenlik sağlanan bağlantılar kalın çizgilerle belirtilmiştir. IMS'te her bir kullanıcıya bir Özel Kullanıcı Kimliği tahsis edilir. Bu kimliğe bağlı bir veya daha çok kullanıcı kimliği tanımlanabilir. Her bir genel kullanıcı kimliği, SIP URI formatındadır ve SIP mesajlarının yönlendirilmesinde kullanılır.

HSS'te kullanıcıya ait tüm bilgiler (Özel kullanıcı kimliği, genel kullanıcı kimliği, şifreler, hizmet profilleri, vs.) barındırılır. Bir özel kimliğe birden çok genel kimlik bağlanması, kullanıcının birden çok terminalden herbiri için ayrı ayrı abonelik yaptırmadan IMS şebeksine bağlanabilmesi anlamına gelir.

Bir IMS kullanıcısının IMS kayıt işleyişinde aynı zamanda doğrulama işlemi de yapılır. IMS'te kayıt alt bölümünde gösterilmeyen IMS doğrulama işlemi adım adım Şekil 6.15'te verilmiştir.

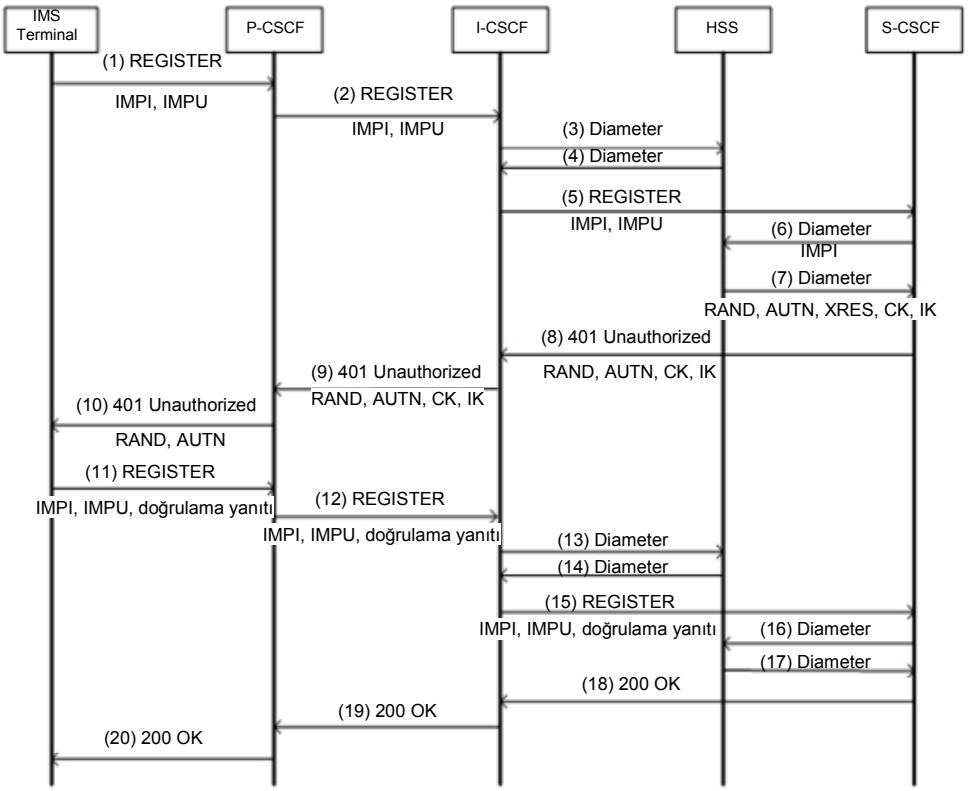
MS, REGISTER isteğini P-CSCF'e iletir. Bu mesaj içeriğinde Genel Kullanıcı Kimliği (IMPU) ve Özel Kullanıcı Kimliği (IMPI) bulunur.



Şekil 6.14 : UMTS R5'te IMS Güvenliği

Bu bilgilerin iletiminde, UMTS sisteminin radyo erişim şebekesindeki güvenlik mekanizmaları kullanılır. S-CSCF HSS'ten doğrulama vektörü (AV) ister. Bu vektör kullanıcının IPMI ve IMPU bilgilerini içerir. HSS, doğrulama bilgisi (AUTN, RAND, XRES, IK ve CK) ile dönüş yapar. AUTN bilgisi, HSS'i UE'ye doğrulatmak için kullanılır. RAND değeri ise doğruluğu sorgulamak için kullanılır ve XRES yanıtı beklenir. CK ve IK şifreleme ve entegrasyon şifreleridir. Bu bilgi alışverişi sonrasında RAND, AUTN, CK ve IK bilgilerinin içeren SIP 401 UNAUTHORIZED mesajı UE'ye iletilir. UE bu bilgiler ışığında oluşturduğu yanıtı (İçeriğinde IMPI, IMPU ve AUTN yanıtı var) aynı yol üzerinden yeni bir REGISTER mesajı oluşturarak S-CSCF'e gönderir.

S-CSCF'den UE'ye gönderilen bilgilerden IK ve CK, P-CSCF'ten UE'ye iletilirken çıkarılır. Bunun nedeni P-CSCF ile UE arasındaki SIP işaretleşmesinde, entegrasyon kontrolü için bu parametrelerin kullanılmasıdır. CK ve IK, UE'ye gelen AUTN ile UE'nin oluşturduğu şifrelerdir. Bilgileri kontrol eden S-CSCF, UE'ye 200 OK mesajı göndererek doğrulamayı tamamlar, aynı zamanda HSS'i de UE'nin kayıt statüsünün değişikliği konusunda bilgilendirir.



