

Second Edition

Mobile Computing

Technology, Applications and Service Creation



**ASOKE K TALUKDER
HASAN AHMED
ROOPA R YAVAGAL**





Tata McGraw Hill

Published by Tata McGraw Hill Education Private Limited,
7 West Patel Nagar, New Delhi 110 008.

Copyright © 2010, by Tata McGraw Hill Education Private Limited.

No part of this publication may be reproduced or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise or stored in a database or retrieval system without the prior written permission of the publishers. The program listings (if any) may be entered, stored and executed in a computer system, but they may not be reproduced for publication.

This edition can be exported from India only by the publishers,
Tata McGraw Hill Education Private Limited.

ISBN (13): 978-0-07-014457-6

ISBN (10): 0-07-014457-5

Vice President and Managing Director—Asia-Pacific Region: *Ajay Shukla*

Executive Publisher: *R Chandra Sekhar*

Manager—Production: *Sohan Gaur*

Manager—Sales & Marketing: *S. Girish*

Deputy Marketing Manager—Science, Technology and Computing: *Rekha Dhyani*

General Manager—Production: *Rajender P Ghansela*

Asst. General Manager—Production: *B L Dogra*

Information contained in this work has been obtained by Tata McGraw-Hill, from sources believed to be reliable. However, neither Tata McGraw-Hill nor its authors guarantee the accuracy or completeness of any information published herein, and neither Tata McGraw-Hill nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information. This work is published with the understanding that Tata McGraw-Hill and its authors are supplying information but are not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought.

Typeset at Bukprint India, B-180A, Guru Nanak Pura, Laxmi Nagar, Delhi 110 092 and printed at
Pashupati Printers Pvt. Ltd., 1/429/16, Gali No. 1, Friends Colony, Industrial Area, G.T. Road, Shahdara, Delhi 110 095

Cover Printer: SDR Printers

Cover Designer: Kapil Gupta

RBZLCRQZDRCCD

The McGraw-Hill Companies

Copyrighted material

Contents

<i>Preface to the Second Edition</i>	vii
<i>Preface to the First Edition</i>	xiii
<i>Acknowledgements</i>	xix
<i>List of Abbreviations</i>	xxix

1. Introduction

1.1 Mobility of Bits and Bytes	1
1.2 Wireless-The Beginning	2
1.3 Mobile Computing	5
1.4 Dialogue Control	9
1.5 Networks	9
1.6 Middleware and Gateways	10
1.7 Application and Services (Contents)	11
1.8 Developing Mobile Computing Applications	16
1.9 Security in Mobile Computing	18
1.10 Standards-Why are they Necessary?	18
1.11 Standards Bodies	19
1.12 Players in the Wireless Space	24
<i>References/Further Reading</i>	25
<i>Review Questions</i>	26

2. Mobile Computing Architecture

2.1 History of Computers	28
2.2 History of Internet	29
2.3 Internet-The Ubiquitous Network	30
2.4 Architecture for Mobile Computing	31
2.5 Three-tier Architecture	32
2.6 Design Considerations for Mobile Computing	41
2.7 Mobile Computing through Internet	54
2.8 Making Existing Applications Mobile-enabled	55
<i>References/Further Reading</i>	56
<i>Review Questions</i>	56

3. Mobile Computing through Telephony

3.1 Evolution of Telephony	58
3.2 Multiple Access Procedures	60

3.3 Satellite Communication Systems	63
3.4 Mobile Computing through Telephone	66
3.5 Developing an IVR Application	71
3.6 Voice XML	75
3.7 Telephony Application Programming Interface (TAPI)	81
3.8 Computer Supported Telecommunications Applications	82
<i>References/Further Reading</i>	82
<i>Review Questions</i>	83
4. Emerging Technologies	84
4.1 Introduction	84
4.2 Bluetooth	84
4.3 Radio Frequency Identification (RFID)	89
4.4 Wireless Broadband (WiMAX)	91
4.5 Mobile IP	95
4.6 Internet Protocol Version 6 (IPV6)	103
4.7 Java Card	111
<i>References/Further Reading</i>	114
<i>Review Questions</i>	115
5. Global System for Mobile Communications (GSM)	116
5.1 Global System for Mobile Communications	116
5.2 GSM Architecture	118
5.3 GSM Entities	119
5.4 Call Routing in GSM	124
5.5 PLMN Interfaces	128
5.6 GSM Addresses and Identifiers	129
5.7 Network Aspects in GSM	130
5.8 Mobility Management	131
5.9 GSM Frequency Allocation	138
5.10 Personal Communications Service	139
5.11 Authentication and Security	140
<i>References/Further Reading</i>	143
<i>Review Questions</i>	144
6. Short Message Service (SMS)	145
6.1 Mobile Computing Over SMS	145
6.2 Short Message Service (SMS)	145
6.3 Value Added Services through SMS	151
6.4 Accessing the SMS Bearer	154
<i>References/Further Reading</i>	171
<i>Review Questions</i>	172
7. General Packet Radio Service (GPRS)	174
7.1 Introduction	174

7.2 GPRS and Packet Data Network	174
7.3 GPRS Network Architecture	175
7.4 GPRS Network Operations	181
7.5 Data Services in GPRS	185
7.6 Applications for GPRS	187
7.7 Limitations of GPRS	188
7.8 Billing and Charging in GPRS	189
7.9 Enhanced Data Rates for GSM Evolution (EDGE)	190
<i>References/Further Reading</i>	192
<i>Review Questions</i>	192
8. Wireless Application Protocol (WAP)	194
8.1 Introduction	194
8.2 WAP	196
8.3 MMS	206
8.4 GPRS Applications	213
<i>References/Further Reading</i>	215
<i>Review Questions</i>	216
9. CDMA and 3G	218
9.1 Introduction	218
9.2 Spread-Spectrum Technology	219
9.3 IS-95	226
9.4 CDMA versus GSM	235
9.5 Wireless Data	236
9.6 Third Generation Networks	238
9.7 Applications on 3G	243
<i>References/Further Reading</i>	249
<i>Review Questions</i>	250
10. Wireless LAN	251
10.1 Introduction	251
10.2 Wireless LAN Advantages	251
10.3 IEEE 802.11 Standards	254
10.4 Wireless LAN Architecture	256
10.5 Mobility in Wireless LAN	267
10.6 Deploying Wireless LAN	268
10.7 Mobile Ad hoc Networks and Sensor Networks	272
10.8 Wireless LAN Security	274
10.9 Wireless Access in Vehicular Environment	279
10.10 Wireless Local Loop	280
10.11 HiperLAN	281
10.12 WIFI versus 3G	283
<i>References/Further Reading</i>	284
<i>Review Questions</i>	285

11. Intelligent Networks and Interworking	287
11.1 Introduction	287
11.2 Fundamentals of Call Processing	287
11.3 Intelligence in the Networks	289
11.4 SS#7 Signaling	291
11.5 IN Conceptual Model (INCM)	300
11.6 Softswitch	304
11.7 Programmable Networks	305
11.8 Technologies and Interfaces for IN	305
11.9 SS7 Security	307
11.10 MAPSec	307
11.11 Virtual Private Network (VPN)	307
<i>References/Further Reading</i>	310
<i>Review Questions</i>	311
12. Client Programming	312
12.1 Introduction	312
12.2 Moving Beyond the Desktop	312
12.3 A Peek Under the Hood: Hardware Overview	315
12.4 Mobile Phones	316
12.5 Features of Mobile Phone	317
12.6 PDA	319
12.7 Design Constraints in Applications for Handheld Devices	321
12.8 Recent Developments in Client Technologies	323
<i>References/Further Reading</i>	325
<i>Review Questions</i>	326
13. Programming for the Palm OS	327
13.1 Introduction	327
13.2 History of Palm OS	327
13.3 Palm OS Architecture	329
13.4 Application Development	334
13.5 Communication in Palm OS	344
13.6 Multimedia	350
13.7 Enhancements in the Current Release	354
13.8 Latest in Palm OS	355
<i>References/Further Reading</i>	356
<i>Review Questions</i>	356
14. Wireless Devices with Symbian OS	358
14.1 Introduction to Symbian OS	358
14.2 Symbian OS Architecture	360
14.3 Applications for Symbian	363
14.4 Controls and Compound Controls	378

14.5 Active Objects	380
14.6 Localization	381
14.7 Security on the Symbian OS	382
14.8 Latest in Symbian	383
<i>References/Further Reading</i>	386
<i>Review Questions</i>	386
15. J2ME	388
15.1 JAVA in the Handset	388
15.2 The Three-Prong Approach to JAVA Everywhere	389
15.3 Java 2 Micro Edition (J2ME) Technology	392
15.4 Programming for CLDC	397
15.5 GUI in MIDP	405
15.6 UI Design Issues	425
15.7 Multimedia	425
15.8 Record Management System	428
15.9 Communication in MIDP	440
15.10 Security Considerations in MIDP	448
15.11 Optional Packages	450
15.12 Mobile Related JSR	451
15.13 Latest in J2ME	459
15.14 Conclusion	460
<i>References/Further Reading</i>	460
<i>Review Questions</i>	461
16. Wireless Devices with Windows CE	463
16.1 Introduction	463
16.2 Different Flavors of Windows CE	465
16.3 Windows CE Architecture	467
16.4 Windows CE Development Environment	476
<i>References/Further Reading</i>	479
<i>Review Questions</i>	479
17. Voice Over Internet Protocol and Convergence	480
17.1 Voice Over IP	480
17.2 H.323 Framework for Voice Over IP	481
17.3 Session Initiation Protocol (SIP)	483
17.4 Comparison between H.323 and SIP	486
17.5 Real-Time Protocols	487
17.6 Convergence Technologies	488
17.7 Call Routing	492
17.8 Voice Over IP Applications	496
17.9 IP Multimedia Subsystem (IMS)	498
17.10 Mobile VoIP	499

17.11 Voice Over Wireless LAN	500
<i>References/Further Reading</i>	501
<i>Review Questions</i>	502
18. Multimedia	504
18.1 Introduction	504
18.2 Why Multimedia	505
18.3 Compression and Decompression	506
18.4 Coder and Decoder (CODEC)	509
18.5 Popular Compression Techniques	515
18.6 Networked Multimedia Application	520
18.7 Issues in Multimedia Delivery Over the Internet	521
18.8 Multimedia Delivery Over the Internet	522
18.9 Multimedia Networking Protocols	524
18.10 Content Distribution Networks	525
18.11 Principles of Best Effort Delivery	526
18.12 Intserv and Diffserv	527
18.13 Multimedia Service Creation	528
<i>References/Further Reading</i>	535
<i>Review Questions</i>	535
19. IP Multimedia Subsystems	537
19.1 Introduction	537
19.2 IMS and Its Evolution	538
19.3 Benefits from IMS	541
19.4 Architecture of IMS Networks	542
19.5 Protocols Used in IMS	543
19.6 Building Blocks in IMS Networks	547
19.7 Call Flow in IMS Network	549
19.8 IMS Charging	550
19.9 Reference Points in IMS	553
19.10 Service Creation in IMS	557
19.11 Policy Management in IMS	559
19.12 Security in IMS	560
<i>References/Further Reading</i>	563
<i>Review Questions</i>	564
20. Security Issues in Mobile Computing	565
20.1 Introduction	565
20.2 Information Security	565
20.3 Security Techniques and Algorithms	571
20.4 Security Protocols	579
20.5 Public Key Infrastructure	583
20.6 Trust	585

20.7 Security Models	588
20.8 Security Frameworks for Mobile Environment	591
<i>References/Further Reading</i>	596
<i>Review Questions</i>	598
21. Next Generation Networks	600
21.1 All in One—The Converged Scenario	601
21.2 Narrowband to Broadband	603
21.3 All IP and B3G Network	605
21.4 OFDM (Orthogonal Frequency Division Multiplexing)	605
21.5 FAMA/DAMA	607
21.6 Multi Protocol Label Switching (MPLS)	607
21.7 Wireless Asynchronous Transfer Mode	609
21.8 Multimedia Broadcast Services	610
21.9 Multiple Play	612
21.10 Future Trends	614
<i>References/Further Reading</i>	614
<i>Review Questions</i>	616
Index	617

List of Abbreviations

1G	First Generation	ACL	Access Control List
2.5G	2.5 Generation	ACL	Asynchronous Connectionless Linkz
2G	Second Generation	ACM	Address Complete Message
3G	Third Generation	ACM	Audio Compression Manager
3GPP	Third Generation Partnership Project	AD	Access Device
3GPP LTE	3GPP Long Term Evolution	ADC	Analog to Digital Converter
3GPP2	Third Generation Partnership Project 2	ADPCM	Adaptive Differential (or Delta) PCM
4G	Fourth Generation communications	aDSL	asynchronous Digital Subscriber Line
A			
AAA	Authentication, Authorization and Accounting	AI	application Interface (prefix to interface class method)
AABS	Automatic Alternative Billing Service	AIFF	Audio Interchange File Format
AAS	Adaptive Antenna System	AIPN	All Internet Protocol Network
AC	Admission Control	ALAC	Apple Lossless Audio Codec
AC	Authentication Centre	ALS	Audio Lossless Coding
ACELP	Algebraic Code Excited Linear Prediction	AM	Amplitude Modulation
ACK	Acknowledgement	AMBE	Advanced Multi-band Excitation
		AMC	Adaptive Modulation and Coding

AMPS	Advanced Mobile Phone System	AVP	Attribute Value Pairs
AMR	Adaptive Multi Rate	AVS	Audio Video Standard
ANM	Answer Message		B
ANSI	American National Standards Institute	B2B	Business to Business
AoC	Advice of Charge	B3G	Beyond 3rd Generation
AP	Access Point	BASIC	Beginners All purpose Symbolic Instructional Code
API	Application Programming Interface	BCCH	Broadcast Control Channel
APN	Access Point Name	BER	Bit Error Rate
APN-NI	APN Network Identifier	BG	Border Gateway
APPUI	Application User Interface	BGCF	Breakout Gateway Control Function
AR	Access Requestor	BIB	Backward Indicator Bit
ARDOR	Adaptive Rate-distortion Optimized sound codeR	BMP	Bit Map
ARFCN	Absolute Radio Frequency Channel Numbers	BPSK	Binary Phase Shift Keying
ARIB	Association of Radio Industries and Businesses	BS	Base Station
ARP	Address Resolution Protocol	BSA	Basic Station Area
ARPA	Advance Research Project Agency	BSC	Base Station Controller
ARPU	Average Revenue Per User	BSN	Backward Sequence Number
ARQ	Automatic Repeat Request	BSS	Base Station Subsystem
ASCII	American Standard Code for Information Interchange	BSS	Basic Service Set
aSi-TFT	amorphous Silicon TFT	BSSAP	BSS Application Part
ASP	Active Server Page	BT	Busy Tone
ASP	Application Service Provider	BTS	Base Transceiver Station
AT	Attention	BTS	Base Transceiver System
ATD	Absolute Time Difference	BWA	Broadband Wireless Access
ATM	Asynchronous Transfer Mode		C
ATN	Automated Trust Negotiation Systems	CA	Certification Authority
ATRAC	Adaptive Transform Acoustic Coding	CA	Content Aggregator
AUC	Authentication Center	CAC	Channel Access and Control
		CAMEL	Customized Application for Mobile Network Enhanced Logic
		CAP	CAMEL Application Part

CAS	Call Associated Signalling	CI	Call Identifier
CAS	Conditional Access System	CICS	Customer Information Control System
CC	Country Code	CID	Cell ID
CC/PP	Composite Capabilities/ Preference Profiles	CIMD	Computer Interface to Message Delivery
CCETT	Centre Commun d'études de Télévision et Telecommunications	CLDC	Connected Limited Device Configuration
CCK	Complementary Code Keying	CLI	Caller Line Identification
CCSA	China Communications Standards Association	CM	Connection Management
CCSSO	Common Channel Signaling Switching Office	CMOS	Complementary Metal Oxide Semiconductor
CDC	Connected Device Configuration	CN	Core Network
CDF	Charging Data Function	CO	Central Office
CDMA	Code Division Multiple Access	CODEC	Coder and Decoder
CDN	Content Distribution Network	COPS	Common Open Policy Service
CDPD	Cellular Digital Packet Data	COPS-PR	COPS for Policy Provisioning
CDR	Call Detail Record	CORBA	Common Object Request Broker Architecture
CDR	Charging Data Records	CoS	Class of Service
CE devices	Customer Edge devices	CP	Content Provider
CEK	Content Encryption Key	CP	Contention Period
CELP	Code Excited Linear Prediction	CPE	Customer Premises Equipment
CEPT	Conference of European Posts and Telegraphs	CPI	Capability and Preference Information
CE-r	Customer Edge routers	CPU	Central Processing Unit
CE-s	Customer Edge switches	CRC	Cyclic Redundancy Code
CF	Contention Free	CRP	Customer Routing Point
CFB	Call Forwarding Busy	CS	Capability Set
CFNA	Call Forwarding Not Answered	CS	Carrier Sense
CFNR	Call Forwarding Not Reachable	CSCF	Call Session Control Function
CFP	Contention-Free Period	CSD	Circuit Switched Data
CFU	Call Forwarding Unconditional	CSE	CAMEL Service Environment
CGF	Charging Gateway Function	CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CGI	Computer Gateway Interface	CSMA/CD	Carrier Sense Multiple Access with Collision Detection
cHTML	compact Hyper Text Markup Language	CSP	Communication Service Provider

CT	Communication Technology	DMA	Direct Memory Access
CTI	Computer Telephony Interface/Computer	DMH	Data Message Handler
CTS	Clear To Send	DNS	Domain Name Server
CUG	Closed User Group	DoCoMo	DO (Everywhere) + COMO (Communication)
CVSD	Continuously Variable Slope Delta Modulation	DoD	Department of Defense
CWTS	China Wireless Telecommunication Standard group	DPC	Destination Point Code
Cyborg	Cyber Organism	DPRMA	Dynamic Packet Reservation Multiple Access
D			
DAB	Digital Audio Broadcast	DRM	Digital Rights Management
DAC	Digital to Analog Converter	DRNC	Drift RNC
DAMA	Demand Assignment Multiple Access	DS	Direct Sequence
DC	Data Center	DS	Distribution System
DCE	Data Circuit terminating Equipment	DSL	Digital Subscriber Line
DCF	Distributed Coordination Function	DSM CC	Digital Storage Media Command and Control
DCF	DRM Content Format	DSP	Digital Signal Processing
DCT	Discrete Cosine Transform	DSS	Digital Signal Processor
DECT	Digital Enhanced Cordless Communications	DSSS	Digital Speech Standard
DECT	Digital Enhanced Cordless Telecommunications	DST	Direct Sequence Spread Spectrum
DFP	Distributed Functional Plane	DT	Direct Stream Transfer
DFRD	Device Family Reference Designs	DTE	Dial Tone
DHCP	Dynamic Host Configuration Protocol	DTMF	Data Terminal Equipment
DIFS	Distributed Inter Frame Space	DUP	Dual Tone Multi Frequency
DL	Downlink	DV Codec	Data User Part
DLB	Dynamic Label Segment	DVB	Digital Video Codec
DLC	Digital Loop Carrier	DVD	Digital Video Broadcasting
DLL	Data Link Layer	DWDM	Digital Video Disc
DLL	Dynamic Link Library	EAP	Dense Wavelength Division Multiplexing
DLNA	Digital Living Network Alliance		E
			Extensible Authentication Protocol