Şekil 6.15 : IMS'te Doğrulama İşlemi

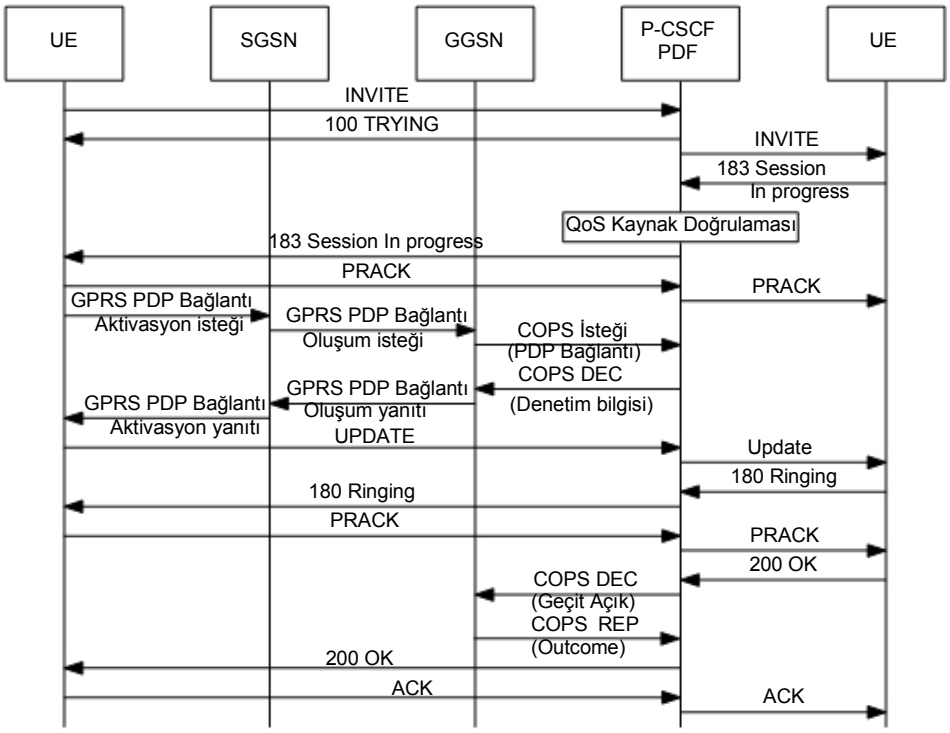
6.2.10. IMS Sisteminde QoS

UMTS R5'ten önceki sürümlerde, uygulama katmanı pazarlıkları anlamında mobil şebekeler, UE ile sunucu arasında sadece iletim görevi görür. R5 ile birlikte UMTS'e bağlı IMS sistemi sayesinde mobil operatörler, bu katmandaki uygulamalara ilişkin doğrulama, yetkilendirme, kontrol, ücretlendirme gibi işlemleri yapabilme yeteneğine kavuşmuşlardır. Bu amaçla şebekeye yeni elemanlar katılmıştır. IMS'in kalite anlamında getirdiği bir diğer yenilik, yeni servislerin operatörler tarafından yaratılmasına ve varolanların geliştirilmesine olanak tanımasıdır.

Bir IMS çağırmasında QoS rezervasyonu 2 kritere göre yapılır. Bunlar kaynaklar ve denetimdir. Kaynak kriteri, şebekede çağırma kabul edecek kapasiteye sahip şebeke elemanları olup olmadığı ile ilişkilidir. UMTS şebekesinde kaynak kontrolü erişim şebekesinde RNC tarafından yapılır. GPRS çekirdek şebekesinde bu işlem SGSN tarafından yürütülür. Denetim kararında ise IMS tarafında PDF birimi sorumludur. PDF, genellikle P-CSCF ile aynı lokasyonda bulunur.

QoS kontrolü 3 aşamadan oluşur:

- QoS kaynaklarının P-CSCF'te yetkilendirilmesi
- Kaynak Rezervasyonu (UE'de)
- QoS'un onaylanması



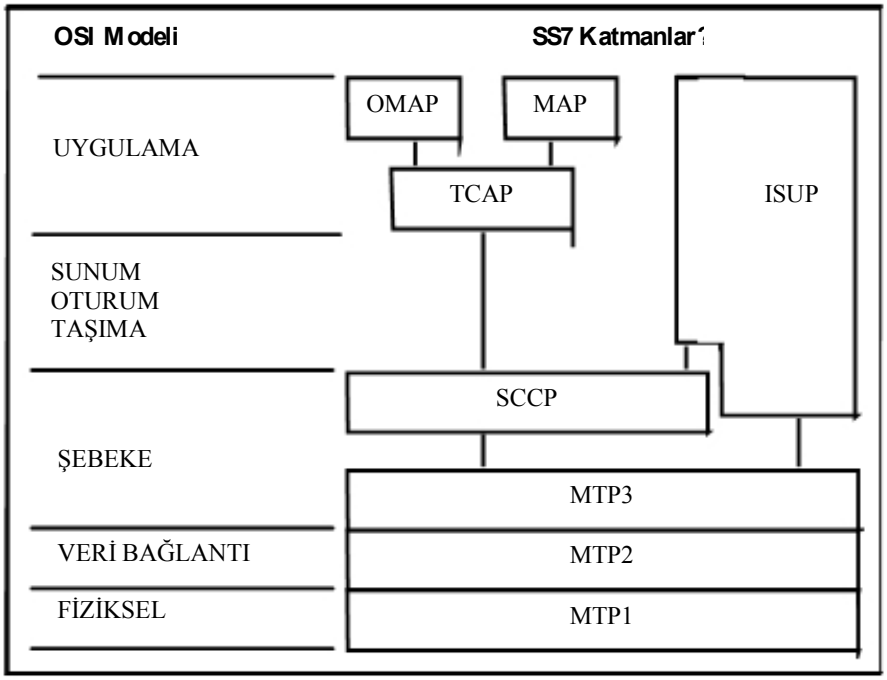
Şekil 6.16 : IMS'te Oturum QoS Kurulumu

İlk adım, P-CSCF tarafından ilk 183 Session In Progress mesajı alındığında başlar. Bu aşamada şebekenin IMS tarafında kodek ve bant genişliği tahsisi için fikir birliğine varılır ve PDF tarafından IMS şebekede yeterli kaynak olup olmadığı kararı verilir. Kaynaklar o çağırma için rezerve edildikten sonra UE'ye In Progress mesajı iletilir. Sonrasında UE tarafında kaynak rezervasyonu işlemi başlar. SIP yanıtının SDP kısmında belirtilen bant genişliği ihtiyacı UE tarafından PDP Bağlantı istek oluşumunda kullanılır. Bu istek UE'den SGSN'e, ardından GGSN'e iletilir. GGSN, bu aşamada PDP Bağlantı kurulumuna izin verip vermeyeceğini sorgulamak için P-CSCF üzerinden PDF'e COPS REQ mesajı gönderir. PDF hangi SIP çağırmasının QoS'u için istek yapıldığını yetkilendirme bayrağı (token) sayesinde bilir. Bu değer her çağırma için tektir ve P-CSCF tarafından üretilir. Bu değeri INVITE mesajı veya UE'de biten 183 Session In Progress mesajı içerisine gömer. Denetim bilgisi elde edilir ve PDP Bağlantı kurulumu yapılıp yapılmayacağına karar verilir. GGSN, bu kararı SGSN üzerinden UE'ye iletir. Aynı zamanda GGSN, PDF'e de kurulumu

kabul ettiğine dair COPS REP mesajı gönderir. Normal çağırma prosedürü sonunda hedef uçtan P-CSCF'e 200 OK mesajı gelir ve sonrasında PDF GGSN'e COPS DEC mesajı göndererek kaynak rezervasyon doğrulaması yapar. Bu aşamada GGSN 2 alt şebeke (UMTS çekirdek şebekesi ve IMS şebekesi) arasında trafik akışını düzenler. Bu işleme geçit açılması (open gate) denir. Yetkilendirme bayrağı (Token), PDP Bağlantı ile SIP çağırmasını arasındaki bağlantıyı sağlamada kullanılır.

6.3. SIGTRAN - İşaretleşme İletimi

İşaretleşme iletim protokolü (Sigtran), IETF tarafından RFC 2719 tavsiyesinde tanımlanmış bir protokoldür. Amacı, SS7 tabanlı işaretlerin (işaretleşme işaretlerinin) IP tabanlı şebeke üzerinden iletimini sağlamaktır. UMTS R4 ile çekirdek şebekede, şebeke katmanında IP tabanlı iletim mümkün olmuştur. UMTS çekirdek şebeke yapısının bir özelliği olarak işaretleşme işaretleri SS7 tabanlı işaretlerdir. Bu nedenle, SS7 işaretlerinin Sigtran protokolü ile şebeke elemanları arasında IP tabanlı iletimi sağlanır. Örneğin, MSC sunucuları arasındaki ve HLR – MSCS arasındaki BICC mesajlarının iletimi için Sigtran kullanılır.



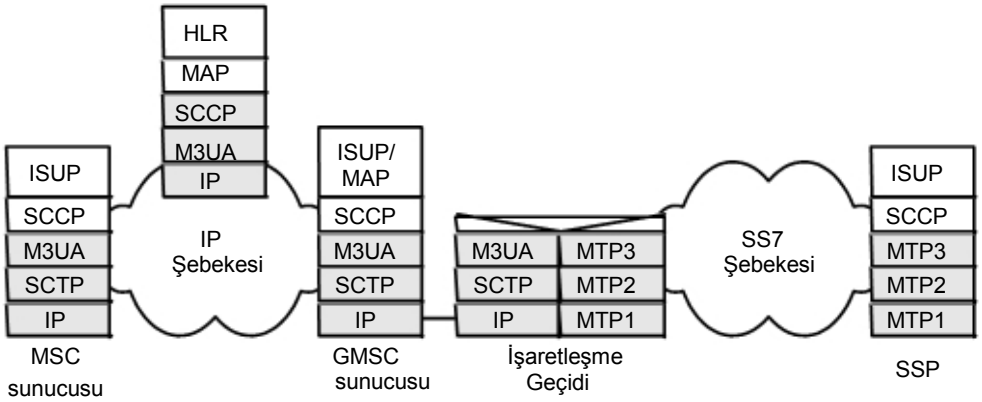
Şekil 6.17 : SS7 Paket Formatı

Bir SS7 şebekesinde, protokol yığını Şekil 6.17'deki gibidir. Bu yapıda mesaj iletim kısmı (MTP1, MTP2 ve MTP3) katmanları kullanılır. Bir üst katmanda işaretleşme

bağlantı kontrol kısmı (SCCP) bulunur. En üst katmanda ise ISDN kullanıcı kısmı (ISUP) bulunur.

Sigtran'da, SS7 işaretlerinin IP şebekede iletime uygun hale gelebilmesi için 2 katman tanımlanmıştır. Bunlar, MTP kullanıcı adaptasyon katmanı (MU3A) ve akım kontrol iletim protokolü (SCTP) katmanıdır. Bir ISDN şebekesinin UMTS şebekeye bağlandığı arabağdaşım ve UMTS şebekedeki MSCS'ler arasındaki işaretleşmeye ilişkin protokol yığını Şekil 6.18'de verilmiştir.

Sigtran, SCCP katmanının alt katmanlarında MTP mi yoksa IP şebeke mi kullanıldığını ayırt etmemesi üzerine tasarlanmıştır.



Şekil 6.18 : SS7 Şebekesi ile IP Şebekesi Arasında İşaretleşme İşaretlerinin İletimi

6.3.1. MU3A Yapısı

Bu protokol RFC 3332 tavsiyesinde tanımlanmıştır. SS7 şebekesinde MTP-3 katmanındaki fonksiyonlara benzer fonksiyonlar yürütür. Görevi, IP şebekede bulunan SS7 uygulama sunucuları (Ör: MSCS, HLR) ve dış SS7 şebeke elemanları arasında iletişimi sağlamaktır.