EDGE	Enhanced Data rate for GSM Evolution	FH	Frequency Hopping
EGPRS	Enhanced GPRS	FHSS	Frequency Hopping Spread Spectrum
EIA	Electronic Industries Alliance	FIB	Forward Indicator Bit
EIFS	Extended Inter Frame Space	FISU	Fill-In Signal Units
EIR	Equipment Identity Register	FLAC	Free Lossless Audio Codec
EMS	Extended Message Service	FM	Frequency Modulation
ENIAC	Electronic Numerical Integrator and Computer	FNC	Federal Networking Council
ENUM	Electronic Numbering	FOFDM	Flash Orthogonal Frequency Division Multiplexing
E-OTD	Enhanced Observed Time Difference	FRA	Fixed Radio Access
ERP	Enterprise Resource Planning	FSN	Forward Sequence Number
ESME	External Short Message Entity	FSNP	Full Service and Network Provider
ESN	Electronic Serial Number	FSU	Fixed Subscriber Unit
ESS	Electronic Switching System	FTP	File Transfer Protocol
ESS	Extended Service Set	FWA	Fixed Wireless Access
ETSI	European Telecommunication Standards Institute		G
EU	End User	GERAN	GSM EDGE Radio Access Network
EVRC	Enhanced Variable Rate Codec	GFP	Global Functional Plane
EY-NPMA	Elimination-Yield Non-Preemptive Multiple Access	GGSN	Gateway GPRS Support Node
F			
FAMA	Fixed Assignment Multiple Access	GIF	Graphics Interchange Format
FCAPS	Fault, Configuration, Accounting, Performance, Security	GIWU	Gateway Inter Working Unit
FDD	Frequency Division Duplex	GMLC	Gateway MLC
FDMA	Frequency Division Multiple Access	GMSC	Gateway MSC
FE	Functional Entity	GPRS	General Packet Radio Service
FEA	Functional Entity Action	GPS	Global Positioning System
FEC	Forward Error Correction	GSM	Global System for Mobile communications
FER	Frame Error Rate	GT	Global Title
		GTT	Global Title Translation
		GUI	Graphical User Interface
H			
		HC SDMA	High Capacity Spatial Division Multiple Access

HCI	Human Computer Interface	I	
HCPDU	HiperLAN CAC Protocol Data Unit	I/O	Input/Output
HCSAP	HiperLAN CAC Service Access Point	IAM	Initial Address Message
HCSDU	HiperLAN CAC Service Data Unit	IAPP	Inter-Access Point Protocol
HDLC	High level Data Link Control	IBSS	Independent Basic Service Set
HDML	Handheld Device Markup Language	IC	Integrated Circuit
HDTP	Handheld Device Transport Protocol	ICAP	Internet Content Adaptation Protocol
HDTV	High Definition Television	ICCC	International Computer Communication Conference
HE AAC	High Efficiency Advance Audio Coding	ICL	International Computers Limited
HE	Home Environment	ICMP	Internet Control Message Protocol
HFC	Hybrid Fiber Coaxial	I-CSCF	Interrogating Call Session Control Function
HiperLAN	High Performance Radio Local Area Network	ICT	Information and Communication Technology
HiperMAN	High Performance Radio Metropolitan Area Network	IDE	Interactive Development Environment
HLF	Home Location Function	IED	Information Element Data
HLR	Home Location Register	IEDL	Information Element Data Length
HMPDU	HiperLAN MAC Protocol Data Unit	IEEE	Institute of Electrical and Electronics Engineers
HPLMN	Home Public Land Mobile Network	IEI	Information Element Identifier
HSDPA	High Speed Downstream Packet Availability	IETF	Internet Engineering Task Force
HSOPA	High Speed OFDM Packet Access	IGMP	Internet Group Management Protocol
HSPA	High Speed Packet Access	IHF	Integrated Hands Free
HSS	Home Subscriber Server	I-HSPA	Internet HSPA
HSUPA	High Speed Uplink Packet Access	iLBC	internet Low Bit rate Codec
HTML	Hyper Text Markup Language	IM SSF	IP Multimedia Services Switching Function
HTTP	Hyper Text Transfer Protocol	IMAP	Internet Message Access Protocol
HVXC	Harmonic Vector Excitation Coding	IMBE	Improved Multi-Band Excitation

IMEI	International Mobile Equipment Identity	ISIM	IP multimedia Subscriber Identity Module
IMS GWF	IMS Gateway Function	ISM	Industrial, Scientific, and Medical
IMS	IP Multimedia Subsystems	ISO	International Organization for Standardization
IMSI	International Mobile Subscriber Identity	ISP	Internet Service Provider
IMT DS	IMT Direct Spread	ISUP	ISDN User Part
IMT FT	IMT FDMA/TDMA	ISV	Independent Software Vendor
IMT FT	IMT Frequency Time	IT	Information Technology
IMT MC	IMT Multi Carrier	ITTP	Intelligent Terminal Transfer Protocol
IMT SC	IMT Single Carrier	ITU	International Telecommunication Union
IMT TC	IMT TDD Carrier	ITU-T	International Telecommunication Union-Telecommunication Standardization
IMT	International Mobile Telecommunications		
IN	International Mobile Telecommunications	IVR	Interactive Voice Response
INAP	Intelligent Networks	IWF	Inter Working Function
INCM	Intelligent Network Application Part	IWMSC	Inter Working MSC
IP	IN Conceptual Model		
IPCP	Internet Protocol		
IPCP	Internet Protocol Control Protocol		
IPDL	Idle Period Downlink	J2EE	Java 2 Enterprise Edition
IPDR	IP Data Record	J2ME	Java 2 Micro Edition
IPNG	Next Generation Internet Protocol	J2SE	Java 2 Standard Edition
IPsec IKE	IPsec Internet Key Exchange	JDBC	Java Data Base Connector
IPsec	Internet Protocol Security	JFIF	JPEG File Interchange Format
IPTV	Internet Protocol Television	JPEG	Joint Photographic Experts Group
IR	Infra Red	JSP	Java Server Pages
IrDA	Infrared Data Association	JSR	Java Specification Request
IrMC	Infrared Mobile Communication		
IRT	Institute für Rundfunktechnik GmbH	KVCD	K Video Compression Dynamics
iSAC	internet Speech Audio Codec		
ISDN	Integrated Services Digital Network	L2CAP	Logical Link Control and Adaptation Protocol
ISI	Inter Symbol Interference		

J
 Java 2 Enterprise Edition
 Java 2 Micro Edition
 Java 2 Standard Edition
 Java Data Base Connector
 JPEG File Interchange Format
 Joint Photographic Experts Group
 Java Server Pages
 Java Specification Request

K
 K Video Compression Dynamics

L
 Logical Link Control and Adaptation Protocol

L2TP	Layer 2 Tunneling Protocol	LSAF	Location Subscriber Authorization Function
LA	Location Application	LSBcF	Location System Broadcast Function
LA	Location Area	LSBF	Location System Billing Function
LA	Lossless Audio	LSCF	Location System Control Function
LAF	Location Application Function	LSOF	Location System Operation Function
LAI	Location Area Identifier	LSP	Label Switched Path
LAN	Local Area Network	LSPF	Location Subscriber Privacy Function
LAP	LAN Access Point	LSR	Label Switching Router
LAP	Link Access Procedure	LSSU	Link Status Signal Unit
LAPD	Link Access Procedure-D	LTAC	Lossless Transform Audio Compression
LBS	Location Based Services	LTE	Long Term Evolution
LCAF	Location Client Authorization Function	LTPS-TFT	Low Temperature Poly Silicon TFT
LCCF	Location Client Control Function	LZW	Lempel Ziv Welch
LCCTF	Location Client Coordinate Transformation Function		M
LCD	Liquid Crystal Diode	M2M	Machine to Machine
LCD	Liquid Crystal Display	MAC	Media Access Control
LCF	Location Client Function	MAN	Metropolitan Area Network
LCP	Link Control Protocol	MAP	Mobile Application Part
LCS	LoCation Services	Mbone	Multicast back bone
LCZTF	Location Client Zone Transformation Function	MCC	Mobile Country Code
LDR	Location Deferred Request	MCU	Master Controller Unit
LED	Light Emitting Diodes	ME	Mobile Equipment
LEO	Low Earth Orbit	MEGACO	Media Gateway Control Protocol
LIR	Location Immediate Request	MELP	Mixed Excitation Linear Prediction
LLC	Logical Link Control	MEO	Medium Earth Orbit
LMP	Link Manager Protocol	MExE	Mobile Execution Environment
LMSI	Local Mobile Subscriber Identity		
LMU	Location Measurement Unit		
LNP	Local Number Portability		
LPAC	Lossless Predictive Audio Compression		
LPC	Linear Prediction Coding		
LPCM	Linear Pulse Code Modulation		

MGCP	Media Gateway Control Protocol	MRFC	Media Resource Function Controller
MGW	Media Gateway	MRFP	Media Resource Function Processor
MIB	Management Information Base	MS	Mobile Station
MIDP	Mobile Information Device Profile	MSAP	Media Service Access Point
MIMO	Multiple Input Multiple Output	MSC	Mobile Switching Centre
MIN	Mobile ID Number	MSDU	MAC Service Data Unit
MIPS	Millions of instructions per second	MSDU	MAC Service Data Unit
MIS	Management Information Systems	MSIN	Mobile Subscriber Identification Number
mITF	mobile IT Forum	MSISDN	Mobile Station ISDN
MLC	Mobile Location Center	MSP	Mobile Service Provider
MLME	MAC sub Layer Management Entity	MSRN	Mobile Station Roaming Number
MM	Mobility Management	MSU	Message Signal Units
MMI	Man Machine Interface	MT	Mobile Terminated
MMS	Multimedia Message Service	MTAS	Multimedia Telephony Application Service
MMSC	MMS Controller		
MMSE	MMS Environment	MT-LR	Mobile Terminated Location Request
MMTel	Multimedia Telephony	MTP	Message Transfer Part
MMU	Memory Management Unit	MVC	Model-View-Controller
MNC	Mobile Network Code	MVNO	Mobile Virtual Network Operator
MNG	Multiple image Network Graphics		
MO	Mobile Originated		
MO-LR	Mobile Originated Location Request	NA-ESRD	North American Emergency Service Routing Digits
MOM	Message Oriented Middleware	NA-ESRK	North American Emergency Service Routing Key
MP2	MPEG-1 layer-2 audio coding	NAT	Network Address Translator
MP3	MPEG 1 Part 3 Layer 3	NAV	Network Allocation Vector
MPDU	MAC Protocol Data Unit	NDC	National Destination Code
MPEG	Moving Pictures Expert Group	NDP	Network Decision Point
MPEG-4 ASP	MPEG 4 Advanced Simple Profile	NFC	Near Field Communications
MPLS	Multiprotocol Label Switching	NGN	Next Generation Network
MPLS	Multiprotocol Label Switching	NIC	Network Interface Card
MRF	Media Resource Function		

N

North American Emergency Service Routing Digits
 North American Emergency Service Routing Key
 Network Address Translator
 Network Allocation Vector
 National Destination Code
 Network Decision Point
 Near Field Communications
 Next Generation Network
 Network Interface Card

NID	Network Identification	OSA	Open Service Architecture
NI-LR	Network Induced Location Request	OSA-SCS	Open Service Access Service Capability Server
NNI	Network to Network Interface	OSS	Operation and Support Subsystem
NO	Network Operator	OSS	Operations Support System
N-PE devices	Network-facing PE devices	OTA	Over-The-Air
NSF	National Science Foundation	OTDOA	Observed Time Difference Of Arrival
NSS	Network and Switching Subsystem		
NTT	Nippon Telegraph and Telephone Corporation		P
		P3P	Platform for Privacy Preference Project
		PAM	Pulse-amplitude Modulation
OBEX	Object Exchange Protocol	PAN	Personal Area Network
OCC	Occasionally Connected Computing	PBX	Private Branch Exchange
OCR	Optimal Call Routing	PBX	Private Business Exchange
OCS	Online Charging System	PC	Point Coordinator
ODBC	Open Data Base Connectivity	PC	Power Control
OEM	Original Equipment Manufacturer	PCF	Point Coordination Function
OFC	Optical Fiber Cable	PCH	Power Calculation Function
OFDM	Orthogonal Frequency Division Multiplexing	PCI	Paging Channels
OFDMA	Orthogonal Frequency Division Multiple Access	PCM	Peripheral Component Interface
OFR	OptimFROG	PCMCIA	Pulse Coded Modulation
OMA	Open Mobile Alliance	PCN	Personal Computer Memory Card International Association
OMAP	Operations, Maintenance and Administration Part	PCS	Personal Communication Networks
OMC	Operation and Maintenance Center	P-CSCF	Personal Communications Service
OOPS	Object Oriented Programming	PDA	Proxy Call Session Control Function
OPC	Originating Point Code	PDC	Personal Digital Assistant
OPL	Organiser Programming Language	PDF	Personal Digital Cellular
OS	Operating System	PDN	Policy Decision Function
OSA	Open Service Access	PDP	Packet Data Network
			Packet Data Protocol

PDP	Policy Decision Point	PP	Physical Plane
PDTCH	Packet Data Traffic Channel	PPDU	PLCP Protocol Data Unit
PDU	Protocol Data Unit	PPG	Push Proxy Gateway
PE devices	Service Provider Edge devices	PPP	Point-to-Point Protocol
PE	Physical Entity	PR	Policy Repository
PEAP	Protected EAP	PRCF	Positioning Radio Co-ordination Function
PEP	Policy Enforcement Point	PRMA HS	Packet Reservation Multiple Access Hindering States
PE-r	Provider Edge routers	PRMA	Packet Reservation Multiple Access
PE-rs	Provider Edge devices that are capable of both routing and switching	PRNG	Pseudo-Random Number Generator
PE-s	Provider Edge switches	PRRM	Positioning Radio Resource Management
PHP	Hypertext Preprocessor	PS	Power Save (mode)
PHS	Personal Handyphone System	PSDN	Public Switched Data Network
PHY	Physical (layer)	PSDU	Physical sublayer Service Data Unit
PIB	Policy Information Bases	PSE	Personal Service Environment
PICS	Platform for Internet Content Selection	PSF	PLCP Signaling Field
PIFS	Point (coordination function)	PSMF	Positioning Signal Measurement Function
	Inter Frame Space	PSPDN	Public Switched Packet Data Networks
PIM	Personal Information Management	PSTN	Public Switched Telephone Network
PKI	Public Key Infrastructure	PTM	Point-To-Multipoint
PLCP	Physical Layer Convergence Procedure	PTP	Point-To-Point
PLL	Physical Link Layer		Q
PLMN	Public Land Mobile Network	QCELP	Qualcomm Pure Voice
PLW	PSDU Length Word	QoS	Quality of Service
PMD	Physical Medium Dependent	QPSK	Quadrature Phase Shift Keyed
PN	Pseudo random Noise		R
PNG	Portable Network Graphics	RA	Routing Area
POI	Point Of Initiation	RACH	Random Access Channel
POI	Privacy Override Indicator		
PoP	Points of Presence		
POP	Post Office Protocol		
POR	Point Of Return		
POS	Point Of Sale		
POTS	Plain Old Telephone Service		

RADIUS	Remote Authentication Dial In User Service	RPE-LPC	Regular Pulse Excited-Linear Predictive Coder
RAM	Random Access Memory	RRM	Radio Resource Management
RAN	Radio Access Network	RSA	Rivest, Shamir, Adelman
RANAP	RAN Application Part	RSACi	Recreational Software Advisory Council internet
RAND	Random Number	RSM	Remote Switching Modules
RAS	Remote Access Service	RSU	Radio Subscriber Unit
RASP	Reliability, Availability, Security, and Performance	RSVP	Resource reSerVation Protocol
RCELP	Relaxed Code Excited Linear Prediction	RT	Ring Tone
RDF	Resource Description Framework	RTCP	RTP Control Protocol
REL	Release	RTD	Real-time Difference
RF	Radio Frequency	RTP	Real-time Transfer Protocol
RFC	Request For Comments	RTS	Request To Send
RFCOMM	Radio Frequency Communication	RTSP	Real-time Streaming Protocol
RTT		RTT	Radio Transmission Technology
RFID	Radio Frequency Identifiers		S
RFL	Radio Frequency Layer	SA	Security Associations
RGB	Red Green Blue	SAP	Service Access Point
RIFF	Resource Interchange File Format	SAT	SIM Application Toolkit
RIP	Routing Information Protocol	SBS	Switched Beam System
RIS	Radio Interface Synchronization	SC	Service Centre
RISC	Reduced Instruction Set Computer	SCCP	Signalling Connection Control Part
RKAU	RK Audio	SCF	Service Capability Feature
RLC	Radio Link Control	SCO	Synchronous Connection Oriented link
RLC	Release Complete	SCP	Service Control Point
RLE	Run Length Encoding	SCS	Service Capability Servers
RLL	Radio Local Loop	S-CSCF	Serving Call Session Control Function
RLP	Radio Link Protocol	SCUA	Service Control User Agent
RNC	Radio Network Controller	SDH	Synchronous Digital Hierarchy
ROM	Read Only Memory	SDK	Software Development Kit
RPC	Remote Procedure Call	SDMA	Space Division Multiple Access
RPCU	Radio Port Control Unit	SDP	Service Discovery Protocol
		SDP	Session Description Protocol

sDSL	synchronous Digital Subscriber Line	SMTP	Simple Mail Transfer Protocol
SDTV	Standard Definition TV	SMV	Selectable Mode Vocoder
SF	Service Feature	SN	Service Node
SGSN	Serving GPRS Support Node	SNA	Subscriber Number
SGW	Signaling Gateway	SNDCF	System Network Architecture
SHN	Shorten	SNDCP	Sub Network Dependent Convergence Function
SI	Service Interface (prefix to interface class method)	SNR	Sub Network Dependent Convergence Protocol
SIB	Service Independent Building block	SOAP	Signal to Noise Ratio
SIBO	Single Board Organizer	SoD	Simple Object Access Protocol
SID	System Identification	SP	Session oriented Dialogue
SIF	Service Information Field	SP	Service Plane
SIFS	Short Inter Frame Space	SPC	Service Point
SIM	Subscriber Identity Module	SPI	Signaling Point Code
SIO	Service Indicator Octet	SQL	Service Provider Interface
SIP AS	SIP Application Server	SRC	Structured Query Language
SIP	Session Initiation Protocol	SRES	Short Retry Count
SIR	Signal Interference Ratio	SRNC	Signature Response
SIS	Symbian OS Installation	SS	Serving RNC
SLF	Subscriber Location Function	SS	Signalling System
SLPP	Subscriber LCS Privacy Profile	SS7	Station Service
SME	Short Message Entity	SS7	Signaling Stack 7
SME	Station Management Entity	SSID	Signaling System No 7
SMG	Special Mobile Group	SSL	Service Set Identifier
SMIL	Synchronization Multimedia Integration Language	SSO	Secured Socket Layer
SMLC	Serving Mobile Location Centre	SSP	Single Sign On
SMMO	Short Message Mobile Originated point-to-point	STA	Service Switching Point
SMMT	Short Message Mobile Terminated point-to-point	STB	Station
SMPP	Short Message Peer-to-Peer	STP	Set Top Boxes
SMS	Service Management System in SMS/800	SVG	Signaling Transfer Point
SMS	Short Message Service	SWAP	Scalable Vector Graphics
SMSC	SMS Centre	TA	Shared Wireless Access Protocol
		TA	T
		TA	Timing Advance
		TA	True Audio

TACS	Total Access Communication System	TTC	Telecommunication Technology Committee-Japan
TCAP	Transaction Capabilities Application Part	TTL	Time To Live
TCP	Transmission Control Protocol	TTML	Tagged Text Mark-up Language
TCP/IP	Transmission Control Protocol/Internet Protocol	TTS	Text To Speech
TCS	Telephony Control Specification	TUP	Telephone User Part
U			
TD-CDMA	Time Division Code Division Multiple Access	UAProf	User Agent Profile
TDD	Time Division Duplex	UDH	User Data Header
TDMA	Time Division Multiple Access	UDHI	User Data Header Indicator
	Telephony Integration	UDP	User Datagram Protocol
TFT	Thin Film Transistor	UDT	Unit Data message
THIG	Topology Hiding Interworking Gateway	UE	User Equipment
TIA	Telecommunication Industries Association	UICC	Universal Integrated Circuit Card
TINA	Telecommunications Information Network Architecture consortium	UL	Uplink
		UMTS	Universal Mobile Telecommunication System
TKIP	Temporal Key Integrity Protocol	UNI	User to Network Interface
TLS	Transport Layer Security	URI	Universal Resource Identifier
TMSI	Temporary Mobile Subscriber Identity	URL	Universal Resource Locator
TN3270	Telnet protocol for IBM 3270	USIM	Universal Subscriber Identity Module
TN5250	Telnet protocol for IBM 5250	USSD	Unstructured Supplementary Service Data
TOA	Time Of Arrival	UTRAN	Universal Terrestrial Radio Access Network
TP	Transaction Processing	V	
TPMS	Transaction Processing Management System	VAS	Value Added Service
TRC	Triple Rate CODER	VASP	Value Added Service Provider
TSCC	Tech Smith Screen Capture Codec	VCD	Video Compact Disc
TSP	Telephone Service Provider	VCR	Video Cassette Recorder
TT	Trouble Ticket	VDU	Visual Display Unit
TTA	Telecommunications Technology Association-Korea	VHE	Virtual Home Environment
		VHS	Video Home System

VLR	Visitor Location Register	WCDMA	Wideband Code Division Multiple Access
VLSI	Very Large Scale Integration	WDP	Wireless Datagram Protocol
VME	Virtual Machine Environment	Wi-Fi	Wireless Fidelity
VoD	Video on Demand	WiLL	Wireless in Local Loop
VOFDM	Vector Orthogonal Frequency Division Multiplexing	WiMAX	Worldwide Interoperability for Microwave Access
VoIP	Voice over IP	WLAN	Wireless LAN
VPLS	Virtual Private LAN Service	WLL	Wireless Local Loop
VPN	Virtual Private Network	WM	Wireless Medium
VPNC	Virtual Private Network Consortium	WMA	Windows Media Audio
VPS	Voice Processing System	WML	Wireless Markup Language
VRML	Virtual Reality Markup Language	WMV	Windows Media Video
VRU	Voice Response Unit	WOFDM	Wideband Orthogonal Frequency Division Multiplexing
VSAT	Very Small Aperture Terminal	WSP	Wireless Session Protocol
VSELP	Vector Sum Excited Linear Prediction	WTA	Wireless Telephony Applications
—		WTAI	Wireless Telephony Application Interface
VT3K	Visual Terminal for HP 3000	WTLS	Wireless Transport Layer Security
W			
W3C	WWW Consortium	WTP	Wireless Transaction Protocol
WAE	Wireless Application Environment	WV	WavPack
WAFU	Wireless Access Fixed Unit	WWAN	Wireless Wide Area Network
WAP	Wireless Application Protocol	WWW	World Wide Web
WATM	Wireless Asynchronous Transfer Mode		
WBMP	Wireless BMP	XML	eXtensible Markup Language
X			



CHAPTER 1



Introduction

1.1 MOBILITY OF BITS AND BYTES

Information is power. But for a long time people did not know how to store information and knowledge which could be easily accessible. Convergence of information and communication technology has created ways to address these challenges. Today even when we are on the move, we can access information from anywhere, any time.

In the last two centuries, mobility has been redefined. Both physical and virtual objects are now mobile. Mobility of physical objects relate to movement of matters, whereas movements of virtual objects relate to movements of bits and bytes.

The foundation of mobility of information was laid by Joseph Henry, (1797–1878), who invented the electric motor and techniques for distant communication. In 1831, Henry demonstrated the potential of using an electromagnetic phenomenon of electricity for long distance communication. He sent electric current over one mile of wire to activate an electromagnet, which caused a bell to ring. Later, Samuel F. B. Morse used this property of electricity to invent the telegraph. Morse transmitted his famous message “What hath God wrought?” from Washington to Baltimore over 40 miles in 1844. Then on March 10, 1876, in Boston, Massachusetts, Alexander Graham Bell laid the foundation of telephone by making the first voice call over wire—“Mr. Watson, come here, I want to see you”.

On October 4, 1957, the USSR (Union of Soviet Socialist Republic, now mainly Russia) launched the Sputnik. It was the first artificial earth satellite launched from Baikonur cosmodrome in Kazakhstan. This demonstrated the technological superiority of USSR. In response to this, the US formed the Advanced Research Projects Agency (ARPA) within the Department of Defense (DoD). The mandate for ARPA was to establish the US as a leader in science and technology. ARPA funded different research projects to help conduct research in computer networks. This laid the

foundation of packet switched data networks. There were multiple flavors of packet switched networks in the US and in Europe. The important ones are TCP/IP and X.25. TCP/IP was driven by education and defense in the US whereas X.25 was driven by European telecommunication industry and governments. With the evolution of computers and packet switched networks, movement of bits and bytes progressed to a new state of maturity. Over the last 175 years, virtual reality evolved from ringing an electric bell to mobile computing.

1.1.1 The Convergence Leading to ICT

The first step towards the convergence between telecommunication and IT happened in 1965 when AT&T used computers to do the switching in an electronic switching system (ESS). On the other hand, packet switch network was bringing communication closer to computers. The World Wide Web (WWW), which was started by Tim Berners-Lee in 1989 as a text processing software, brought these two faculties of technology together and established Internet as a powerful media. The Internet meets four primary needs of the society: communication, knowledge sharing, commerce, and entertainment. This convergence is called Information and Communications Technologies (ICT). Through ICT we are now moving towards an information-based society. ICT will address the need to access data, information, and knowledge from anywhere, anytime.

1.2 WIRELESS—THE BEGINNING

In 1947, researchers in AT&T Bell Labs conceived the idea of cellular phones. They realized that by using small service areas or cells they can reuse the frequency. This in turn can enhance the traffic capacity of mobile phones. AT&T requested the Federal Communication Commission (FCC) to allocate a large number of radio-spectrum frequencies so that widespread mobile telephone services would become feasible. FCC is a government agency in the US that regulates the usage and licensing of frequency bands. Every country has its regulatory agencies like FCC. In India the regulatory authority is Telecom Regulatory Authority of India (TRAI). FCC in the US is charged with regulating interstate and international communications by radio, television, wire, satellite and cable. Initially, FCC agreed to license a very small band to AT&T. This small frequency range made only 23 simultaneous phone conversations possible in one service area. With 23 channels there was no market incentive for either research or commercial deployment for AT&T. Though the idea of cellular telephony was very much there in the late forties, it did not take off.

1.2.1 Evolution of Wireless Networks

The first wireless network was commissioned in Germany in 1958. It was called A-Netz and used analog technology at 160 MHz. Only outgoing calls were possible in this network. That is to say that connection set-up was possible from the mobile station only. This system evolved into B-Netz operating at the same 160 MHz. In this new system, it was possible to receive an incoming call from a fixed telephone network, provided that location of the mobile station was known. This system was also available in Austria, the Netherlands, and Luxemburg. A-Netz was wireless but not a cellular network. Therefore, these systems (A-Netz and B-Netz) did not have any function,

which permitted handover or change of base station. The B-Netz had 13,000 customers in West Germany and needed a big transmitter set, typically installable in cars.

In 1968, in the US, the FCC reconsidered its position on the cellular network concept. FCC agreed to allocate a larger frequency band for more number of mobile phones provided the technology to build a better mobile service be demonstrated. AT&T and Bell Labs proposed a cellular system to the FCC with many small, low-powered, broadcast towers, each covering a hexagonal 'cell' of a few kilometers in radius. Collectively these cells could cover a very large area. Each tower would use only a few of the total frequencies allocated to the system. As the phones traveled across the area, calls would be passed from tower to tower.

Besides AT&T and Bell Labs, other enterprises were also engaged in research in the wireless domain. In April 1973, Martin Cooper of Motorola invented the first mobile phone handset and made the first call from a portable phone to Joel Engel, his rival in AT&T and Bell Labs. By 1977, AT&T and Bell Labs constructed a prototype of a public cellular network. In 1978, public trials of the cellular telephony system started in Chicago with over 2000 trial customers. In 1982, FCC finally authorized commercial cellular service for the US. A year later in 1983, the first American commercial analog cellular service AMPS (Advanced Mobile Phone Service) was made commercially available in Chicago. This was the first cellular mobile network in the world.

While the US was experiencing the popularity of cellular phones, Japan and Europe were not lagging behind. In 1979, the first commercial cellular telephone system began operations in Tokyo. During the early 1980s, cellular phone experienced a very rapid growth in Europe, particularly in Scandinavia and the United Kingdom. There was decent growth of cellular phones in France and Germany as well. The message was quite clear by then that mobile technology was here to stay.

To take advantage of this growing market, each country in Europe developed its own analog mobile system and joined the bandwagon. These cellular systems developed by each country in Europe were mutually incompatible. These incompatibilities made the operation of the mobile equipment limited to national boundaries. Also, a mobile subscriber of one network cannot use the same device in another network in another country. Though the market was growing, these incompatible systems made the market very limited for equipment manufacturers. This became an increasingly unacceptable situation in a unified Europe.

To cope with these problems Europeans decided to evolve a standard for mobile phone technology. In 1982, the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Groupe Spécial Mobile (GSM) to develop a standard for the pan-European mobile system. In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and GSM became a technical committee within ETSI. In 1990, Phase I of the GSM specifications were published. Commercial services of GSM started in mid-1991. Although standardized in Europe, GSM became popular outside Europe as well. Therefore, to give a global flavor, GSM was renamed as 'Global System for Mobile communications'. This has grown to more than 1 billion by the end of February 2004 in over 200 countries. At the beginning of 2009 the number of mobile phones in the world crossed the 4 billion mark—two phones in every three persons in the world. In the beginning of 1994, there were 1.3 million subscribers worldwide. In October 2004, the number of mobile subscribers in India crossed the number of fixed phones.

If we look at the critical success factor of GSM, we find quite a few technical and non-technical reasons for its tremendous success. These are:

- The developers of GSM sat together to arrive at a standard before they built the system. The advantage of standards is that they provide enough standardization to guarantee proper interoperability between different components of the system. GSM standards also facilitate the interworking between different vendors. Over 8000 pages of GSM recommendations ensure competitive innovation among suppliers.
- International roaming between networks. A subscriber from one network can seamlessly roam in another network and avail of services without any break.
- Emergence of SMS (Short Message Service) has spawned several applications within the GSM framework.
- The developers of GSM took considerable technological risks by choosing an unproven (in 1980s) digital system. They had the confidence that advancements in compression algorithms and digital signal processing would allow the continual improvement of the system in terms of quality and cost.

1.2.2 Evolution of Wireless Data

Like computers, the evolution of wireless technology has also been defined in generations. The first generation or 1G wireless technology uses analog technology. It uses FDMA (Frequency Division Multiple Access) technology for modulation; for example, AMPS (Advanced Mobile Phone Service) in the US. The second generation or 2G technology uses digitized technology. It uses a combination of TDMA (Time Division Multiple Access) and FDMA technologies. An example is GSM. In 2G technology, voice is digitized over a circuit. In 1G and 2G networks, data is transmitted over circuits. This technology is called Circuit Switched Data or CSD in short. Using modems, a data connection is established between the device and the network. This is similar to what happens in a dial-up network over analog telephones at home. The next phase in the evolution is 2.5G. In 2.5G technology, voice is digitized over a circuit. However, data in 2.5G is packetized. 2.5G uses the same encoding techniques as 2G. GPRS networks is an example of 2.5G. The Third Generation or 3G wireless technology makes a quantum leap from a technology point of view. 3G uses Spread Spectrum techniques for media access and encoding. In 3G networks, both data and voice use packets. UMTS and CDMA2000 are examples of 3G networks.

While 1G, 2G, or 3G were making their mark in the metropolitan area wireless networks (MAN), wireless technology has been getting popular in local area networks (LAN) and personal area networks (PAN). Wireless technology offers convenience and flexibility. With the success of wireless telephony and messaging services like paging, wireless communication is beginning to be applied to the realm of personal and business computing in the domain of local area networks. Wireless LANs are being deployed in homes, campuses, and commercial establishments. Wireless LANs are also being deployed in trains and commercial vehicles. The domain of wireless data networks today comprises Wireless PAN (Bluetooth, Infrared), Wireless LAN (IEEE 802.11 family) and Wireless WAN (Wide Area Networks) (GSM, GPRS, 3G).

1.2.3 Evolution of Wireless LAN

In late 1980s, vendors started offering wireless products, which were to substitute the traditional wired LAN (Local Area Network) ones. The idea was to use a wireless local area network to avoid

the cost of installing LAN cabling and ease the task of relocation or otherwise modifying the network's structure. When Wireless LAN (WLAN) was first introduced in the market, the cost per node was higher than the cost of its counterpart in the wired domain. However, as time progressed, the cost per node started dropping, making wireless LAN quite attractive. Slowly WLAN started becoming popular and many companies started offering products. The question of interoperability between different wireless LAN products became critical. IEEE Standards committee took the responsibility to form the standard for WLAN. As a result the IEEE 802.11 series of standards emerged.

WLAN uses the unlicensed Industrial, Scientific, and Medical (ISM) band that different products can use as long as they comply with certain regulatory rules. These rules cover characteristics such as radiated power and the manner in which modulation occurs. The ISM bands specified by the ITU-R are: 6.765–6.795 MHz, 13.553–13.567 MHz, 26.957–27.283 MHz, 40.66–40.70 MHz, 433.05–434.79 MHz, 902–928 MHz, 2.400–2.500 GHz, 5.725–5.875 GHz, 24.00–24.25 GHz, 61.00–61.5 GHz, 122–123 GHz, 244–246 GHz. WLAN uses 2.4 GHz and 5.8 GHz ISM bands. WLAN works both in infrastructure mode and ad hoc mode. WLAN is also known as Wireless Fidelity or WiFi in short. There are many products which use these unlicensed bands along with WLAN; examples could be cordless telephone, microwave oven, etc.

1.2.4 Evolution of Wireless PAN

Wireless technology offers convenience and flexibility. Some people will call this freedom from being entangled with the wire. The success of wireless technology in cellular telephones or Wireless MAN (Metropolitan Area Network) made people think of using the technique in Wireless LAN and Wireless Personal Area Network (WPAN). Techniques for WPANs are infrared and radio waves. Most of the laptop computers support communication through infrared, for which standards have been formulated by IrDA (Infrared Data Association—www.irda.org). Through WPAN, a PC can communicate with another IrDA device like another PC or a Personal Digital Assistant (PDA) or a Cellular phone.

The other best known PAN technology standard is Bluetooth. Bluetooth uses radio instead of infrared. It offers a peak over the air speed of about 2.1 Mbps over a short range of about 100 meters (power dependent). The advantage of radio wave is that unlike infrared it does not need a line of sight. WPAN works in ad hoc mode only.

1.3 MOBILE COMPUTING

Mobile computing can be defined as a computing environment of physical mobility. The user of a mobile computing environment will be able to access data, information, or other logical objects from any device in any network while on the move. A mobile computing system allows a user to perform a task from anywhere using a computing device in the public (the Web), corporate (business information) and personal information spaces (medical record, address book). While on the move, the preferred device will be a mobile device, while back at home or in the office the device could be a desktop computer. To make the mobile computing environment ubiquitous, it is necessary that the communication bearer is spread over both wired and wireless media. Be it for the mobile

workforce, holidayers, enterprises, or rural population, access to information and virtual objects through mobile computing is absolutely necessary for optimal use of resource and increased productivity.

Mobile computing is used in different contexts with different names. The most common names are:

- *Mobile Computing*: This computing environment moves along with the user. This is similar to the telephone number of a GSM (Global System for Mobile communication) phone, which moves with the phone. The offline (local) and real-time (remote) computing environment will move with the user. In real-time mode the user will be able to use all his remote data and services online.
- *Anywhere, Anytime Information*: This is the generic definition of ubiquity, where the information is available anywhere, all the time.
- *Virtual Home Environment*: Virtual Home Environment (VHE) is defined as an environment in a foreign network such that the mobile users can experience the same computing experience as they have in their home or corporate computing environment. For example, one would like to keep the room heater on when one has stepped outside for about 15 minutes.
- *Nomadic Computing*: The computing environment is nomadic and moves along with the mobile user. This is true for both local and remote services.
- *Pervasive Computing*: A computing environment, which is pervasive in nature and can be made available in any environment.
- *Ubiquitous Computing*: A (nobody will notice its presence) everyplace computing environment. The user will be able to use both local and remote services.
- *Global Service Portability*: Making a service portable and available in every environment. Any service of any environment will be available globally.
- *Wearable Computers*: Wearable computers can be worn by humans like a hat, shoe or clothes (these are wearable accessories). Wearable computers need to have some additional attributes compared to standard mobile devices. Wearable computers are always on; operational while on the move; hands-free, context-aware (with different types of sensors). Wearable computers need to be equipped with proactive attention and notifications. The ultimate wearable computers will have sensors implanted in the body and supposedly integrate with the human nervous system. These are part of a new discipline of research categorized by “Cyborg” (Cyber Organism).

1.3.1 Mobile Computing Functions

We can define a computing environment as mobile if it supports one or more of the following characteristics:

- *User Mobility*: The user should be able to move from one physical location to another and use the same service. The service could be in a home or remote network. For example, a user moves from London to New York and uses Internet to access the corporate application the same way the user uses it in the home office.
- *Network Mobility*: Network mobility deals with two types of use-cases. In one use-case, the user is moving from one network to another and uses the same service seamlessly. An example could be a user moving from a WiFi network within the university campus and changing to

3G network outside while using the same online service.

In other use-case of network mobility, the network itself is mobile like in a Mobile Ad hoc Network (MANET). In MANET, each node in the network is a combination of a host and a router. As the nodes move, the routers within the network also move changing the routing table structure. These types of networks are used in battlefields or sensor networks, where routers/nodes are constantly moving.

- **Bearer Mobility:** The user should be able to move from one bearer to another and use the same service. An example could be a user using a service through WAP bearer in his home network in Bangalore. He moves to Coimbatore where WAP is not supported and switches over to the voice or SMS (short message service) bearer to access the same application.
- **Device Mobility:** The user should be able to move from one device to another and use the same service. An example could be sales representatives using their desktop computer in their home office. During the day while they are on the street they would like to use their Palmtop to access the application.
- **Session Mobility:** A user session should be able to move from one user-agent environment to another. An example could be a user using his service through a CDMA (Code Division Multiple Access) 1X network. The user entered into the basement to park the car and got disconnected from his CDMA network. He goes to his home office and starts using the desktop. The unfinished session in the CDMA device moves from the mobile device to the desktop computer.
- **Agent Mobility:** The user-agent or the applications should be able to move from one node to another. Examples could be aglets, crawler software, or even a malicious worm or virus software that moves from one node to another. There is another use-case of mobile agent in the Cloud Computing paradigm, where applications will be moving from platform to platform and infrastructure to infrastructure depending on temporal and economic considerations. In Cloud Computing, there will not be any fixed association between the application and the host running it—software agents in the cloud will constantly be mobile.
- **Host Mobility:** The user device can be either a client or server. When it is a server or host, some of the complexities change. In case of host mobility, mobility of the IP needs to be taken care of.

The mobile computing functions can be logically divided into the following major segments (Fig. 1.1):

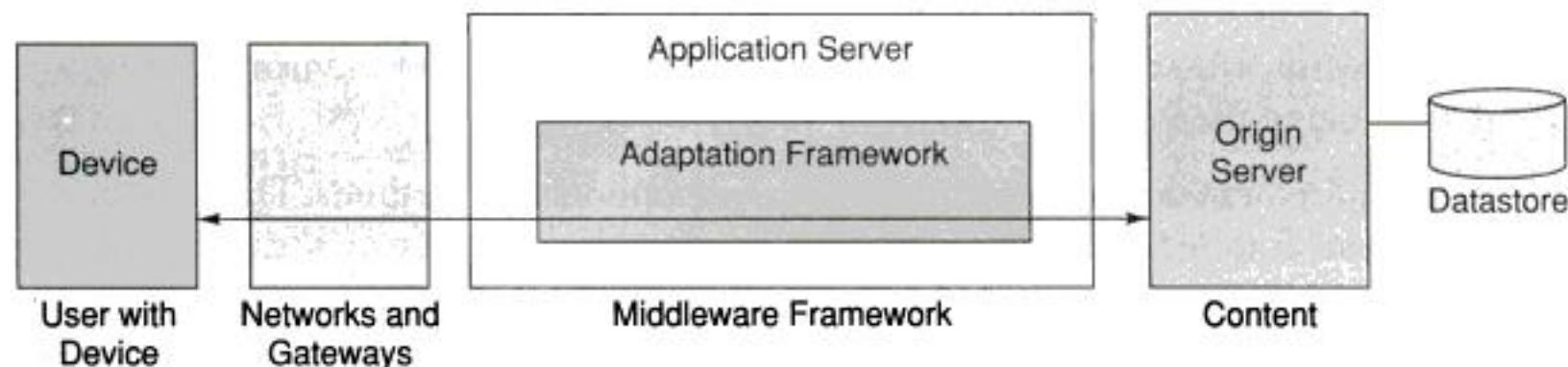


Figure 1.1 Mobile Computing Functions

1. *User with device*: This means that this could be a fixed device like a desktop computer in an office or a portable device like mobile phone. Example: laptop computers, desktop computers, fixed telephone, mobile phones, digital TV with set-top box, palmtop computers, pocket PCs, two-way pagers, handheld terminals, etc.
2. *Network*: Whenever a user is mobile, he will use different networks at different locations at different times. Example: GSM, CDMA, iMode, Ethernet, Wireless LAN, Bluetooth, etc.
3. *Gateway*: This acts as an interface between different transport bearers. These gateways convert one specific transport bearer to another. Example: From a fixed phone (with voice interface) we access a service by pressing different keys on the telephone. These keys generate DTMF (Dual Tone Multi Frequency) signals. These analog signals are converted into digital data by the IVR (Interactive Voice Response) gateway to interface with a computer application. Other examples will be WAP gateway, SMS gateway, etc.
4. *Middleware*: This is more of a function rather than a separate visible node. In the present context, middleware handles the presentation and rendering of the content on a particular device. It may optionally also handle the security and personalization for different users.
5. *Content*: This is the domain where the origin server and content is. This could be an application, system, or even an aggregation of systems. The content can be mass market, personal or corporate content. The origin server will have some means of accessing the database and storage devices.