SS7 adreslemesi ile IP adreslemesi tamamen farklıdır. Mesajların yönlendirilmesinde, MU3A katman protokolü uygulanır.

6.3.2. SCTP Yapısı

SCTP, RFC 2960 tavsiyesinde tanımlanıştır. TCP ve UDP, taşıma katmanında genel olarak kullanılan protokoller olmalarına rağmen, SS7 işaretlerinin iletimini sağlayamamıştır. SCTP'nin oluşumunun ana nedeni budur ve SS7 işaretlerinin IP şebeke içerisinde iletiminden sorumludur TCP protokolüne benzer şekilde, veri

aktarımı başlamadan önce çağırma kurulumunun yapılmasına ihtiyaç duyar. SCTP, TCP bilgi güvenli bir bağlantı sağlar.

TCP'de bağlantı yönelimli, güvenilir, sıralı iletim ve yığılma kontrolü yapılır. İletilen veri bayt akımı olarak tanınır. TCP'nin mesajları tanıma veya mesajların sınırlarını bilme gibi bir yeteneği yoktur. SS7'de her mesajın tanınarak ayrı ayrı iletilmesi gereksinimi vardır. TCP'de olmayan özellik budur. TCP'de 1 bayt kaybolursa, tekrar iletim oluncaya kadar o akım bekletilir. SCTP'de ise kaybolan baytın bağlı olduğu mesaj bekletilir, diğer mesajlar bu nedenle herhangi bir gecikmeye uğramazlar.

SCTP, SS7 işaretlerinin güvenilir ve sağlam bir şebeke üzerinden iletimi için "çok-lokasyonlu" olarak adlandırılan bir özellik tanımlamıştır. Buna göre oturum başlatma fazında, her iki uç birimi de kendilerine ulaşılabilecek IP adreslerinin listesini karşılıklı iletirler. Normal şartlarda, ilk verilen IP adresi geçerlidir. Bu özellik sadece birden çok IP adresine ve arabağdaşıma sahip uç birimleri (host) için geçerlidir.

SCTP, TCP gibi hız dengeleme mekanizmasına sahiptir. Bu sayede şebekedeki yük koşullarına göre veri iletim hızını artırıp azaltabilir.

SCTP, içerisinde barındırdığı doğrulama etiketi sayesinde, paketi gönderen uçtan emin olur. Güvenlik için bu hizmete ek olarak IPSec'den de yararlanılır. SCTP'ye ait genel başlık Şekil 6.19'da verilmiştir.

Kaynak Port Numarası: SS7 işaretini oluşturan kaynak ucun port numarasıdır.

Hedef Port Numarası: SS7 işaretinin varacağı hedef ucun port numarasıdır.

Doğrulama etiketi: SCTP paketlerini gönderen ucun doğrulanması için kullanılır.

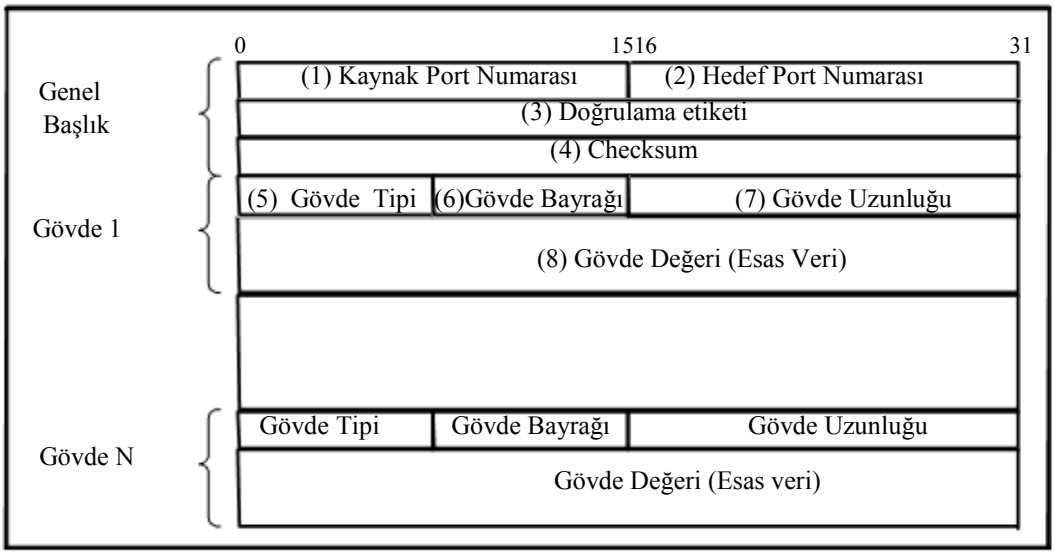
Checksum: SCTP paketlerinin entegrasyonunu sağlamak amacıyla kullanılır.

Gövde (Chunk): SCTP paketinin esas kısmına gövde denir. Bir SCTP paketinin son bölümünde bir veya birden fazla gövde bulunur. Her gövde 3 alt bölümden oluşur:

Gövde tipi: Gövde değeri alt bölümündeki verinin tipini belirtir.

Gövde Uzunluğu: Gövdenin uzunluğunu belirtir.

Gövde Değeri: SCTP mesajı içerisinde iletilecek ana mesajı taşıyan alt bölümdür.