1.3.2 Mobile Computing Devices

The device for mobile computing can be either a computing or a communication device. In the computing device category it can be a desktop, laptop, or a palmtop computer. On the communication device side it can be a fixed line telephone, a mobile telephone or a digital TV. Usage of these devices are becoming more and more integrated into a task flow where fixed and mobile, computing and communication functions are used together. The device is a combination of hardware and software; the hardware is technically called the User Equipment (UE) with software inside, which functions as an agent to connect to the remote service—this software is called a User Agent (UA). One of the most common UA today is a Web browser. When computing technology is embedded into equipment, Human-Computer Interaction (HCI) plays a critical role in effectiveness, efficiency, and user experience. This is particularly true as mobile information and communication devices are becoming smaller and more restricted with respect to information presentation, data entry and dialogue control. The human computer interface challenges are:

1. Interaction must be consistent from one device to another.
2. Interaction must be appropriate for the particular device and environment in which the system is being used.

Note: The requirement does not call for identical metaphors and methods. The desktop computer allows for different interaction techniques than a palmtop computer or a digital TV. Using the keyboard and a mouse may be appropriate for the desktop computer. Using the pen may be appropriate for the palmtop or Tablet PC. Microphones and speakers may be appropriate for a fixed or mobile phone. A remote control on the other hand will be more desirable for a digital TV.

1.4 DIALOGUE CONTROL

In any communication there are two types of user dialogues. These are long session-oriented transactions and short sessionless transactions. An example of a session-oriented transaction is: Reading a few pages from one chapter of a book at a time. Going to a particular page directly through an index and reading a particular topic can be considered a short sessionless transaction. Selection of the transaction mode will depend on the type of device we use. A session may be helpful in case of services offered through computers with large screens and mouse. For devices with limited input/output like SMS for instance, short sessionless transactions may be desired.

For example, consider enquiring about your bank balance over the Internet. In case of Internet banking through a desktop computer, the user has to go through the following minimum dialogues:

1. Enter the URL of the bank site.
2. Enter the account number/password and login into the application.
3. Select the balance enquiry dialogue and see the balance.
4. Logout from Internet banking.

This example is a session-oriented transaction. Using short sessionless transactions, the same objective can be met through a single dialogue. In a short sessionless transaction, the user sends an SMS message, 'mybal' to the system and receives the information on balance. The application services all the five dialogue steps as one dialogue. In this case steps like authentication and selection of transactions need to be performed in smarter ways. For example, user authentication will be done through the user's mobile number. It can be assumed that mobile devices are personal, therefore, authenticating the mobile phone implies authenticating the user account.

1.5 NETWORKS

Mobile computing will use different types of networks. These can be fixed telephone networks, GSM, GPRS, ATM (Asynchronous Transfer Mode), Frame Relay, ISDN (Integrated Service Digital Network), CDMA, CDPD (Cellular Digital Packet Data), DSL (Digital Subscriber Loop), Dial-up, WiFi (Wireless Fidelity), 802.11, Bluetooth, Ethernet, Broadband, etc.

1.5.1 Wireline Networks

This is a network, which is designed over wire or tangible conductors. This network is called fixedline or wireline network. Fixed telephone networks over copper and fiber-optic will be part of this network family. Broadband networks over Digital Subscriber Line (DSL) or cable will also be part of wireline networks. Wireline networks are generally public networks and cover wide areas. Though microwave or satellite networks do not use wire, when a telephone network uses microwave or satellite as part of its longhaul transmission infrastructure, it is considered part of wireline networks. When we connect to Internet Service Providers (ISP), it is generally a wireline network. The Internet backbone is a wireline network as well.

1.5.2 Wireless Networks

Mobile networks are called wireless network. These include wireless networks used by radio taxis, one-way and two-way pager, cellular phones. Examples will be PCS (Personal Cellular System), AMPS (Advanced Mobile Phone System), GSM, CDMA, DoCoMo, GPRS, etc. WiLL (Wireless in Local Loop) networks using different types of technologies are part of wireless networks as well. In a wireless network the last mile is wireless and works over radio interface. In a wireless network, other than the radio interface, rest of the network is wireline and is generally called the PLMN (Public Land Mobile Network).

1.5.3 Ad hoc Networks

In Latin, *ad hoc* means “for this purpose only”. An ad hoc (or spontaneous) network is a small area network, especially one with wireless or temporary plug-in connections. In these networks some of the devices are part of the network only for the duration of a communication session. An ad hoc network is also formed when mobile or portable devices operate in close proximity to each other or with the rest of the network. When we beam a business card from our PDA (Personal Digital Assistant) to another, or use an IrDA port to print documents from our laptop, we have formed an ad hoc network. The term ad hoc has been applied to networks in which new devices can be quickly added using, for example, Bluetooth or wireless LAN (802.11). In these networks, devices communicate with the computer and other devices through wireless transmission. Typically based on short-range wireless technology, these networks don't require subscription services or carrier networks.

1.5.4 Bearers

For different type of networks, there are different types of transport bearers. These can be TCP/IP, HTTP, protocols or dial-up connection. For GSM it could be SMS, USSD (Unstructured Supplementary Service Data) or WAP. For mobile or fixed phone, it will be Voice.

1.6 MIDDLEWARE AND GATEWAYS

Any software layered between a user application and operating system is a middleware. Middleware examples are communication middleware, object-oriented middleware, message-oriented middleware, transaction processing middleware, database middleware, behavior management middleware, Remote Procedure Call (RPC) middleware, etc. There are some middleware components like behavior management middleware, which can be a layer between the client device and the application. In a mobile computing context we need different types of middleware components and gateways at different layers of the architecture (Fig. 1.2). These are:

1. Communication middleware.
2. Transaction processing middleware.
3. Behavior management middleware.
4. Communication gateways.

1.6.1 Communication Middleware

The application will communicate with different nodes and services through different communication middleware. Different connectors for different services will fall in this category. Examples could be TN3270 for IBM mainframe services, or Javamail connector for IMAP or POP3 services.

1.6.2 Transaction Processing Middleware

In many cases a service will offer session-oriented dialogue (SoD). For a session we need to maintain a state over the stateless Internet. This is done through an application server. The user may be using a device, which demands a sessionless dialogue (SID) made of short sessionless transactions whereas the service at the backend offers a SoD. In such cases a separate middleware component will be required to convert a SoD to a SID. Management of the Web components will be handled by this middleware as well.

1.6.3 Behavior Management Middleware

Different devices deliver differently. We can have applications which are developed specially to deliver in a certain manner. For example, we can have one application for the Web, another for WAP, and a different one for SMS. On the contrary, we may choose to have a middleware, which will manage device-specific rendering at run-time. This middleware will identify the device properly and handle all device-specific rendering independent of the application. The system may be required to have some context awareness, which will be handled by the behavior management middleware.

1.6.4 Communication Gateways

Between the device and the middleware there will be a system of networks. Gateways are deployed when there are different transport bearers or networks with dissimilar protocols. For example, we need an IVR gateway to interface Voice with a computer, or a WAP gateway to access Internet over a mobile phone.

Figure 1.2 presents a schematic diagram of services in a mobile computing environment with different devices providing different services.

1.7 APPLICATION AND SERVICES (CONTENTS)

Data and information, through mobile computing services, are required by all people regardless of their mobility. Mobile users include people like mobile executives, sales people, service engineers, farmers in the field, milkmen, newspaper boys, courier or pizza delivery boy. Logically, everyone is a mobile user at some time or the other in life. For people who are stationary, mobile computing becomes necessary outside office hours. For example, we may need to do a bank transaction from home at night or respond to an urgent mail while at home.

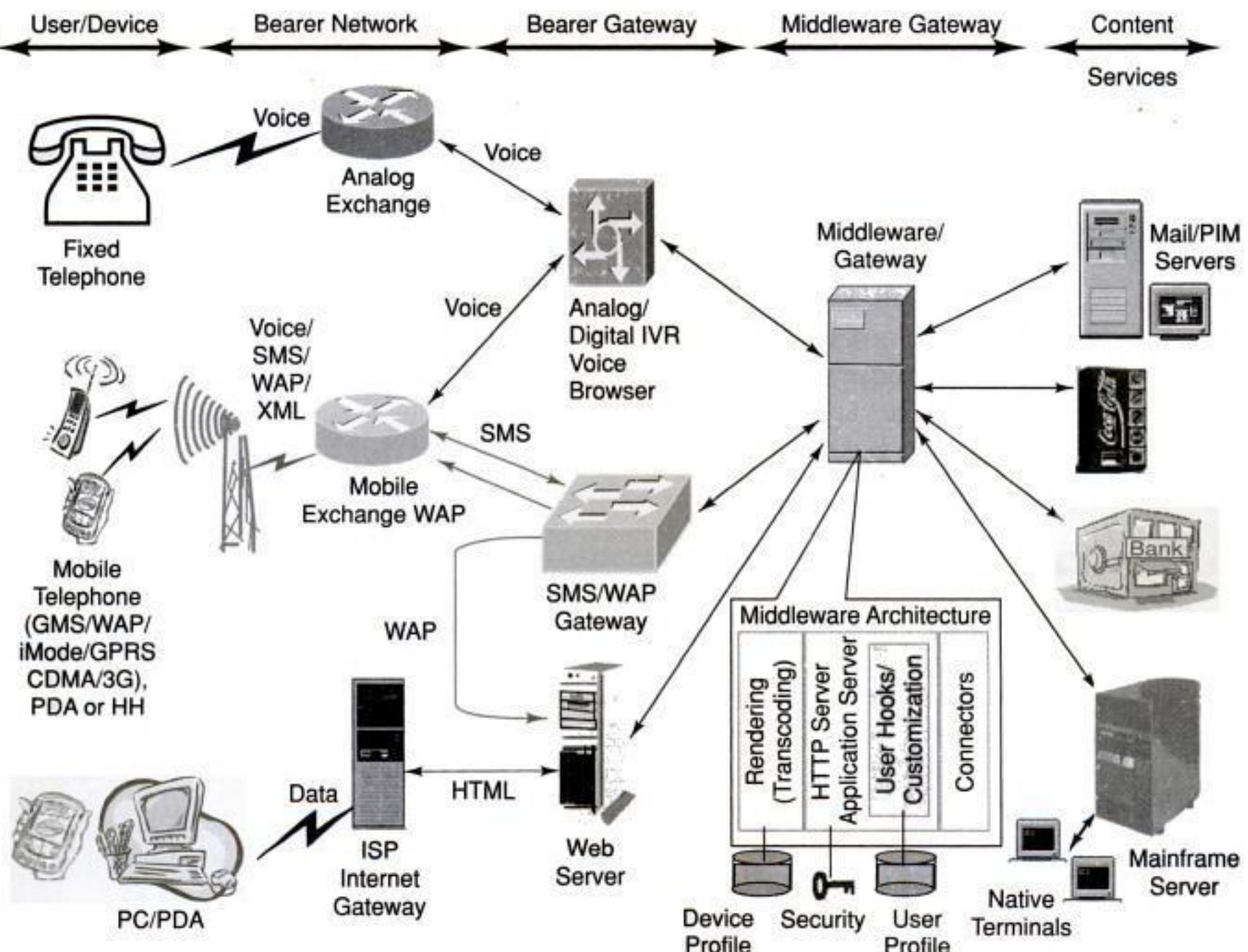


Figure 1.2 Schematic Representation of a Mobile Computing Environment

There can be many applications and services for the mobile computing space. These applications or services run on the origin server. These are also known as content servers. Content will primarily be lifestyle-specific. An individual has different lifestyles in different social environments. Also, lifestyles change during the day. One individual can be an executive needing the corporate MIS (Management Information System) application during the day while at home the same individual can use applications related to lifestyle or entertainment. The list of possible mobile applications can never be complete. On the basis of life styles, they can be grouped into different categories, such as:

Personal: Belongs to the user (wallet, medical records, diary).

Perishable: Time-sensitive and of relevance and passes quickly (general news, breaking news, weather, sports, business news, stock quotes).

Transaction-oriented: Transactions need to be closed (bank transactions, utility bill payment, mobile shopping).

Location-specific: Information related to current geographical location (street direction map, restaurant guide).

Corporate: Corporate business information {mail, Enterprise Requirements Planning (ERP), inventory, directory, business alerts, reminders}.

Entertainment: Applications for fun, entertainment. Social networking sites like Facebook can be part of this category.

Here are some examples:

News: This is a very big basket of applications having different types of news. News could be political, current affairs, breaking news, business news, sports news, community news, etc. While people are on the move, they can always be connected to their culture and community through news, using mobile computing.

Youth: This is a very high growth market with different applications to suit the lifestyles of the youth. These are primarily message-based applications like person-to-person messaging, chat, forums, dating, etc.

Weather: There are different types of applications and services where mobile computing can make a difference. Notification services on weather is a very sought after application. If we have access to information related to the weather while on vacation or while driving from one location to another then the global positioning system (GPS) can help locate a person or sometimes save lives in case of a natural calamity.

Corporate application: Standard corporate information is an important piece of information for mobile workers and includes corporate mail, address book, appointments, MIS applications, corporate Intranet, corporate ERP, etc.

Sales force automation: This group will offer many applications. It will cater to the large population of sales personnel. Applications will include sales order bookings, inventory enquiry, shipment tracking, logistics related applications, etc. These applications will be very effective over wireless devices.

m-broker: Getting correct and timely information related to different stocks are very important. Also, online trading of stocks while on the move is quite critical for certain lifestyles. Stock tickers, stock alerts, stock quotes, and stock trading can be made ubiquitous so that users can check their portfolio and play an active role in the market.

Telebanking: We need to access our bank information for different transactions. Earlier, people used to go to the bank, but things are changing. Banks are coming to customers through telebanking. If telebanking can be made ubiquitous it helps the customer as well as the bank. Many banks in India are today offering banking over Internet (web), voice and mobile phones through SMS.

m-shopping: This mobile application is used to shop with the help of mobile devices like Palm top, Pocket PC, mobile phones, etc. You can use this application to pay for a soft drink or soda from a vending machine in an airport or a movie theatre using a mobile phone, especially when you do not have sufficient cash.

Micropayment-based application: Micropayments involve transactions where the amount of money involved is not very high—it could be a maximum of Rs 1000 (\$ 25) or so. Micropayment through mobile phones can help rural people to do business effectively.

Interactive games: Many mobile network operators have started offering different types of contests and interactive games that can be played through mobile phones. The applications could be similar to any quiz, housie, etc.

Interactive TV shows: Many TV companies around the world use email, SMS and Voice as a bearer for interactive TV or reality TV shows. In these shows viewers are encouraged to participate by asking questions, sharing opinions or even answering different quizzes. Nowadays viewers vote for their favorite TV stars using SMS.

Digital/Interactive TV: These are interactive TV programs through digital TV using set-top boxes and Internet. Video-on-demand, community programs, healthcare, and shopping applications are quite popular under this media category.

Experts on call: This is an application system for experts. Experts use these services to schedule their time and business with clients; clients use this to schedule business with the expert. A typical example could be to fix up an appointment with the tax consultant.

GPS-based systems: Applications related to location tracking come under this category. This could be a simple service like tracking a vehicle. Another example could be tracking an individual who got stuck due to bad weather while on a trekking trip. Fleet management companies and locations-aware software systems need GPS-based applications.

Remote monitoring: This is important for children at home where parents monitor where their children are or what are they doing. Also, monitoring and controlling of home appliances will be part of this application.

Entertainment: This contains a very large basket of applications starting from horoscope to jokes. Many people in some parts of Asia decide their day based on the planetary positions and horoscope information.

Directory services: This includes information related to movies, theatre, public telephones, restaurant guide, public information systems and Yellow pages.

Sports: This service offers online sports updates. In India live cricket score is the most popular mobile computing application. Getting scores of a live cricket match is the most popular mobile computer application. This service is available in India through Web, Voice, SMS, and WAP.

Maps/navigation guide: This is an application which has a lot of demand for traveling individuals. These services need to be location-aware to guide the user to use the most optimum path to reach a destination. The directions given by these applications also take traffic congestion, one way, etc., into consideration. GPS-based driving is becoming very popular in the US and advanced countries, where a user enters the postal address of the destination. The GPS-based system calculates the route, loads the right map and helps the driver navigate in real-time.

Virtual office: There are many people who are self-employed and do not have a physical office. Thus mobile and virtual office where they can check their mails, schedules, appointments, etc., while they are on the move are a must for them. Insurance agents and many other professions need these types of services.

m-exchange for industries: Manufacturing industry exchange from a mobile device can be a very cost effective solution for small/cottage industries. It may not be possible for a cottage industry to invest in a computer. However, accessing an exchange for a manufacturing company through a SMS may be affordable.

m-exchange for agricultural produce: Exchange for farmers on different type of agricultural products can be very useful for countries like India. If farmers can get information about where to get a good price for their product, it helps both farmers and consumers. There is a system www.echoupal.com to do exactly this. Think of this available over mobile phones.

Applications for speech/hearing challenged people: Telecommunication always meant communicating through Voice. There are people who cannot speak or hear. These include people with disabilities and senior citizens who lost their speech due to old age or after suffering a stroke. Text-based communication can help rehabilitate some of these disabled individuals.

Agricultural information: Think about a case where a farmer receives an alert in his local language through his mobile phone and immediately knows that the moisture content in air is 74%. He can then decide how much to water his harvest. This can save his money, the harvest (excess water is sometimes harmful), and the scarce water resource. Portable devices with voice interface can change the economics of rural India with this kind of application.

Corporate knowledge-based applications: Many corporates today have a knowledge base. Making this ubiquitous can reduce cost and increase productivity.

Community knowledge-based applications: Knowledge is equally important for a community. Making knowledge ubiquitous always help society.

Distance learning: Applications related to distance learning are a must for countries with limited or no access to digital and information technology. For virtual schools in Asia or Africa, it is possible to have access to good faculty through the distance learning mode.

Digital library: These are libraries which can be accessed from anywhere anytime because of the Internet. Digital libraries can go a long way in shortening the digital divide as they also have support of local language and are easy and cheaper to commission.

Telemedicine and healthcare: Making telemedicine and healthcare easily available can save many lives. For example, a person complains of chest pain while traveling and requires immediate medical attention. He has to be taken to a doctor in a remote town. In this case, access to the patient's record can help expedite diagnosis. Reminder services for medicines or checkups can be very useful. In rural India, virtual clinics can help those who otherwise do not have access to medical care.

Micro-credit schemes: Micro-credit has a distinct role to play for a country's microeconomy. Grameen Bank with all its applications in Bangladesh is the best example of micro-credit.

Environmental protection and management: Ubiquity is a must for applications on environmental protection and management. Applications related to industrial hygiene will be part of this category.

e-governance: These applications are very important to bridge the digital divide. The Bhoomi project of Karnataka government has computerized 20 million land records of 0.67 million farmers living in 30,000 villages in the state. Many such projects of the government can be made electronic, resulting in better and faster access to information managed by the government.

Virtual laboratories: There are many laboratories and knowledge repositories around the world which are made accessible to various cultures and countries through digital and information technology.

Community forums: There are different social and community meetings. In the case of India, panchayats can be made electronic. These may help increase the involvement of more people in community development work.

Law enforcements: Most of the time law enforcement staff are on the streets and need access to different types of services through wireless methods. These may be access to criminal records, information related to vehicles, or even a picture of the accident site taken through a MMS phone. This information can help insurance companies to resolve the claim faster.

Job facilitator: These could be either proactive alerts or information related to jobs and employment opportunities.

Telemetric applications: Almost every industry and sphere of life has the need for telemetric applications. Examples could be monitoring and control in manufacturing industry; vehicle tracking; meter reading; health care and emergency services; vending machine monitoring; research (telemetric orthodontic); control and service request for different emergency services for utilities like power plants, etc.

Downloads: Different types of downloads starting from ring tones to pictures are part of this category. In many countries this type of application is very popular. It is estimated that the market for ring tone downloads is more than 1 billion dollars.

Alerts and notifications: This can be either business or personal alerts. Simple examples could be breaking news alerts from a newspaper. Complex examples of alert could be for a doctor when the patient is in critical condition. In India many mobile operators are offering cricket alerts. In this service, subscribers receive score information every 15 minutes, about every wicket fall!

1.8 DEVELOPING MOBILE COMPUTING APPLICATIONS

Any portal system today supports user mobility. If I have an Internet mail account like Google-mail or Yahoo-mail, I can access my mail from anywhere. I need a desktop or laptop computer to access my mailbox. I may not be able to access the same mail through some other device like a fixed phone. There are a number of factors that make mobile computing different from desktop computing. As a result of mobility, the attributes associated with devices, network, and users are constantly changing. These changes imply that the context and behavior of applications need to be adapted to suit the current environment. Context and behavior adaptation are required to provide a service that is tailored to the user's present situation. There are several ways in which

context and behavior can be adapted. One way is to build applications without any context or behavior awareness. Context and behavior adaptation will be handled by a behavior management middleware at runtime. Another option is to build different applications specific to different context and behavior patterns. There could be some system in the organization, which was originally developed 15 years ago for some direct connected terminals like VT52. Due to change in market expectation these systems need to be made mobile. Complexities involved in making an existing application mobile versus developing a new mobile system will be different. For a new application it is possible to embed the behavior within the application. However, for a long-life system or a legacy application the content behavior adaptation will need to be done externally.

1.8.1 New Mobile Applications

Let us assume that in a bank, some new applications need to be built for e-Commerce. The bank wants to offer banking through Voice (telephone) and Web (Internet). Assuming that the bank already has a computerized system in place, the bank will develop two new applications. One will handle the telephone interface through Interactive Voice Response (IVR) and the other through Web. At a later point in time, if the bank decides to offer SMS and WAP, they will develop two new applications to support SMS and WAP interfaces respectively. To protect the investment and quick adaptation, the bank may decide to use transaction processing middleware and RPC middleware. All these are possible only if it is a fresh applications development.

1.8.2 Making Legacy Application Mobile

How do we make an existing legacy application which has been functioning for long mobile? We define an application as legacy if it has one or more of the following characteristics:

1. It has moved into the sustenance phase in the software development lifecycle.
2. It cannot be modified. This could be due to unavailability of the original development platforms, unavailability of original source code or unavailability of expertise to make the necessary changes.
3. It is a products and packaged software where enterprise does not have any control. This could be due to high cost of ownership for the new upgrade or the vendor does not have any plan to support the new requirement.

Let us assume that an enterprise has licensed an ERP system from an external vendor. The enterprise wants to offer a notification of yesterday's sales figures to some select executives at 9:30 a.m. every morning through SMS. The ERP vendor plans to offer a similar function in its next release six months down the line. The license fee for the next upgrade will be very expensive. Another example is that a wireless network operator wants to offer enterprise mails through its network. In all such cases the adaptation will be done without changing the base product. This requires a framework that attempts to perform most of the adaptation dynamically. Content and behavior management will be managed real-time through a behavior management middleware.

1.9 SECURITY IN MOBILE COMPUTING

Security issues in mobile computing environment pose a special challenge. This is because we have to offer services over the air using networks over which we do not have any control. All the infrastructure and technology designed by GSM and other forums are primarily to increase the revenue of the network operators. This makes the technology complex and very much dependent on the network operator. For example, the SMS technology is operator centric; WAP requires WAP gateway. These gateways are installed in the operator's network and managed by the operator. The security policy implemented by the network operator depends on the operator's priority and revenue generation potential and not on the need of the content provider.

In a mobile computing environment, the user can move from one network to another, one device to another or one bearer to another. Therefore, theoretically the security implementations need to be device independent, network independent, bearer independent, and so on. The requirement is to arrive at a security model, which can offer homogenous end-to-end security.

1.10 STANDARDS—WHY ARE THEY NECESSARY?

Standards are documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines or definitions of characteristics. Standards ensure that materials, products, processes and services are fit for their defined and agreed purpose. A standard begins as a technical contribution, which is supported by a number of interested parties to the extent that they indicate their willingness to participate in the standard's development. Standards are available for experts to challenge, examine and validate. No industry in today's world can truly claim to be completely independent of components, products, and rules of application that have been developed in other sectors. Without standards, interoperability of goods and services will not be possible.

When the proposed standard or technical document is near completion, the formulating engineering committee circulates the draft of the document for a ballot. The purpose of this ballot is to identify any unresolved issues and to establish consensus within the formulating group. Every effort is made to address and resolve the comments received.

The opposite of standard is proprietary. Proprietary systems for similar technologies are seen as technical barriers to trade and competition. Today's free-market economies increasingly encourage diverse sources of supply and provide opportunities for expanding markets. On the technology front, fair competition needs to be based on identifiable and clearly defined common references that are recognized from one country to another, and from one region to the next. An industry-wide standard, internationally recognized, developed by consensus among trading partners, serves as the language of trade.

There are some fundamental differences between how the US and Europe adapt technology. In the US, market force and time to market drive the technology. Interoperability has always been the primary issue in Europe. Therefore, in Europe, standards drive the adaptation of technology. This is one of the reasons why the US has more proprietary systems compared to Europe.

1.10.1 Who Makes the Standards?

There are many institutes that generate and provide standards across the world. There are standard bodies at the regional, country as well as international level. Based on the area of operations, standard bodies are formed by the governments, professional institutes or industry consortiums. These standard bodies sometimes also function as regulators. In India there is a standard body under the Government of India, which is called Bureau of Indian Standard or simply BIS (www.bis.org.in). A standards process include the following steps:

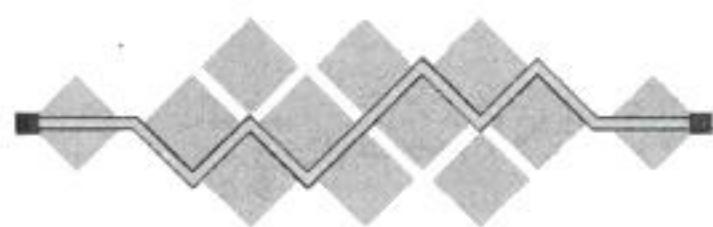
1. Consensus on a proposed standard by a group or “consensus body” that includes representatives from materially affected and interested parties.
2. Broad-based public review and comments on draft standards.
3. Consideration of and response to the comments submitted by voting members of the relevant consensus body and by public review commenters.
4. Incorporation of approved changes in a draft standard.
5. Right to appeal by any participant who believes that due process principles were not sufficiently respected during the standards development in accordance with the ANSI-accredited procedures of the standards developer.

1.11 STANDARDS BODIES

The International Organization for Standardization (ISO) (<http://www.iso.ch>) is a worldwide federation of national standards bodies from more than 140 countries, one from each country. ISO is a non-governmental organization established in 1947. The mission of ISO is to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity. Though ISO is commonly believed as the acronym for International Standard Organization, in fact the word “ISO” is derived from the Greek *isos*, meaning “equal”. Sometimes ISO makes its own standard or it adapts standards from its member organizations. The adapted standard is then made an international one by ISO. One of the most widely known standard from ISO is ISO 9000. ISO 9000 relates to software quality. The famous 7-layer model for Open System Interconnection (OSI) is ISO standard (ISO 7498). For information security ISO has come up with the recommendation ISO 17799.



International
Organization for
Standardization



I E T F®

Internet Engineering Task Force (IETF) (<http://www.ietf.org>) is the standard-making body for Internet and related technologies. IETF is an open international community of network designers, operators, vendors and researchers concerned with the evolution of Internet architecture and smooth operation of the Internet. It is open to any individual. The actual technical work of the IETF is done in its working groups. Working groups are

organized into several areas by topic (e.g., routing, transport, security, etc.). The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of a unique IP address. The IANA is chartered by the Internet Society (ISOC) to act as the clearing house to assign and coordinate the use of numerous Internet protocol parameters. Standards defined by IETF are called Request For Comment or RFC. The standard for email is defined in RFC821 (Simple Mail Transfer Protocol or SMTP); RFC2616 describes the version 1.1 of Hypertext Transfer Protocol (HTTP/1.1).

ETSI (the European Telecommunications Standards Institute) (<http://www.etsi.org>) is an organization whose mission is to produce telecommunications standards that will be used for decades to come throughout Europe and possibly beyond. ETSI unites members from countries inside and outside of Europe, and represents regulators, network operators, manufacturers, service providers, research bodies and users. ETSI plays a major role in developing a wide range of standards and other technical documentation as Europe's contribution to world-wide standardization in telecommunications, broadcasting and information technology. ETSI's prime objective is to support global harmonization by providing a forum in which all the key players can contribute actively. ETSI is officially recognized by the European Commission. GSM Standard is created, maintained and managed by a committee within ETSI. GSM standards document GSM 01.04 (ETR 350): 'Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms'. GSM 12.13 standard defines the interface digital cellular telecommunications system (Phase 2+); Man-Machine Interface (MMI) of the Mobile Station (MS) (GSM 02.30 version 7.1.0 Release 1998).



OMA and WAP Forum (<http://www.wapforum.org>) (<http://www.openmobilealliance.org>): The Open Mobile Alliance (OMA) has been established by the consolidation of the WAP Forum and the Open Mobile Architecture initiative. It intends to expand the market for the entire industry by removing barriers to interoperability and supporting a seamless and easy-to-use mobile experience for end users. The Open Mobile Alliance encourages competition through innovation and differentiation, while ensuring the interoperability of mobile services through the entire value chain. The supporters of the Open Mobile Alliance recognize the significant industry benefits of creating a standards organization that will include all elements of the wireless value chain, and contribute to timely and efficient introduction of services and applications to the market. WAP and MMS standards are created, maintained, and managed by OMA.

ITU (International Telecommunication Union) (www.itu.int) is an organization within the United Nations System. It was founded on the principle of cooperation between governments and the private sector. With a membership encompassing telecommunication policy-makers and regulators, network operators, equipment manufacturers, hardware and software developers, regional standards-making organizations and financing institutions, ITU's activities, policies and strategic direction are determined and shaped by the industry it serves. ITU has three sectors of the Union; they are Radio communication (ITU-R), Telecommunication Standardization (ITU-T), and



Telecommunication Development (ITU-D). Their activities cover all aspects of telecommunication, from setting standards that facilitate seamless interworking of equipment and systems to adopting operational procedures for the wireless services, and designing programs to improve telecommunication infrastructure. ITU Telecommunication Standardization Sector (ITU-T)'s mission is to ensure an efficient and on-time production of high quality standards (recommendations) covering all fields of telecommunications. ITU-T was founded in 1993, replacing the former International Telegraph and Telephone Consultative Committee (CCITT) whose origins go back to 1865. Any telephone in this world has a unique number (technically known as global title). These numbering schemes are defined through the ITU-T standards E.164.



IEEE Standards Association (IEEE-SA) (<http://standards.ieee.org>) is an organization that produces standards, which are developed and used internationally. While the IEEE-SA focuses considerable resources on the long-respected full consensus standards process carried out by the standards

committees and IEEE societies, the IEEE-SA pioneers new and innovative programs to increase the value of IEEE standards to members, industry, and the global society. IEEE-SA members continue to set the pace for the development of standards products, technical reports and documentation that ensure sound engineering practices worldwide. IEEE-SA demonstrates strong support of an industry-led consensus process for the development of standards and operating procedures and guidelines. Standards for Wireless LAN are created, maintained and managed by IEEE. These are defined through different 802.11 standards.

The Electronic Industries Alliance (EIA) (<http://www.eia.org>) is a national trade organization within the US that includes the full spectrum of its electronics industry. The Alliance is a partnership of electronic and high-tech associations and companies whose mission is promoting the market development and competitiveness of the US high-tech industry through domestic and international policy efforts. EIA comprises companies whose products and services range from the smallest electronic components to the most complex systems used by defense and space and industry, including the full range of consumer electronic products. The progressive structure of the Alliance enables each sector association to preserve unique autonomy while uniting for a common cause under EIA. One of the most commonly used EIA standard is EIA RS-232. This is a standard for the 25-pin connector between a computer and a modem.



World Wide Web Consortium (W3C) (<http://www.w3.org>) develops interoperable technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential. W3C is a forum for information, commerce, communication and collective understanding. By promoting interoperability and encouraging an open forum for discussion, W3C is committed to leading the technical evolution of the Web. To meet the growing expectations of users and increasing power of machines, W3C is already laying the foundations for the next generation of the Web. W3C's technologies will help make the Web a robust, scalable and adaptive infrastructure for a world of information. W3C contributes to efforts to standardize Web technologies by producing specifications (called



recommendations) that describe the building blocks of the Web. W3C recommendations include HTML, XML, CSS (Cascading Style Sheet), Web Services, DOM (Document Object Model), MathML (Maths Markup Language), PNG (Portable Network Graphics), SVG (Scalable Vector Graphics), RDF (Resource Description Framework), P3P (Platform for Privacy Preferences), etc.



A GLOBAL INITIATIVE

3GPP (<http://www.3gpp.org>) is to produce globally applicable technical specifications and technical reports for 3rd Generation Mobile System based on evolved GSM core networks and radio access technologies that they support, i.e., Universal Terrestrial Radio Access (UTRA) both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes. The scope was subsequently amended to include maintenance and development of the Global System for Mobile communication (GSM) technical specifications and technical reports including evolved radio access technologies (e.g., General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE)).

The American National Standards Institute (ANSI) (www.ansi.org) is the national standard organization in the United States. In many instances, the US standards are taken forward to ISO and IEC (International Electrotechnical Commission), where they are adapted in whole or in part as international standards. For this reason, ANSI plays an important part in creating international standards that support the worldwide sale of products, which prevent regions from using local standards to favor local industries. ANSI Standard X3.4-1968 defines the 'American National Standard Code for Information Interchange (ASCII)' character set. ASCII character set is used in almost every modern computer today. The same standard has also been adapted as ISO 8859-1 standard.



UMTS Forum

Universal Mobile Telecommunications System (UMTS) (www.umts-forum.org) represents an evolution in terms of services and data speeds from today's second-generation mobile networks like GSM. As a key member of the global family of third generation (3G) mobile technologies identified by the ITU, UMTS is the natural evolutionary choice for operators of GSM networks. Using fresh radio spectrum to support increased numbers of customers in line with industry forecasts of demand for data services over the next decade and beyond, UMTS is synonymous with a choice of WCDMA radio access technology that has already been selected by many licensees worldwide. UMTS-Forum is the standards-making body for WCDMA (Wideband Code Division Multiple Access) and UMTS technology.



Bluetooth (<http://www.bluetooth.com>) wireless technology is a worldwide specification for a small-form factor, low-cost radio solution that provides links between mobile computers, mobile phones, other portable handheld devices, and connectivity to the Internet. The standards and specification for Bluetooth are developed, published and promoted by the Bluetooth Special Interest Group.



The CDMA Development Group (CDG) (<http://www.cdg.org>) is an international consortium of companies who have joined together to lead the adoption and evolution of CDMA wireless systems around the world. The CDG comprises the world's leading CDMA service providers and manufacturers. By working together, the

members will help ensure interoperability among systems, while expediting the availability of CDMA technology to consumers.

The Public-Key Cryptography Standards (PKCS) (<http://www.rsasecurity.com/rsalabs/pkcs/>) are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography. First published in 1991 as a result of meetings with a small group of early adopters of public-key technology, the PKCS documents have become widely referenced and implemented. Contributions from the PKCS series have become part of many formal and de facto standards, including ANSI X9 documents, PKIX, SET, S/MIME and SSL (Secure Sockets Layer).

PAM Forum (<http://www.pamforum.org>). In the world of ubiquitous computing, knowing the position and context of a device is very important. The Presence and Availability Management (PAM) Forum is an independent consortium with a goal to accelerate the commercial deployment of targeted presence and availability applications and services that respect users' preferences, permissions and privacy. Working in partnership with industry participants, the PAM Forum defines a framework for the various standards and specifications needed for context/location aware applications.



Parlay Group (<http://www.parlay.org>). The Parlay Group is a multi-vendor consortium formed to develop open, technology-independent application programming interfaces (APIs). Parlay integrates intelligent network (IN) services with IT applications via a secure, measured, and billable interface. By releasing developers from underlying code, networks and environments, Parlay APIs allow for innovation within the enterprise. These new, portable, network-independent applications are connecting the IT and telecom worlds, generating new revenue streams for network operators, application service providers (ASPs), and independent software vendors (ISVs). Using Parlay APIs, one will be able to develop applications, which rely on network-related data like service provisioning. Parlay will also help develop location/context aware applications and services.

DECT (www.dect.org) stands for Digital Enhanced Cordless Communications. It is an ITSI standard for portable phones. DECT is known in ITU as a 3G system and is commonly referred to as IMT-FT (IMT Frequency Time).



WiMAX Forum (www.wimaxforum.org) is Worldwide Interoperability for Microwave Access Forum dedicated to certifying the operations of interconnecting devices. WiMAX aims to provide wireless data over long distances in different forms ranging from point-to-point links to full scale mobile access networks for wireless broadband communication. WiMAX Forum is the industry body that does the job of certification, promotion and producing interoperability specifications for WiMAX.



TTA (www.tta.or.kr/English/new/main/index.htm) is Telecommunications Technology Association. TTA is an IT standards organization catering to development of new standards based in Korea. It provides one-stop services for comprehensive IT standards.

Wi-Fi (www.wi-fi.org) owns trademark to Wi-Fi alliance. It was previously known as Wireless Ethernet Compatibility Alliance. It is focused on interoperability and compatibility of Wireless LAN devices and committed to continuous improvements in design and better user experience.



Association of Radio Industries and Businesses (ARIB) (www.arib.or.jp/english/) is an institution, based in Japan, dedicated to efficient use of radio spectrum and its implications in businesses.

China Communications Standards Association (CCSA) (www.ccsa.org.cn/english/) is an attempt of Chinese Ministry of IT to reform telecommunications industry and market. It aims to become a nationally unified standards organization in China.



Digital Living Network Alliance (DLNA) (www.dlna.org) is a cross-industry association of consumer electronics, computing industry and mobile device companies. The objective of DLNA is to establish a conglomeration of wired and wireless interoperable network of personal computers, consumer electronics and mobile devices in the home and outside in order to enable a seamless environment for sharing digital media content.

1.12 PLAYERS IN THE WIRELESS SPACE

In a wireless network there are many stakeholders. These are:

1. Regulatory authorities.
2. The operator or service provider.
3. The user or the subscriber.
4. Equipment vendors (network equipment and user device).
5. Research organizations.

In most parts of the world, the radio spectrums are regulated. Generally, a license is required to use a part of this spectrum. There are certain bands like ISM (Industry, Scientific and Medical) used by cordless telephones or microwave ovens or 802.11 which are unregulated. This means that if one develops equipment which needs to use these bands, then one need not go to the government and ask for permission to use them. However, for the regulated bands, one has to get a license before it can be used. GSM, CDMA etc., use frequency bands, which are regulated. Therefore, a network company offering these services, needs to get clearance from the government. Governments generally auction these spectrums to different network operators. The spectrums for 3G networks were auctioned in Europe for about 100 billion US Dollars. In India, the whole country was divided into metros and circles. The average license fee for GSM for these circles was in the tune of hundreds of crores of rupees.

Once the license is obtained, the network operator needs to conduct a detailed survey of the region with a plan for the cell sites. Cell site survey is very important and critical for any wireless network. Cell site survey is logically the design of the architecture of the network. During this phase the network operator determines the location of the base station and positioning of the cell. The location of a wireless base station tower will be determined by many factors; examples could be subscriber density, hills, and other obstacles. Similarly, for wireless LAN or WiFi, the location of AP (Access Points) will be determined by the layout of the building floor, concrete, glass walls, etc. A site survey is necessary for a wireless LAN as well before the APs are installed.