Şekil 6.19 : SCTP Paket Formatı

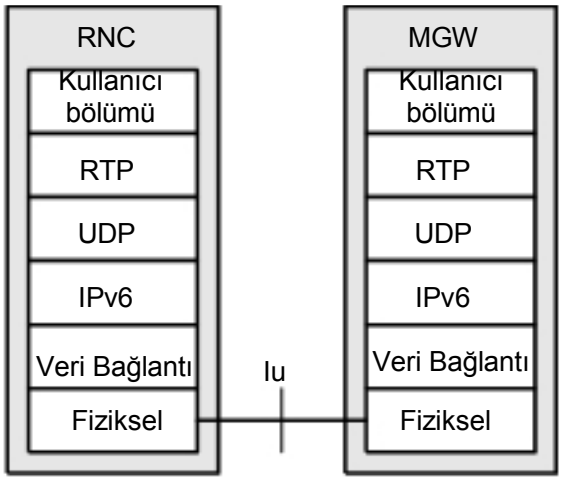
6.4. UMTS Radyo Erişim Şebekesi'nde IP

UMTS R5 ile şebekeye gelen yeni bir özellik IP'nin UTRAN'da şebeke katmanında kullanılabilmesidir. Bu özellik ile birlikte uçtan uca tamamen IP tabanlı iletim sağlanır. R5'ten önceki versiyonlarda, ATM tabanlı iletim yapılır. Fiziksel katman ve veri bağlantı katmanı ATM ile sağlanmaya devam edilebilir. Mevcut çalışan ve yeni kurulacak mobil şebekeler için IP'nin UTRAN'da kullanılması esneklik getirir. Yeni operatörler için IP'ye uygun herhangi bir veri bağlantı katmanı kullanılabilme imkanı oluşur. Mevcut işleyen şebekesi olan operatörler ise ATM yapısını değiştirmeden, bazı güncellemeler ile IP kullanımına elverişli hale getirilebilir.

UTRAN'da IP'de sadece IPv6 desteklenir. Daha önceki sürümlerin desteklenmesi amacıyla çift yığın (dual stack) kullanılır ve IPv4 ile IPv6'nın her ikisi de desteklenir.

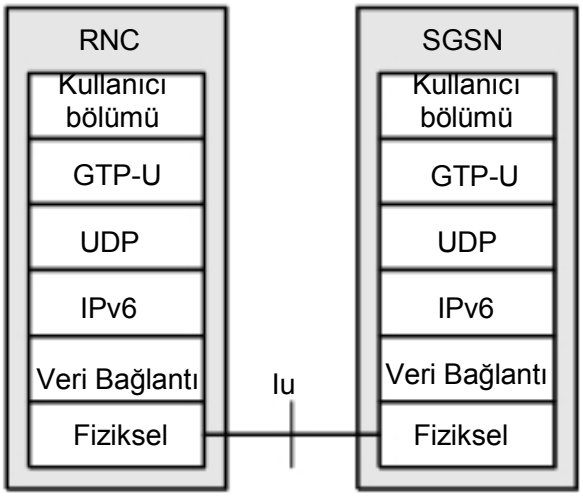
6.4.1. Iu Arabağdaşımında IP

IP'nin UTRAN'da Iu arabağdaşımında kullanımı, ITU'nun TS25.414 tavsiyesinde belirtilmiştir. RNC ile MGW arasındaki Iu-CS domenine (kullanıcı düzlemi için) ilişkin protokol yığını Şekil 6.20'de verilmiştir. Her RTP ek yükü, bir kullanıcı düzlemi (UP) PDU'su içerir. UP seviyesinde yürütülen zamanlama fonksiyonu nedeniyle RTP'deki zamanlama fonksiyonu gereksizdir.



Şekil 6.20 : RNC ile MGW Arasında Kullanıcı Düzleminde Iu-CS Protokol Yığını

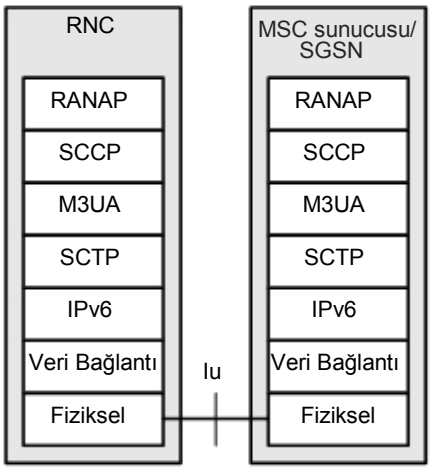
Iu-PS domeninde ise kullanıcı düzlemi için Şekil 6.21'deki protokol yığını kullanılır. PS domeninde RTP yerine GTP protokolü kullanılır ve kullanıcı düzlemi olduğundan GTP-U seçilir. UDP protokolünün ek yükü GTP-U paketleridir.



Şekil 6.21 : RNC ile MGW Arasında Kullanıcı Düzleminde Iu-PS Protokol Yığını

Kontrol düzleminde ise her iki arabağdaşım için (Iu-CS ve Iu-PS) Şekil 6.22'deki protokol yığını kullanılır.

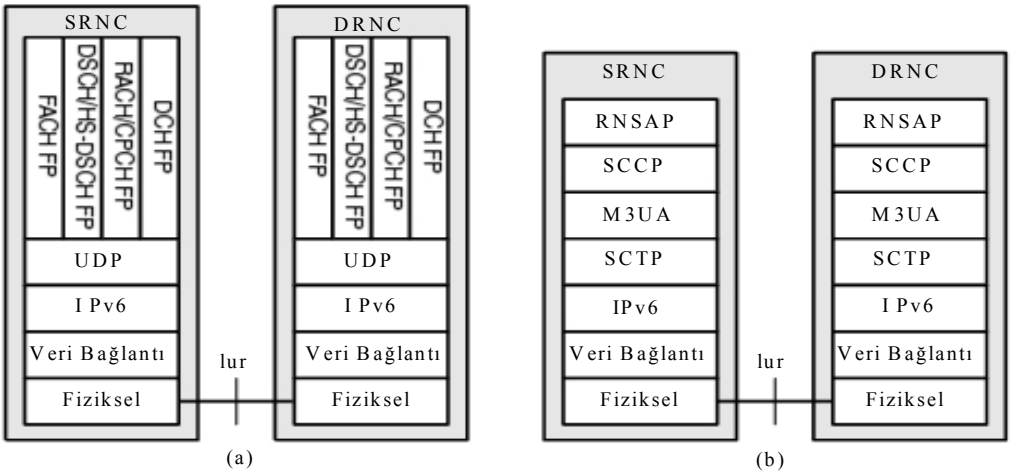
RANAP, SS7 uygulama protokolü olması nedeniyle, IP tabanlı şebekede iletimine imkan sağlayan Sigtran protokolü sayesinde iletilir. SIGTRAN içerisinde tanımlanan M3UA ve SCTP protokolleri, SS7 işaretlerinin IP tabanlı şebeke üzerinden taşınmasını sağlar.



Şekil 6.22 : Kontrol Düzlemi için Iu Protokol Yığını

6.4.1.1. Iur Arabağdaşımında IP

RAN içerisinde iki RNC arasında kullanılan Iur arabağdaşımında, R5 ile birlikte IP tabanlı iletim olanaklı hale gelmiştir. Şekil 6.23'te kaynak ve hedef RNC'ler arasındaki protokol yığını verilmiştir. İki RNC arasındaki kontrol düzlemi işaretleri,



Şekil 6.23 : Iur Arabağdaşımına İlişkin Protokol Yığını

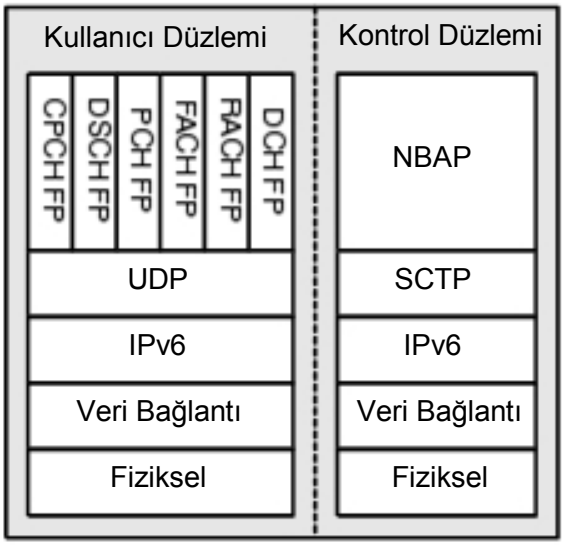
(a) Kullanıcı Düzlemi (b) Kontrol Düzlemi

RNSAP protokolü ile taşınır. RNSAP da RANAP gibi SS7 tabanlı bir protokol olduğundan, iletiminde Sigtran kullanılır.

6.4.1.2. Iub Arabağdaşımında IP

Iub arabağdaşımı, Node B ile RNC arasındaki iletişimi sağlar. Şekil 6.24'te Iub protokol yığını verilmiştir. Iub, kullanıcı düzlemi düşünüldüğünde, Iur arabağdaşımı ile aynı protokol yığınına sahiptir.

BTS kontrol işaretleşmesini tanımlayan Node B uygulama kısmı (NBAP) mesajları, SCTP protokolü üzerinde direk yerleştirilerek iletilir. NBAP mesajlarında IP adresleri ve UDP portları karşılıklı iletilir.



Şekil 6.24 : Iub Arabağdaşımına ilişkin Protokol Yığını

6.5. IP-ATM Uyumlu Çalışması

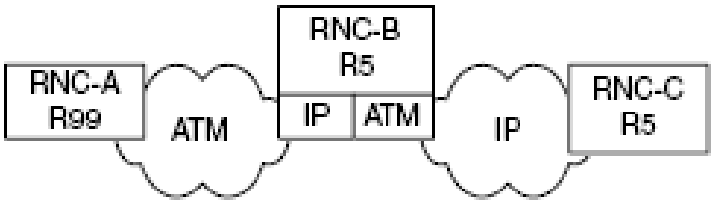
UMTS R99'dan R5'e ve dolayısıyla Tüm-IP yapısına geçişte, uyumlu çalışma (interoperability) kavramı ortaya çıkmıştır. Örneğin, sadece ATM'yi destekleyen UTRAN Node B'si ile sadece IP'yi destekleyen R5 Node B'sinin uyumlu çalışması verilebilir. Bunu sağlamak için geliştirilmiş 2 yöntem vardır:

- Uyumlu çalışma birimi ile iki sistem arasındaki karşılıklı çeviri yöntemi
- Çift yığın yöntemi

Çift yığın yönteminde, şebeke elemanı her iki sistemi de destekleyecek bir yapıya sahiptir. Bu sayede farklı altyapı özellikleri bulunan şebeke elemanlarından gelen veri doğru olarak işlenir. Iub arabağdaşımı düşünüldüğünde, çift yığın yöntemi efektif bir çözümdür. Bunun nedeni, farklı Node B'lerin ortak tek bir RNC'ye

bağlanmasıdır. Bu durumda RNC'de çift yığın özelliği olması, tüm Node B'leri destekleyebileceği anlamına gelir. Örneğin bir R99 Node B'si ile R5 Node B'si aynı RNC'ye bağlı olsun. R99 Node B'si için ATM destekleyen protokol yığını, R5 Node B'si için ise IP destekleyen protokol yığını kullanılır ve şebeke aksamadan işler.

Iur arabağdaşımı için çift yığın yöntemi uygun değildir. Bunun nedeni Şekil 6.25'teki örnek ile açıklanmıştır. Bu örnekte, RNC-B çift yığın özelliğine sahiptir ve hem ATM, hem de IP tabanlı sistemleri desteklemektedir.