Cellular network operators need to create the infrastructure. There are a few equipment manufacturers who supply the hardware to the network operators. These hardware will be MSC (Mobile Switching Centre), BSC (Base Station Controller), BTS (Base Transceiver Station), and the Cells. Cells and BTSSs are spread across the region; however, MSCs and BSCs are generally installed under one roof commonly known as switching room. Some of the leading manufacturers of these hardware are Ericsson and Nokia in Europe; Motorola and Lucent in the US; Samsung in Asia.

To use a cellular network, we need a handset or device. There are different types of handsets available in the market today. All these devices offer voice and SMS as minimum, and range up to fancy handsets which offer WAP, MMS, J2ME or even digital cameras. Some of the leading suppliers of these handsets are Nokia, Sony Ericsson, Motorola, Samsung, LG, etc.

In GSM world, all these handsets contain a small piece of card known as SIM (Subscriber Identity Module). These are technically Smart Cards or processor cards with a small memory and an independent processor. The size of the memory ranges from 8K bytes to 64K bytes. They contain some secured data installed by the network operator related to the subscriber and the network. Some of the leading suppliers of SIM card are Gemplus, Schlumberger, Orga, etc.

When a person wants to subscribe to a cellular phone, he contacts a cellular operator. The subscriber is then registered with the network as a prepaid or postpaid subscriber. In a GSM network, the operator issues a SIM card to the subscriber that contains all relevant security information. The subscriber buys a handset and installs the SIM card inside the handset; however, in Europe and the US, in certain subscription plans the handset is bundled with the plan. A provisioning and activation needs to be done within the network for this new subscriber. During the provisioning, some of the databases within the operator will be updated. Once the databases for authentication and billing are completed, the subscriber is activated. Following the activation, the subscriber can use the network for making or receiving calls.

REFERENCES/FURTHER READING

1. 'An Investment Perspective' *UMTS Report*, Durlacher Research, www.durlacher.com.
2. 'Africa: The Impact of Mobile Phones, Moving the debate forward', *The Vodafone Policy Paper Series*, 2, March 2005.
3. Banks, Ken and Richard Burge, (2004), *Mobile Phones: An Appropriate Tool for Conservation and Development*, Fauna & Flora International, UK: Cambridge.
4. 'Enabling UMTS Third Generation Services and Applications', *UMTS Forum Report # 11*, October 2000, <http://www.umts-forum.org>.

5. Eyers, Dean, 'Telecom Markets and the Recession: An Imperfect Storm', *Gartner Report*, AV-14-9944, 27 November 2001.
6. Horrigan, John B., Senior Researcher, Lee Rainie, Director, (2002), 'Getting Serious Online', *Pew Internet & American Life Project Report*, March 2002.
7. Jhunjhunwala, Ashok, Bhaskar Ramamurthi, and Timothy A. Gonsalves, (1998), 'The Role of Technology in Telecom Expansion in India', *IEEE Communications Magazine*, November 1998.
8. Lewin David and Susan Sweet, 'The economic benefits of mobile services in India: A case study for the GSM Association', *OVUM*, CLM28, Version 1, January 2005.
9. McGraw, Alistair, Christophe de Hauwer, Tim Willey, and Adam Mantzos, 'Industry Analysis Wireless Data: The World in Your Hand, Arthur Andersen Technology.' *Media and Communications*, October 2000.
10. Milojicic, D., F. Douglis, and R. Wheeler, (Eds), (1999), *Mobility Processes, Computers, and Agents*, Addison-Wesley.
11. Talukder Asoke K., (2002), *Mobile Computing—Impact in Our Life, Harnessing and Managing Knowledge*, Chakravarthy, C.R., L.M. Pathak, T. Sabapathy, M.L. Ravi (Eds), 13, Tata McGraw-Hill.
12. 'The Future Mobile Market Global Trends and Developments with a Focus on Western Europe, *UMTS Forum Report # 8*, March 1999, <http://www.umtsforum.org>.
13. 'The Path Towards UMTS: Technologies for the Information Society', *UMTS Forum Report # 2*, 1998, <http://www.umts-forum.org>.

REVIEW QUESTIONS

- Q1: What are the essential functional differences between 1st generation, 2nd generation, and 3rd generation of networks?
- Q2: Describe what do you understand by Wireless PAN, Wireless LAN and Wireless MAN.
- Q3: What is an ISM band? Why is it called a free band?
- Q4: What are the characteristics of a mobile computing environment?
- Q5: Give examples for five mobile computing applications.
- Q6: What are the advantages and disadvantages of standards? Name the standard committees responsible for 3G?
- Q7: Describe the variants of Mobile Computing.
- Q8: Describe the various aspects of mobility with respect to Mobile Computing.
- Q9: What should be the characteristics of Mobile Computing devices?
- Q10: How should dialogues be controlled for communication in a Mobile Computing environment?
- Q11: Briefly describe the following networks with example and applications:
 - (a) Wired networks
 - (b) Wireless networks
 - (c) Ad hoc networks

- Q12: What are the differences between middleware and gateways? Enunciate with examples in the context of Mobile Computing?
- Q13: How would you broadly classify Mobile Computing applications?
- Q14: Describe the design of Mobile Computing applications using at least two transport communication bearers. Make assumptions, if required.
- Q15: How could one achieve the migration of legacy application to it being mobile?
- Q16: Who are the players in wireless space? Explain the role of each of them assuming you are going to launch a mobile computing application in the commercial domain and what should you be prepared with when tackling them.

CHAPTER 2

Mobile Computing Architecture

2.1 HISTORY OF COMPUTERS

Nothing has changed the world around us the way digital technology and computers have. Computers have entered every aspect of our life and the environment around us. The origin of computers can be traced back to thousands of years. Though different forms of computers were in existence for centuries, the real transformation happened with electronic or digital computers. Development of the electronic computer started during the Second World War. In 1941, German engineer Konrad Zuse developed a computer called Z3 to design airplanes and missiles. In 1943, the British developed a computer called Colossus for cryptanalysis to decode encrypted messages transmitted by Germans. With a team of engineers in 1944, Howard H. Aiken developed the Harvard–IBM Automatic Sequence Controlled Calculator Mark I, or Mark I for short. This is considered as the early general-purpose computer. In 1945, John von Neumann introduced the concept of stored program. Another general-purpose computer development spurred by the war was the Electronic Numerical Integrator and Computer, better known as ENIAC, developed by John Presper Eckert and John W. Mauchly in 1946. In 1947, the invention of the transistor by John Bardeen, Walter H. Brattain, and William Shockley at Bell Labs changed the development scenario of digital computers. The transistor replaced the large, energy-hungry vacuum tube in first generation computers. Jack Kilby, an engineer with Texas Instruments, developed the integrated circuit (IC) in 1958. IC combined all the essential electronic components (inductor, resistor, capacitor, etc.) on to a small silicon disc, which was made from quartz. By the 1980s, very large scale integration (VLSI) squeezed hundreds of thousands of components on to a chip. VLSI led the development of third generation computers. All these early computers contained all the components we find today in any modern-day computers like printers, persistent storage, memory, operating systems and stored programs. However, one aspect of modern-day computers was missing in these machines—that was the networking aspect of today's computers.

2.2 HISTORY OF INTERNET

Following the successful launch of Sputnik in 1957 by the Russians, the US felt the need of research in certain focused areas. Therefore, Advance Research Project Agency (ARPA) was formed to fund Science and Technology projects and position the US as a leader in technology. Internet represents one of the best examples of the benefits of sustained investment on research and development through ARPA. Beginning with the early research in packet switching, the government, industry and academia have been partners in evolving and deploying the exciting Internet technology. People in almost all parts of life starting from education, IT, telecommunications, business, and society have felt the influence of this pervasive information infrastructure. Today, almost everybody uses terms like “faculty@iiitb.ac.in” or “<http://www.isoc.org>”.

In the early sixties, Leonard Kleinrock developed the basic principles of packet switching at Massachusetts Institute of Technology (MIT). During the same period Paul Baran in a series of RAND Corporation reports recommended several ways to accomplish packet switch network as well. In 1965, Lawrence G. Roberts in association with Thomas Merrill, connected the TX-2 computer in Massachusetts to the Q-32 in California with a low speed dial-up telephone line creating the first computer network. In 1971, Ray Tomlinson at BBN wrote the software to send and read simple electronic mail. In October 1972, demonstration of the ARPANET was done at the International Computer Communication Conference (ICCC). This was the first public demonstration of this new network technology to the public. It was also in 1972 that the initial ‘hot’ application, electronic mail, was introduced. In 1973, work began on the Transmission Control Protocol (TCP) at a Stanford University laboratory headed by Vincent Cerf.

In 1986, the US NSF (National Science Foundation) initiated development of the NSFNET which provides a major backbone communication service for the Internet. In Europe, major international backbones such as NORDUNET and others provide connectivity to a large number of networks. Internet slowly evolved as the universal network of networks, which connects almost every data network of the world with a reach spread across earth. It can be debated as to what the definition and scope of this global network is. On 24 October 1995, the Federal Networking Council (FNC) unanimously passed a resolution to officially define the term Internet. According to this resolution, the definition of Internet is “Internet refers to the global information system that (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.”

Vannevar Bush through his July 1945 essay “As We May Think”, described a theoretical machine he called a “memex”, which was to enhance human memory by allowing the user to store and retrieve documents linked by associations. This can be considered as the early hypertext. During the 1960s, Doug Engelbart prototyped an ‘oNLine System’ (NLS) that does hypertext browsing, editing, etc. He invented the mouse for this purpose. In 1991, Tim Berners-Lee invented HTML (Hyper Text Markup Language) and HTTP (Hyper Text Transport Protocol). Tim wrote a client program and named it ‘WorldWideWeb’, which finally became the ‘www’ (World Wide Web),

almost synonymous with Internet. We would like to differentiate all these technologies by different names. We will use Web for the HTTP (WWW technology), Internet for the interworking with the network of networks, and Internet for the Internet managed by IETF (Internet Engineering Task Force).

2.3 INTERNET—THE UBIQUITOUS NETWORK

For any content to be available anywhere, we need a ubiquitous network that will carry this content. As of today, there are two networks which are ubiquitous. One is the telecommunication network and the other is the Internet network. Both these networks are in real terms the network of networks. Different networks have been connected together using a common protocol (glue). In simple terms it can be stated that SS#7 is the glue for telecommunication network whereas TCP/IP is the glue for Internet. We need one of these networks to transport content from one place to another.

We have three types of basic content: audio, video and text. Some of these content can tolerate little delays in delivery whereas some cannot. Packet switched networks like Internet are better suited for content which can tolerate little delays. Telecommunication or circuit switch networks are better suited for real-time content that cannot tolerate delays. A ubiquitous application needs to use these networks to take the content from one place to another. A network can be divided into three main segments, viz., Core, Edge and Access.

Core: As the name signifies, core is the backbone of the network. This is the innermost part of the network. The primary function of the core network is to deliver traffic efficiently at the least cost. Core looks at the traffic more from the bit stream point of view. Long-distance operators and backbone operators own core networks. This part of the network deals with transmission media and transfer points.

Edge: As the name suggests, this is at the edge of the network. These are generally managed and owned by ISPs (Internet Service Providers) or local switches and exchanges. Edge looks at the traffic more from the service point of view. It is also responsible for the distribution of traffic.

Access: This part of the network services the end point or the device by which the service will be accessed. This deals with the last mile of transmission. This part is either through a wireline or the wireless. From the mobile computing point of view, this will be mostly through the wireless.

Internet is a network of networks and is available universally. In the last few years, the popularity of web-based applications has made more and more services available through the Internet. This had a snowball effect encouraging more networks and more content to be added to the Web. Therefore, Internet is the preferred bearer network for audio, video or text content that can tolerate delays. Internet supports many protocols. However, for ubiquitous access, web-based applications are desirable. A web-based application in the Internet uses HTTP protocol and works like a request/response service. This is similar to the conventional client/server application. The fundamental difference between a web application and a conventional client/server paradigm is that in the case of conventional client/server application, the user facing the client interface contains part of the business logic. However, in the case of web applications, the client will be a thin client without any business logic. The thin client or the agent software in the client device will relate only to the

rendering functions. Such user agents will be web browsers like Mozilla, Internet Explorer or Netscape Navigator.

The types of client devices that can access the Internet are rapidly expanding. These client devices are networked either through the wireless or through a wireline. The server on the contrary, is likely to be connected to the access network through wired LAN. In addition to standard computers of different shapes and sizes, client devices can be Personal Digital Assistants (PDA) such as the PalmPilot, Sharp Zaurus, or iPaq; handheld personal computers such as the EPOC, Symbian, Psion and numerous Windows- CE machines; mobile phones with GPRS/WAP and 3G capability such as Nokia, Sony Ericsson, etc.; Internet-capable phones such as the Smartphone (cellular) and Screenphone (wired); set-top boxes such as WebTV, etc. Even the good old voice-based telephone can be used as the client device. Voice-activated Internet browsers will be very useful for visually challenged people. To fulfill the promise of universal access to the Internet, devices with very diverse capabilities need to be made available. For the wireless, devices range from the small footprint mobile phone to the large footprint laptop computers.

2.4 ARCHITECTURE FOR MOBILE COMPUTING

In mainframe computers many mission critical systems use a Transaction Processing (TP) environment. At the core of a TP system, there is a TP monitor software. In a TP system, all the terminals—VDU (Visual Display Terminal), POS (Point of Sale Terminal), printers, etc., are terminal resources (objects). There are different processing tasks, which process different transactions or messages; these are processing resources (objects). Finally, there are database resources. A TP monitor manages terminal resources, database objects and coordinates with the user to pick up the right processing task to service business transactions. The TP monitor manages all these objects and connects them through policies and rules. A TP monitor also provides functions such as queuing, application execution, database staging, and journaling. When the world moved from large expensive centralized mainframes to economic distributed systems, technology moved towards two-tier conventional client/server architecture. With growth in cheaper computing power and penetration of Internet-based networked systems, technology is moving back to centralized server-based architecture. The TP monitor architecture is having a reincarnation in the form of three-tier software architecture.

In the early days of mainframes, the TP monitor and many other interfaces were proprietary. Even the networked interfaces to different terminals were vendor-specific and proprietary. The most successful early TP system was the reservation system for the American Airlines. This was over a Univac computer using U100 protocol. For IBM TP environment, which runs on OS/390 known as CICS (Customer Information Control System), the network interface was through SNA. In India DoT (Department of Telecommunication; currently BSNL and MTNL) launched the 197 telephone directory enquiry system in 1986, it used TPMS (Transaction Processing Management System) on ICL mainframe running VME operating system. The network interface was over X.25 interface.

The network-centric mobile computing architecture uses three-tier architecture as shown in Figure 2.1. In the three-tier architecture, the first layer is the User Interface or Presentation Tier. This layer deals with user facing device handling and rendering. This tier includes a user system interface where user services (such as session, text input, dialog and display management) reside. The second tier is the Process Management or Application Tier. This layer is for application programs or process management where business logic and rules are executed. This layer is capable of accommodating hundreds of users. In addition, the middle process management tier controls transactions and asynchronous queuing to ensure reliable completion of transactions. The third and final tier is the Database Management or Data Tier. This layer is for database access and management. The three-tier architecture is better suited for an effective networked client/server design. It provides increased *performance*, *flexibility*, *maintainability*, *reusability*, and *scalability*, while hiding the complexity of distributed processing from the user. All these characteristics have made three-tier architectures a popular choice for Internet applications and net-centric information systems. Centralized process logic makes administration and change management easier by localizing changes in a central place and using them throughout the system.

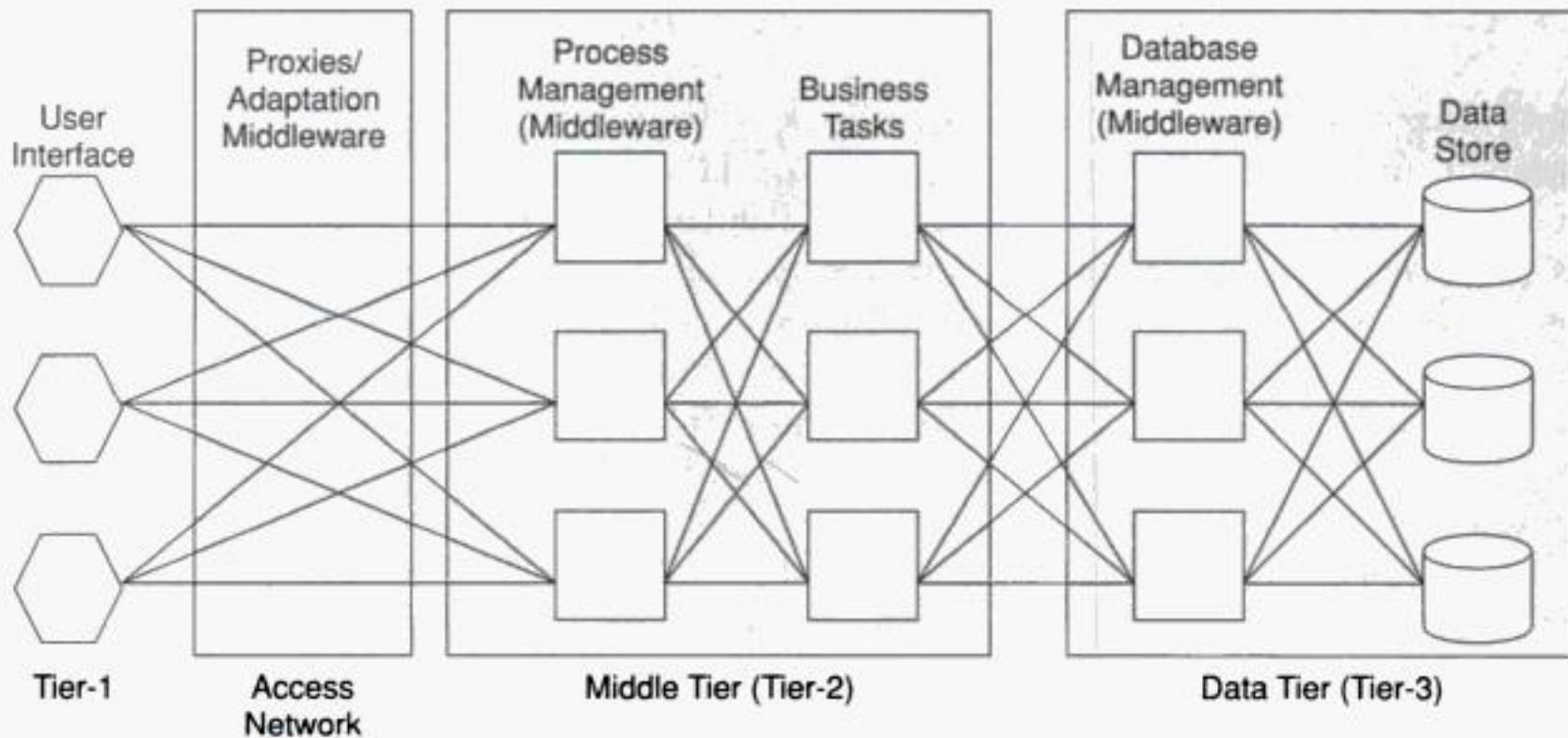


Figure 2.1 Three-tier Architecture for Mobile Computing

2.5 THREE-TIER ARCHITECTURE

To design a system for mobile computing, we need to keep in mind that the system will be used through any network, bearer, agent and device. To have universal access, it is desirable that the server is connected to a ubiquitous network like the Internet. To have access from any device, a web browser is desirable. The reason is simple; web browsers are ubiquitous, they are present in any computer. The browser agent can be Internet Explorer or Netscape Navigator or Mozilla or any other standard agent. Also, the system should preferably be context aware. We will discuss context awareness later.

We have introduced the concept of three-tier architecture. We have also discussed why it is necessary to go for Internet and three-tier architecture for mobile computing. The important question is what a mobile three-tier application actually should consist of. Figure 2.2 depicts a three-tier architecture for a mobile computing environment. These tiers are presentation tier, application tier and data tier. Depending upon the situation, these layers can be further sublayered.