Şekil 6.25 : ATM-IP Çalışması İçin Çift Yığın Yöntemi

RNC-A ve RNC-C, RNC-B ile sorunsuz iletişim kurabilmektedir. Fakat RNC-A, RNC-C ile iletişime geçmek istediğinde, bu mümkün olmayacaktır. Buna neden olan faktör, RNC-B'nin diğer iki RNC'ye sadece bağlanırlık (connectivity) hizmeti sağlamasıdır. RNC-A'dan RNC-C'ye gitmesi hedeflenen işaret, RNC-B'de sonlanacağından bağlantı reddedilir. RNC-B, farklı iki şebeke arasında mesajları yönlendirebilme özelliğine sahip değildir. Sadece bağlanırlık özelliği vardır. RNC-A ile RNC-C'nin iletişim kurmasına olanak tanıyacak yapı, Uyumlu Çalışma Birimi'ni (IWU) şebekeye dahil etmektir. IWU, protokol çevirisi yapma yeteneğine sahiptir ve her iki domenden gelen mesajların diğer domende iletilmesini sağlar. Her iki sistemin adresleme yapısı farklıdır. Bu nedenle SS7 kod noktaları, tüm şebekede global adresleme yöntemi olarak kullanılır. IWU'nun görev alanı adresleme ile sınırlı olmayıp, taşıyıcı kurulumu prosedüründe de rolü vardır.

7. SONUÇLAR

Mobil telekomünikasyon, günümüzde standart iletişim sistemlerinden biri haline gelmiştir. Konumdan ve zamandan bağımsız olarak her an ve her yerde iletişim kurabilme olanağı, insanlara cazip gelmiş ve mobil iletişim araçlarını daha da artan bir oranda kullanmalarını teşvik etmiştir. Öte yandan, iletim teknolojilerinde, IP'nin ağırlığı gün geçtikçe artmakta ve buna bağlı olarak IP tabanlı uygulamalar sürekli gelişmektedir. Bir mobil iletişim sistemi olan UMTS de bu gelişmelere kayıtsız kalmamış, taşıma teknolojisi yönünden bir değişim sürecine girmiştir. UMTS şebekesi, iletim teknolojisi olarak ATM tabanlı iletimden IP tabanlı iletime doğru bir yönelim göstermektedir.

Bir şebeke katmanı protokolü olan IP, OSI katmanlı mimarisinde kendisinden alt ve üst seviyedeki katman yapılarından olabildiğince bağımsız bir iletim protokolü olarak tasarlanmıştır. Bu kavramı en kısa ve öz ifade eden cümle, "Her Şey IP üzerinden, IP Her Şey Üzerinden" (Everything over IP, IP over Everything) olmuştur. IP, veri iletimi anlamında bant genişliğini en verimli kullanan iletim protokolleri arasındadır. Diğer yönden, gerçek zamanlı ses / video aktarımı konusunda diğer standartlara göre (Ör: ATM) gelişmesinin gerekli olduğu kanısı hakimdir. Son dönemde, bu zaafı minimize edecek standart geliştirme çalışmaları yoğunlaştırılmıştır. Buna paralel olarak, uçtan uca tamamen IP tabanlı şebekelerin oluşumuna yönelik çalışmalar da yürütülmektedir. UMTS şebekesinde de bu gelişmeler doğrultusunda belirli zaman aralıklarıyla farklı sürümler oluşturulmuştur. "UMTS R3" ile başlayan ilk sürümde, IP'nin şebeke içerisindeki kullanım alanı EDGE'den çok farklı olmamıştır. Sadece radyo erişim şebekesinde yapılan değişiklikler ile veri iletim hızında artış ve bant genişliğinin verimli kullanımı sağlanmıştır. Bir sonraki sürüm olan "UMTS R4" ile birlikte IP, sadece UMTS çekirdek şebekesinin paket bağlaşma domeninde değil, devre bağlaşma domeni içerisinde oluşturulan alt bir bölümde (paket bağlaşmalı) kullanılabilir hale gelmiştir. Bir sonraki sürüm (UMTS R5) ile birlikte, hem çekirdek şebekede, hem de radyo erişim şebekesinde tamamen IP tabanlı iletime elverişli bir yapı oluşturulmuştur. Bu

sürümde bir diğer yeni gelişme, UMTS şebekesi içerisinde yeni bir alt şebeke olan IP Multimedya Alt Sistemi'dir (IMS). IMS, mobil operatörlere, servis sağlayıcılarına ve içerik sağlayıcılarına çok esnek hizmetler sunma olanağı tanımıştır. IMS'in buna ek olarak sağladığı hizmetler; IP uygulamalarının belirli bir standarda kavuşması, mobil abonelerin daha esnek ve zengin içeriklere sahip uygulamalar kullanabilmesine olanak tanıması ve en önemlisi TÜM-IP yapısına geçişte önemli bir adım olmasıdır.

Mevcut GSM ve UMTS şebekeleri, ağırlıklı olarak ATM tabanlı iletim yapmaktadır. IP tabanlı iletim, UMTS şebekesinin sadece paket bağlaşmalı domeninin bir bölümünde geçerlidir. Tamamen IP tabanlı iletime geçiş, aniden yapılabilecek bir değişim değildir. Hali hazırdaki sistemleri destekleyen şebeke elemanlarının ve uç birimlerinin, aşamalı olarak değişime uğrayacağı tahmin edilmektedir. Bu olay bir süreci ifade eder. İlk aşamada, hem mevcut hem de planlanan sistemlerde destekleyici düzenlemeler yapılması; ikinci aşamada, adım adım Tüm-IP'ye uygun yapıya geçilmesi planlanmaktadır.

İletim teknolojisi standartlarındaki gelişmeler, sadece IP alanında değil, diğer alanlarda da yaşanmaktadır. UMTS sistemi baz alındığında, genel olarak ATM, TDM ve IP tabanlı iletim standartları benimsenmektedir. Tezde yapılan araştırmalar sonucunda, IP'nin diğer standartlara göre gelecekte daha avantajlı olacağı ve yakın geleceğin genel iletim standardı olacağı kanısına varılmıştır.

KAYNAKLAR

[1] **Wilesly Dave, ve Eardley Philip, ve Burness Louise**, 2002. IP For 3G, John Wiley and Sons, İngiltere.