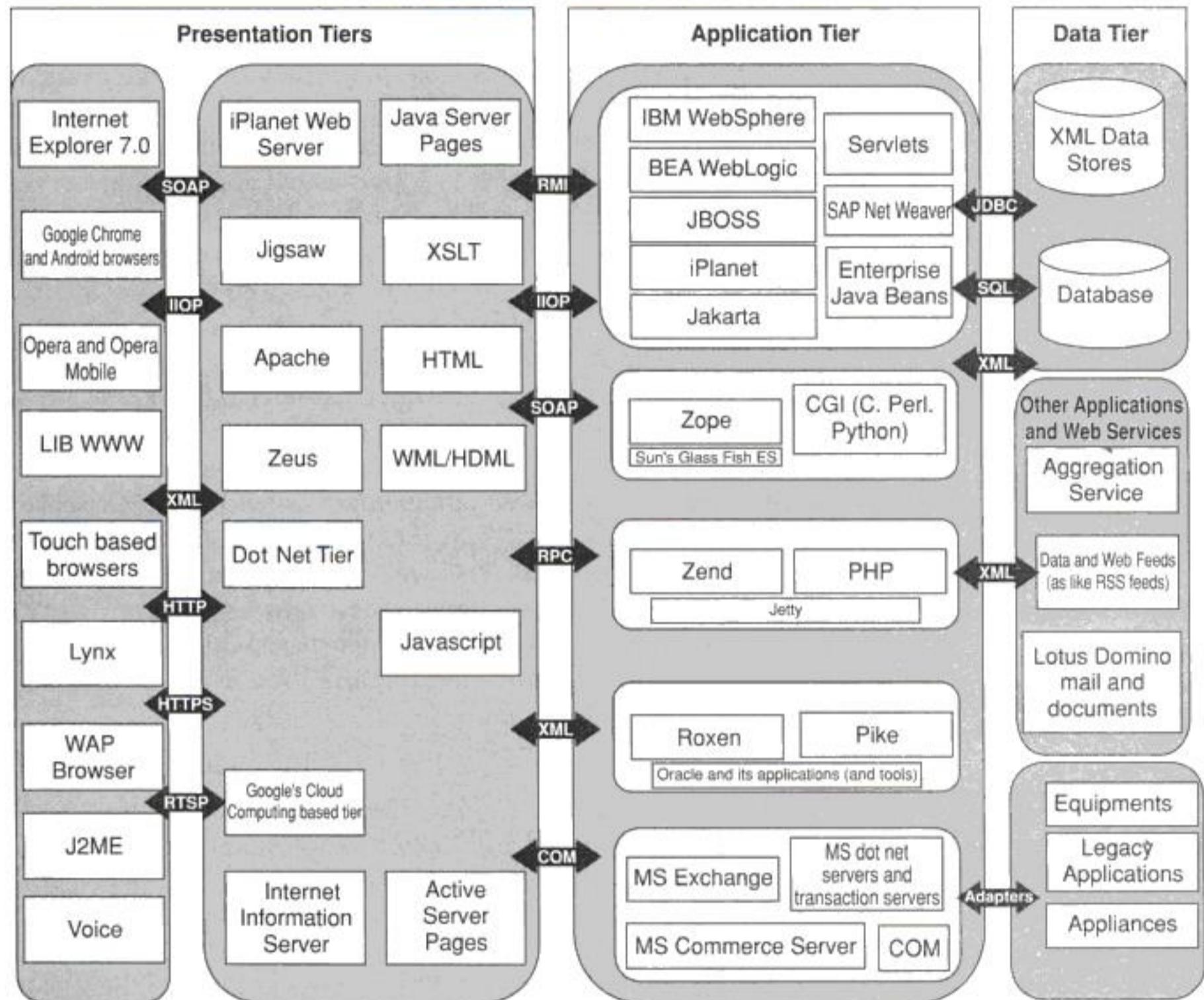


Figure 2.2 The Mobile Computing Architecture

2.5.1 Presentation (Tier-1)

This is the user facing system in the first tier. This is the layer of agent applications and systems. These applications run on the client device and offer all the user interfaces. This tier is responsible for presenting the information to the end user. Humans generally use visual and audio means to

receive information from machines (with some exceptions like vibrator in mobile phones). Humans also use keyboard (laptop computers, cell phones), pen (tablet PC, palmtops), touch screen (kiosks), or Voice (telephone) to feed the data to the system. In the case of the visual, the presentation of information will be through a screen. Therefore, the visual presentation will relate to rendering on a screen. ‘Presentation Tier’ includes web browsers (like Mozilla, Lynx, Internet Explorer and Netscape Navigator), WAP browsers and customized client programs. A mobile computing agent needs to be context-aware and device independent.

In general, the agent software in the client device is an Internet browser. In some cases, the agent software is an applet running on a browser or a virtual machine (Java Virtual Machine, for example). The functions performed by these agent systems can range from relatively simple tasks like accessing some other application through HTTP API, to sophisticated applications like real-time sales and inventory management across multiple vendors. Some of these agents work as web scrapers. In a web scraper, the agent embeds functionality of the HTTP browser and functions like an automated web browser. The scraper picks up part of the data from the web page and filters off the remaining data according to some predefined template. These applications can be in Business to Business (B2B) space, Business to Consumer (B2C) space or Business to Employee (B2E) space, or machine to machine (M2M) space. Applications can range from e-commerce, workflow, supply chain management to legacy applications.

There are agent software in the Internet that access the remote service through telnet interface. There are different flavors of telnet agents in use. These are standard telnet for UNIX servers; TN3270 for IBM OS/390; TN5250 for IBM AS/400 or VT3K for HP3000. For some applications, we may need an agent with embedded telnet protocol. This will work like an automated telnet agent (virtual terminal) similar to a web scraper. These types of user agents or programs work as M2M interface or software robots. These kinds of agents are used quite frequently to make legacy applications mobile. Also, such systems are used in the telecommunication world as mediation servers within the OSS (Operation and Support Subsystem).

2.5.2 Application (Tier-2)

The application tier or middle tier is the “engine” of a ubiquitous application. It performs the business logic of processing user input, obtaining data, and making decisions. In certain cases, this layer will do the transcoding of data for appropriate rendering in the Presentation Tier. The Application Tier may include technology like CGIs, Java, JSP, .NET services, PHP or ColdFusion, deployed in products like Apache, WebSphere, WebLogic, iPlanet, Pramati, JBOSS or ZEND. The application tier is presentation and database-independent.

In a mobile computing environment, in addition to the business logic there are quite a few additional management functions that need to be performed. These functions relate to decisions on rendering, network management, security, datastore access, etc. Most of these functions are implemented using different middleware software. A middleware framework is defined as a layer of software, which sits in the middle between the operating system and the user facing software. Stimulated by the growth of network-based applications and systems, middleware technologies are gaining increasing importance in net-centric computing. In case of net-centric architecture, a middleware framework sits between an agent and business logic. Middleware covers a wide range of software systems, including distributed objects and components, message-oriented

communication, database connectors, mobile application support, transaction drivers, etc. Middleware can also be considered as a software gateway connecting two independent open objects.

It is very difficult to define how many types of middleware are there. A very good description of middleware is available in Carnegie Mellon University Software Engineering Institute (<http://www.sei.cmu.edu/str/descriptions/middleware.html>), which readers can refer to.

We can group middleware into the following major categories:

1. Message-oriented Middleware.
2. Transaction Processing Middleware.
3. Database Middleware.
4. Communication Middleware.
5. Distributed Object and Components.
6. Transcoding Middleware.

Message-oriented Middleware (MOM)

Message-oriented Middleware is a middleware framework that loosely connects different applications through asynchronous exchange of messages. A MOM works over a networked environment without having to know what platform or processor the other application is resident on. The message can contain formatted data, requests for action, or unsolicited response. The MOM system provides a message queue between any two interoperating applications. If the destination process is out of service or busy, the message is held in a temporary storage location until it can be processed. MOM is generally asynchronous, peer-to-peer, and works in publish/subscribe fashion. In the publish/subscriber mode one or many objects subscribe to an event. As the event occurs, it will be published by the loosely coupled asynchronous object. The MOM will notify the subscribers about this event. However, most implementations of MOM support synchronous (request/response) message passing as well. MOM is most appropriate for event-driven applications. When an event occurs, the publisher application hands on to the messaging middleware application the responsibility of notifying subscribers that the event has happened. In a net-centric environment, MOM can work as the integration platform for different applications. An example of MOM is Message Queue from IBM known as MQ Series. The equivalent from Java is JMS (Java Message Service).

Transaction Processing (TP) Middleware

Transaction Processing Middleware provides tools and an environment for developing transaction-based distributed applications. An ideal TP system will be able to input data into the system at the point of information source and the output of the system is delivered at the point of information sink. In an ideal TP system, the device for input and output can potentially be different (Fig. 2.3). Also, the output can be an unsolicited message for a device. TP is used in data management, network access, security systems, delivery order processing, airline reservations, customer service, etc., to name a few. TP systems are generally capable of providing services to thousands of clients in a distributed client/server environment. CICS (Customer Information Control System) is one of the early TP application systems on IBM mainframe computers.

TP middleware maps numerous client requests through application-service routines to different application tasks. In addition to these processing tasks, TP middleware includes numerous management features, such as restarting failed processes, dynamic load balancing and ensuring

consistency of distributed data. TP middleware is independent of the database architecture. TP middleware optimizes the use of resources by multiplexing many client functions on to a much smaller set of application-service routines. This also helps in reducing the response time. TP middleware provides a highly active system that includes services for delivery-order processing, terminal and forms management, data management, network access, authorization, and security. In the Java world and net-centric systems, transaction processing is done through the J2EE application server with the help of entity and session beans.

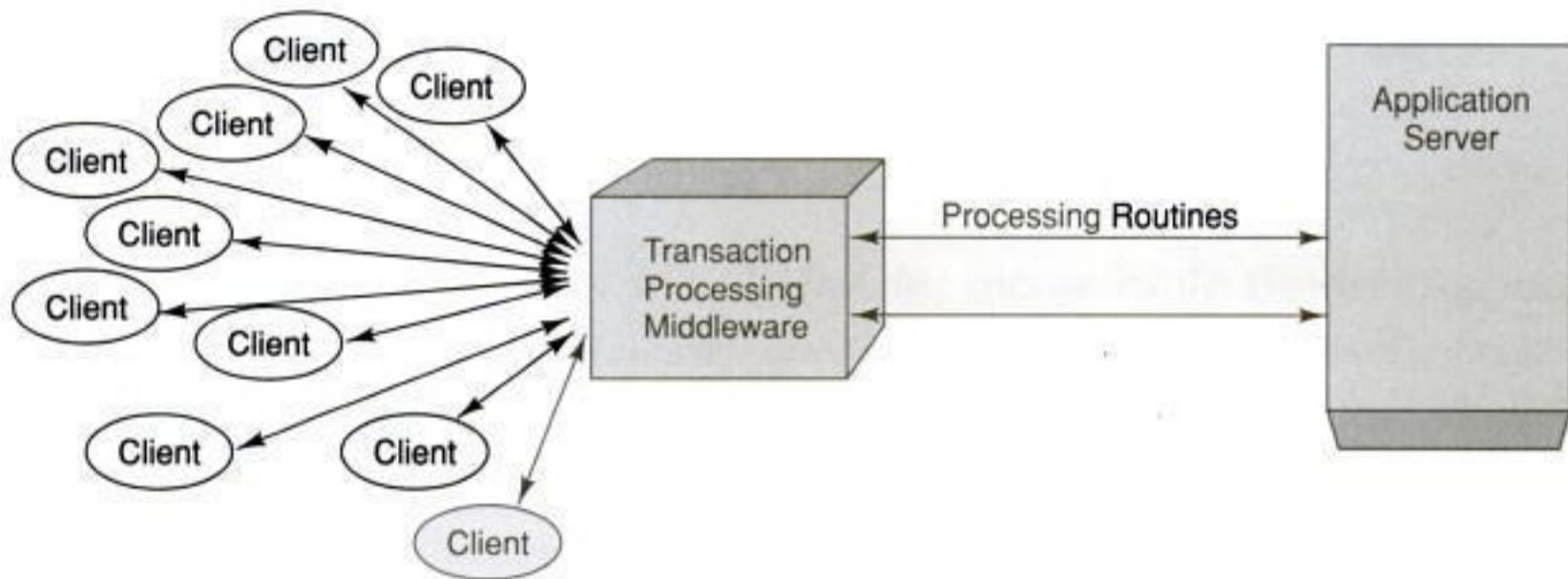


Figure 2.3 Transaction Processing Middleware

Model View Controller (MVC): Java uses the MVC architectural pattern which is an example of transaction processing system. It splits an application into separate layers, viz., presentation, domain logic, and data access. *Model* is the domain-specific representation of the information on which the application operates. Domain logic manipulates and adds meaning to the raw data. MVC does not specifically mention the data access layer because it is assumed to be encapsulated by the model. *View* is responsible for rendering the model into a form suitable for interaction and understood by the user, typically a user interface element. *Controller* manages processes and responds to events, typically user actions, and may invoke changes on the model. In the context of Web applications and J2EE, the MVC pattern is widely used. In Web applications, where the view is the actual HTML page, and the controller is the code which gathers dynamic data and generates the content within the HTML, the model is represented by the actual content, usually stored in a database.

Communication Middleware

Communication Middleware is used to connect one application to another through some communication middleware, like connecting one application to another through telnet. These types of middleware are quite useful in the telecommunication world. There are many elements in the core telecommunication network where the user interface is through telnet. A mediation server automates the telnet protocol to communicate with these nodes in the network. Another example could be to integrate legacy applications through proprietary communication protocols like TN5250 or TN3270.

Distributed Object and Components

An example of distributed objects and components is CORBA (Common Object Request Broker Architecture). CORBA is an open distributed object computing infrastructure being standardized by the Object Management Group (<http://www.omg.org>). CORBA simplifies many common network programming tasks used in a net-centric application environment. These are object registration, object location, and activation; request demultiplexing; framing and error-handling; parameter marshalling and demarshalling; and operation dispatching. CORBA is vendor-independent infrastructure. A CORBA-based program from any vendor on almost any computer, operating system, programming language and network, can interoperate with a CORBA-based program from the same or another vendor, on almost any other computer, operating system, programming language and network. CORBA is useful in many situations because of the easy way that CORBA integrates machines from so many vendors, with sizes ranging from mainframes through minis and desktops to hand-holds and embedded systems. One of its most important, as well as the most frequent uses is in servers that must handle a large number of clients, at high hit rates, with high reliability.

Transcoding Middleware

Transcoding Middleware is used to transcode one format of data to another to suit the need of the client. For example, if we want to access a web site through a mobile phone supporting WAP, we need to transcode the HTML page to WML page so that the mobile phone can access it. Another example could be accessing a map from a PDA. The same map, which can be shown in a computer, needs to be reduced in size to fit the PDA screen. Technically transcoding is used for content adaptation to fit the need of the device. Content adaptation is also required to meet the network bandwidth needs. For example, some frames in a video clip need to be dropped for a low bandwidth network. Content adaptation used to be done through proprietary protocols. To allow interoperability, IETF has accepted the Internet Content Adaptation Protocol (ICAP). ICAP is now standardized and described in RFC3507.

Internet Content Adaptation Protocol (ICAP)

Popular web servers are required to deliver content to millions of users connected at ever-increasing bandwidths. Progressively, content is being accessed through different devices and agents. A majority of these services have been designed keeping the desktop user in mind. Some of them are also available for other types of protocols. For example, there are a few sites that offer contents in HTML and WML to service desktop and WAP phones. However, the model of centralized services that are responsible for all aspects of every client's request seems to be reaching the end of its useful life. ICAP, the Internet Content Adaptation Protocol, is a protocol aimed at providing simple object-based content vectoring for HTTP services. ICAP is a lightweight protocol to do transcoding on HTTP messages. This is similar to executing a "remote procedure call" on a HTTP request. The protocol allows ICAP clients to pass HTTP messages to ICAP servers for some sort of transformation. The server executes its transformation service on messages and sends back responses to the client, usually with modified messages. The adapted messages may be either HTTP requests or HTTP responses. For example, before a document is displayed in the agent, it is checked for virus.

There are two major components in ICAP architecture:

1. What are the semantics for the transformation? How do I ask for content adaptation?

2. How is policy of the transformation managed? What kind of adaptation do I ask for and from where? How do I define and manage the adaptation?

ICAP works at the edge part of the network as depicted in Figure 2.4. It is difficult, if not impossible, to define the devices users may like to use to access content from within the Internet. Customized edge delivery of Internet content will help to improve user experience. When applications are delivered from an edge device, end users find that the applications execute more quickly and are more reliable. Typical data flow in an ICAP environment is depicted in Figure 2.4 and described here.

1. A user agent makes a request to an ICAP-capable surrogate (ICAP client) for an object on an origin server.
2. The surrogate sends the request to the ICAP server.
3. The ICAP server executes the ICAP resource's service on the request and sends the possibly modified request, or a response to the request back to the ICAP client.
4. The surrogate sends the request, possibly different from the original client's request, to the origin server.
5. The origin server responds to the request.
6. The surrogate sends the reply (from either the ICAP or the origin server) to the client.

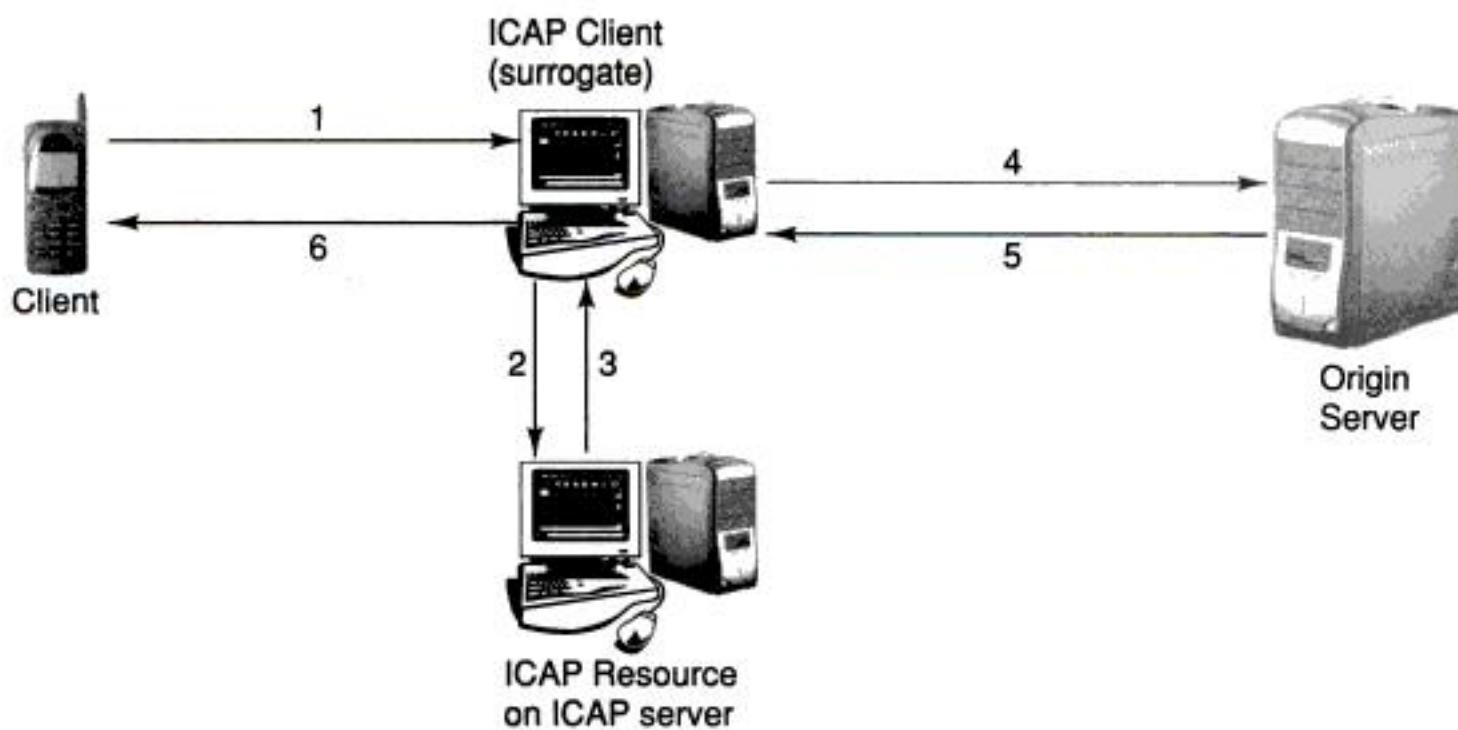


Figure 2.4 Typical Data Flow in an ICAP Environment

It is envisioned that in future, ICAP servers may be available to provide some of the following services:

- Suit content delivery based on network bandwidth.
- Suit content delivery based on device characteristics.
- Language translation based on the user's preference.
- Virus checking for the requested content.
- Content filtering based on sensor rating like PG (parental guidance), R (restricted).
- Local real-time advertisement insertion like television.
- Local real-time advertisement elimination for premium subscribers.