[2] **Bannister, J. ve Mather, P. ve Coope, S. ,** 2004. Convergence Technologies For 3G Neworks, John Wiley and Sons, İngiltere.

[3] **Prof. Dr. Günsel DURUSOY**, TCP / IP Protokolleri, Ders Notları.

[4] **Chakraborty, S. ve Frankkila, T. ve Peisa, J. ve Synnergren, P.** , 2007. IMS Multimedya Telephony over Cellular Systems, John Wiley and Sons, İngiltere.

[5] **Nielsen, T. T. ve Jacobsen, R. H.** , 2005, Opportunities for IP in Communications Beyond 3G, *Springer*, Danimarka, **33**, 243-259.

[6] **Ibe, Oliver C.** , 2002. Converged Network Architectures, John Wiley and Sons, New York.

[7] **Gomez, G. ve Sanchez, R. ,** 2005. End-To-End Quality of Service Over Cellular Networks, John Wiley and Sons, İngiltere.

[8] **Prof. Dr. Günsel DURUSOY**, Telsiz Haberleşme Teknolojileri, Ders Notları.

[9] **Soldani, D. ve Li, M. ve Cuny, R.** , 2006. QoS and QoE Management in UMTS Cellular Systems, John Wiley and Sons, İngiltere.

[10] **Poikselka, M. ve Mayer, G. ve Khartabil, H. ve Niemi, A.** , 2006. The IMS, John Wiley and Sons, İngiltere.

[11] **Widegren, I.** , 2000. Architectural Principles (3GPP All-IP Wokshop - ERICSSON).

[12] **Ollikainen, H.** , 2004. IP in UMTS Networks (Sunum).

[13] **Griffoul, F. ve Hartenstein, H. ve Jonas, K. ve Pokorski, W. ve Schaller, S.** , The All-IP Option: Architecture and Migration Path, Workshop - Migrating to Mobility.

[14] **Nortel Networks**, 2003. Mobil IP & IPv6 in 3G UMTS / cdma2000 Mobil Networks, Nortel Networks.

[15] **Hanrahan, H.** , 2007. Network Convergence, John Wiley and Sons, İngiltere.

[16] **Hongyan, C. ve Yunlong, C. ve Ying, W. ve Ping, Z.** , 2005, Design and Implementation Of All IP Architecture For Beyond 3G System, IEEE, s. 667-671.

[17] **Smith, L. Ve Krob, J. Ve Schwefel H.** , 2001. IP Technology in 3.rd Generation Mobile Networks, Siemens AG. (Tutorial).

[18] **Bos, L. , 2004**. Fixed Mobile Convergence, Alcatel (Sunum).

[19] **Tabbane, S.** , 2005. Mobile Network Evolution Towards New Generation Networks, Tunus (sunum).

[20] WCDMA Protocols and Procedures (Öğrenci Kitabı), 2005. Ericsson, İsveç.

[21] **Wei, Q. Ve Su, S. Ve Chen, J.** , 2003. Study on Application of Softswitch in Wireless Networks, Beijing Üniversitesi, Çin, s. 127-130.

[22] **Petrak, L. Ve Hoene, C. Ve Carle, G.** , 2006, UMTS Networks, Tübingen Üniversitesi (sunum).

[23] Chuah**, M. C. Ve Medepalli, K. ve Park, Se-Yong ve Wang, J.** , 2002. Quality of Service in Third-Generation IP-Based Radio Access Networks, Wiley Interscience, s. 67-89.

[24] **Bahgat, T.** , 2006. Step to IMS, Step To Future, ZTE (sunum).

[25] **Lin, Yi-Bing and Pang, Ai-Chun,** 2005. Wireless and Mobil ALL-IP Networks, Wiley Publishing Inc., Hindistan.

[26] **Etoh, M.** , 2005. Next Generation Mobil Systems 3G and Beyond, John Wiley and Sons, İngiltere.

[27] **TS 29.414,** 2001. CN Nb Data Transport and Transport Signalling, 3GPP, France.

[28] **TR 23.981,** 2005. Interworking aspects and migration scenarios of IPv4 based IMS implementation, 3GPP.

[29] **TS 29.232,** 2005. Media Gateway – Media Gateway Controller Interface, 3GPP.

[30] **RFC 2865,** 2000, Remote Authentication Dial In User Service, IETF.

[31] **RFC 2210**, 1997. The Use of RSVP with the IETF Integrated Services, IETF.

[32] **RFC 1889**, 1996. Real Time Protocol, IETF.

[33] **RFC 3261**, 2002. Session Inıtiation Protocol, IETF.

[34] **RFC 3321[85]**, 2003. Signalling Compression, IETF.

[35] **RFC 3485**, 2003. SIP and SDP Static Dictionary for SigComp, IETF.

[36] **RFC 2327**, 1998. Session Description Protocol, IETF.

[37] **RFC 2748**, 2000. Common Open Policy Service, IETF.

[38] **RFC 2719**, 1999. Signalling Transport, IETF.

[39] **RFC 3332**, 2002. SS7 MTP3-MU3A, IETF.

[40] **RFC 2960**, 2000. SCTP, IETF.

ÖZGEÇMİŞ

Nuran DEMİRCİ, 16 Temmuz 1982 yılında İstanbul'da doğdu. İlk, orta ve lise öğrenimini İstanbul'da tamamladı. 2004 yılında İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Elektronik ve Haberleşme Mühendisliği programından mezun oldu. Aynı yıl içerisinde İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Telekomünikasyon Mühendisliği Yüksek Lisans programında yüksek lisans eğitimine başladı. Eğitimine 1 yıl ara vererek vatani görevini tamamladı. 2006 yılı içerisinde görev yapmaya başladığı TURKCELL İletişim Hizmetleri A.Ş. 'de halen Hücre Planlama ve Optimizasyon bölümünde görev yapmaktadır. İlgilendiği konular hücresel mobil sistemlerin radyo erişim şebekeleri ve çekirdek şebekeleridir.