- Wireless protocol translation.
- Anonymous Web usage profiling for a dating service.
- Transcoding or image enhancement.
- Image magnification for the elderly.
- Image size reduction based on device display characteristics.
- Intelligent video condensation by dropping frames.
- Digest production/batch download of Web content.
- Content filtering based on copyright or digital signature.
- Peer-to-Peer compression and encryption of data.

Web Services

As the need for peer-to-peer, application-to-application communication and interoperability grows, the use of Web services on the Internet will also grow. Web services provide a standard means of communication and information exchange among different software applications, running on a variety of platforms or frameworks. Web service is a software system identified by a URI, whose public interfaces and bindings are defined using XML (eXtensible Markup Language). Its definition can be discovered by other software systems connected to the network. Using XML-based messages these systems may then interact with the Web service in a manner prescribed by its definition.

The basic architecture includes Web service technologies capable of:

- Exchanging messages.
- Describing Web services.
- Publishing and discovering Web service descriptions.

The Web services architecture defines the standards for exchange of messages between the service requester and service provider. Service providers are responsible for publishing a description of the services they provide. Requesters must be able to find and discover descriptions of the services.

Software agents in the basic architecture can take on one or all of the following roles:

- Service requester—requests the execution of a Web service.
- Service provider—processes a Web service request.
- Discovery agency—agency through which a Web service description is published and made discoverable.

The interactions involve the publish, find and bind operations. A service is invoked after the description is found, since the service description is required to establish a binding.

2.5.3 Data (Tier-3)

The Data Tier is used to store data needed by the application and acts as a repository for both temporary and permanent data. The data can be stored in any form of datastore or database. These can range from sophisticated relational database, legacy hierarchical database, to even simple text files. The data can also be stored in XML format for interoperability with other systems and datasources. A legacy application can also be considered as a data source or a document through a communication middleware.

Database Middleware

We have discussed that for a mobile computing environment, the business logic should be independent of the device capability. Likewise, though not essential, it is advised that business logic should be independent of the database. Database independence helps in maintenance of the system better. Database middleware allows the business logic to be independent and transparent of the database technology and the database vendor. Database middleware runs between the application program and the database. These are sometimes called database connectors as well. Examples of such middleware will be ODBC, JDBC, etc. Using these middleware, the application will be able to access data from any data source. Data sources can be text files, flat files, spreadsheets, or a network, relational, indexed, hierarchical, XML database, object database, etc., from vendors like Oracle, SQL, Sybase, etc.

SyncML

SyncML protocol is an emerging standard for synchronization of data access from different nodes. When we moved from the conventional client/server model of computing to the net-centric model of computing, we moved from distributed computing to centralized computing with networked access. The greatest benefit of this model is that resources are managed at a centralized level. All the popular mobile devices like handheld computers, mobile phones, pagers and laptops work in an occasionally connected computing mode and access these centralized resources from time to time. In an occasionally connected mode, some data are cached in the local device and accessed frequently. The ability to access and update information on the fly is key to the pervasive nature of mobile computing. Examples are emails and personal information like appointments, address book, calendar, diary, etc. Storing and accessing phone numbers of people from the phone address book is more user-friendly compared to accessing the same from a server. However, managing the appointments database is easier in a server, though caching the same on the mobile client is critical. Users will cache emails into the device for reference. We take notes or draft a mail in the mobile device. For workflow applications, data synchronization plays a significant role. The data in the mobile device and server need to be synchronized. Today vendors use proprietary technology for performing data synchronization. SyncML protocol is the emerging standard for synchronization of data across different nodes. SyncML is a new industry initiative to develop and promote a single, common data synchronization protocol that can be used industry-wide.

The ability to use applications and information on a mobile device, then to synchronize any updates with the applications and information back at the office or on the network, is key to the utility and popularity of mobile computing. The SyncML protocol supports naming and identification of records and common protocol commands to synchronize local and network data. It supports identification and resolution of synchronization conflicts. The protocol works over all networks used by mobile devices, both wireless and wireline. Since wireless networks employ different transport protocols and media, a SyncML will work smoothly and efficiently over:

- HTTP 1.1 (i.e., the Internet).
- WSP (the Wireless Session Protocol, part of the WAP protocol suite).
- OBEX (Object Exchange Protocol, i.e., Bluetooth, IrDA and other local connectivity).
- SMTP, POP3 and IMAP.
- Pure TCP/IP networks.
- Proprietary wireless communication protocols.

2.6 DESIGN CONSIDERATIONS FOR MOBILE COMPUTING

The mobile computing environment needs to be context-independent as well as context-sensitive. Context information is the information related to the surrounding environment of an actor in that environment. The term "context" means, all the information that helps determine the state of an object (or actor). This object can be a person, a device, a place, a physical or computational object, the surrounding environment or any other entity being tracked by the system. In a mobile computing environment, context data is captured so that decisions can be made about how to adapt content or behavior to suit this context. Mobility implies that attributes associated with devices and users will change constantly. These changes mean that content and behavior of applications should be adapted to suit the current situation. There are many ways in which content and behavior can be adapted. Following are some examples:

- 1. Content with context awareness:** Build each application with context awareness. There are different services for different client context (devices). For example, a bank decides to offer mobile banking application through Internet, PDA and mobile phone using WAP. These services are different and are <http://www.mybank.com/inet.html>, <http://www.mybank.com/palm.html> and <http://www.mybank.com/wap.wml>, respectively. The service <http://www.mybank.com/inet.html> assumes that the user will use computers to access this service. Therefore it is safe to offer big pages with text boxes and drop down menus. Also, it is fine to add a few animated pictures for the new product the bank is launching. We know that <http://www.mybank.com/palm.html> is a service for a PalmOS PDA. As the display size is small, we design the screen to be compact for the PDA and do not offer the same product animation. For the WAP service at <http://www.mybank.com/wap.wml>, we do a completely different user interface; we make all drop down options available through the option button in the mobile phone and remove all the graphics and animations.
- 2. Content switch on context:** Another way is to provide intelligence for the adaptation of content within the service. This adaptation happens transparent to the client. In this case the service is the same for Internet, PDA and WAP. All access the bank's service through <http://www.mybank.com/>. An intelligent piece of code identifies the agent to decide what type of device or context it is. This intelligent code does the adaptation at runtime based upon the agent in hand. The simplest way to do this is to look at the user-agent value at the HTTP header and decide whether to route the request to <http://mybank.com/inet.html> or <http://www.mybank.com/palm.html> or <http://www.mybank.com/wap.wml>.
- 3. Content transcoding on context:** Another way is to provide an underlying middleware platform that performs the adaptation of the content based on the context and behavior of the device. This adaptation happens transparent to the client and the application. The middleware platform is intelligent enough to identify the context either from the HTTP or additional customized parameters. In this case the service may be in html or XML, the middleware platform transcodes the code from html (or XML) to html, and wml on the fly. It can also do the transcoding based on policy so that the html generated for a computer is different from a PDA.

Following sections describe different types of context that can enhance the usability, reliability and security of the service. Figure 2.5 depicts the old web and web of the future for mobile computing.

2.6.1 Client Context Manager

When we humans interact with other persons, we always make use of the implicit situational information of the surrounding environment. We interpret the context of the current situation and react appropriately. For example, we can go close to a lion in a zoo, but definitely not in the wild. Or, a person discussing some confidential matter with another person observes the gestures and tone of the other person and reacts in an appropriate manner or changes the subject if someone shows up suddenly. When we use content through a PC within the four walls of an organization, we do not have any problem. A majority of the applications can safely assume that the context is the enterprise LAN. It can be assumed that the environment is secured; it can also be assumed that the user will be using the systems in a particular fashion using the browser standardized by the company. These applications are developed keeping the large screen (for mainly PC) and browsers in mind. A mobile computing application, on the other hand, needs to operate in dynamic conditions. This is due to various device characteristics and network conditions. This demands a reactive platform that can make decisions about how to respond to changes to device capability, user preferences, enterprise policy, network policy and many other environmental factors. Context can be used as the basis by which an adaptation manager or algorithm decides to modify content or application behavior. We therefore need a Client Context Manager to gather and maintain information pertaining to the client device, user, network and the environment surrounding each mobile device. All these information will be provided by a set of Awareness Modules. Awareness

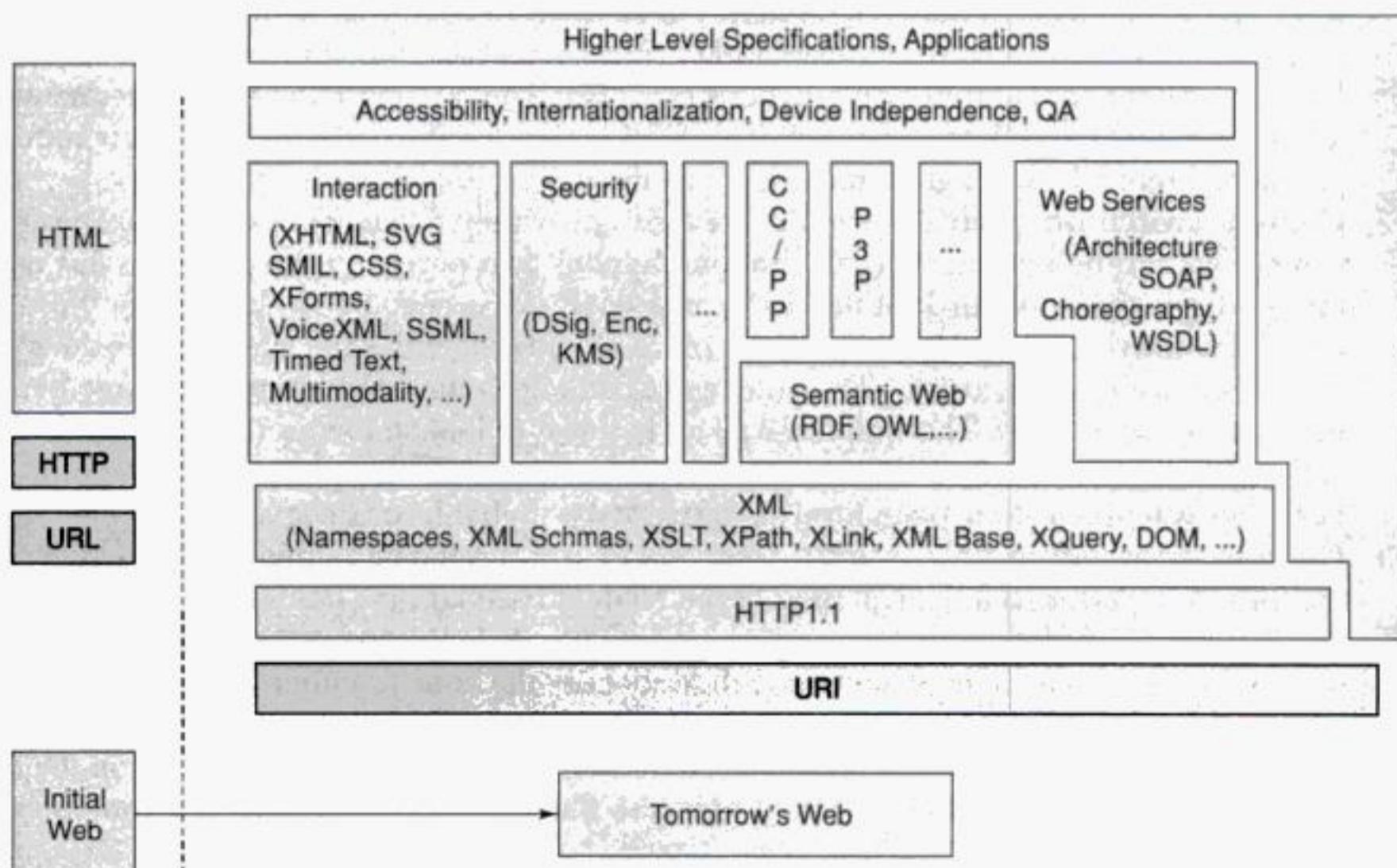


Figure 2.5 The Content Architecture with Respect to Mobile Computing

modules are sensors of various kinds. These sensors can be hardware sensors or software sensors or a combination of these. A hardware sensor can be used to identify the precise location of a user; whereas, a software sensor can be used to determine the type of the user agent. These awareness modules can be in the device, network, or even in the middleware. We use the term middleware in a very generic context. A middleware can be a functional module in the content server, a proxy or an independent system. For example, an awareness module in the device will provide information about its capabilities. Another example could be a location manager that tracks the location and orientation of the mobile device.

Almost any information available at the time of an interaction can be seen as context information. Some examples are:

1. **Identity:** The device will be in a position to communicate its identity without any ambiguity.
2. **Spatial information:** Information related to the surrounding space. This relates to location, orientation, speed, elevation and acceleration.
3. **Temporal information:** Information related to time. This will be time of the day, date, time zone and season of the year.
4. **Environmental information:** This is related to the environmental surroundings. This will include temperature, air quality, moisture, wind speed, natural light or noise level. This also includes information related to the network and network capabilities.
5. **Social situation:** Information related to the social environment. This will include who you are with, and people that are nearby; whether the user is in a meeting or in a party.
6. **Resources that are nearby:** This will relate to the other accessible resources in the nearby surroundings like accessible devices, hosts or other information sinks.
7. **Availability of resources:** This will relate to information about the device in use. This will include battery power, processing power, persistence store, display, capabilities related to I/O (input/output) and bandwidth.
8. **Physiological measurements:** This relates to the physiological state of the user. This includes information like blood pressure, heart rate, respiration rate, muscle activity and tone of voice.
9. **Activity:** This relates to the activity state of the user. This includes information like talking, reading, walking and running.
10. **Schedules and agendas:** This relates to the schedules and agendas of the user.

A system is context-aware if it can extract, interpret and use context-related information to adapt its functionality to the current context. The challenge for such systems lies in the complexity of capturing, representing, filtering and interpreting contextual data. To capture context information generally some sensors are required. This context information needs to be represented in a machine-understandable format, so that applications can use this information. In addition to being able to obtain the context-information, applications must include some 'intelligence' to process the information and deduce the meaning. These requirements lead us to three aspects of context management:

1. **Context sensing:** The way in which context data is obtained.
2. **Context representation:** The way in which context information is stored and transported.
3. **Context interpretation:** The way in which meaning is obtained from the context representation.

W3C has proposed a standard for context information. This standard is called Composite Capabilities/Preference Profiles (CC/PP), for describing device capabilities and user preferences. All these context information are collated and made available to the management components.

Composite Capabilities/Preference Profiles (CC/PP)

Composite Capabilities/Preference Profiles (CC/PP) is a proposed W3C standard for describing device capabilities and user preferences. Special attention has been paid to wireless devices such as mobile phones and PDAs. In practice, the CC/PP model is based on RDF (resource description framework) and can be serialized using XML.

A CC/PP profile contains a number of attribute names and associated values that are used by an application to determine the appropriate form of a resource to deliver to a client. This is to help a client or proxy/middleware to describe their capabilities to an origin server or other sender of resource data. It is anticipated that different applications will use different vocabularies to specify application-specific properties within the scope of CC/PP. However, for different applications to interoperate, some common vocabulary is needed. The CC/PP standard defines all these. Following is an example of a device RDF in CC/PP terminology.

```
<?xml version="1.0"?>
<!– Checked by SiRPAC 1.16, 18-Jan-2001 –>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
           xmlns:ccpp="http://www.w3.org/2000/07/04-ccpp#">
  <rdf:Description rdf:about="MyProfile">
    <ccpp:component>
      <rdf:Description rdf:about="TerminalHardware">
        <rdf:type rdf:resource="HardwarePlatform" />
        <display>320x200</display>
      </rdf:Description>
    </ccpp:component>
    <ccpp:component>
      <rdf:Description rdf:about="TerminalSoftware">
        <rdf:type rdf:resource="SoftwarePlatform" />
        <name>EPOC</name>
        <version>2.0</version>
        <vendor>Symbian</vendor>
      </rdf:Description>
    </ccpp:component>
    <ccpp:component>
      <rdf:Description rdf:about="TerminalBrowser">
        <rdf:type rdf:resource="BrowserUA" />
        <name>Mozilla</name>
        <version>5.0</version>
        <vendor>Symbian</vendor>
        <htmlVersionsSupported>
          <rdf:Bag>
            <rdf:li>3.0</rdf:li>
            <rdf:li>4.0</rdf:li>
          </rdf:Bag>
        </htmlVersionsSupported>
      </rdf:Description>
```

```
</ccpp:component>
</rdf:Description>
</rdf:RDF>
```

CC/PP is designed in such a way that an origin server or proxy can perform some sort of content to device matching. CC/PP is designed to suit an adaptation algorithm. The sequence of steps in the general case would look something like the following (Fig. 2.6):

1. Device sends serialized profile model with request for content.
2. Origin server receives serialized RDF profile and converts it into an in-memory model.
3. The profile for the requested document is retrieved and an in-memory model is created.
4. The device profile model is matched against the document profile model.
5. A suitable representation of the document is chosen. At this stage the document to be returned can be chosen from a number of different versions of the same document (content switch on context) or it can be dynamically generated (content transcoding on context).
6. Document is returned to device and presented.

If a document or application is specific about how it should be displayed, or if there are several versions of the document or application for different devices, then the adaptation manager can ask the client context manager for detailed context information. The client context manager will enquire with the relevant awareness module and extract the necessary context information. This fine-grained approach allows a high level of adaptation to take place. In cases where the document does not provide profile information, or the profile is limited in description, the adaptation manager can obtain a general context class from the context manager and perform some limited adaptation. For example, some adaptation can still take place where the location of the user is important. The policy manager can specify some rules about how adaptation should take place when a user is at a certain location, regardless of the information provided in an application or document profile.

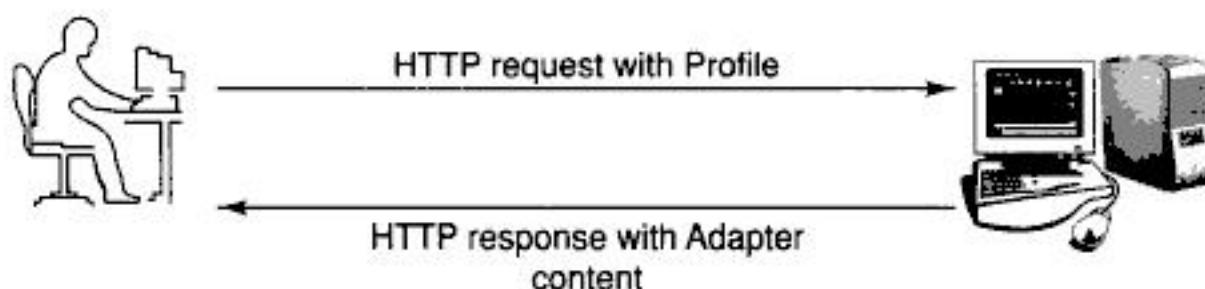


Figure 2.6 The Simplest Use of CC/PP

Policy Manager

The policy manager is responsible for controlling policies related to mobility. A policy is a set of rules; these rules need to be followed under different conditions. Introduction of mobility within an enterprise brings with it different types of challenges that are not normally seen in traditional computing environments. When we consider mobility, it is assumed that the data or information will be visible from outside the four walls of the enterprise. Organizations generally have policies regarding the disclosure of information. For example, documents from certain systems can be

printed only on certain printers in the organization. Some hard copy documents may be viewed only at the office of the CEO. These kinds of policies must be transferable to a mobile computing environment. Mobile computing policy manager will be able to define policy for documents/services and assign roles to users. Each role will have permissions, prohibitions and obligations associated with it. Each policy will have access rights associated with respect to read, write, execute. A policy in combination with role and current context information will be able to determine what actions a user is allowed to perform, or what actions a user is obligated to perform.

Semantic Web

As mentioned earlier, policies are sets of rules. When we drive in the street we are expected to follow the right of way. In a party there are some etiquettes to be followed. We humans learn these rules, policies, laws, and etiquettes from documents or experienced people. This is to help us to behave correctly in the society. The question is how to make a machine understand policies and make them behave in the expected fashion? Data in the Web is generally hidden away in HTML files, how do we determine which content is useful in some contexts, but often not in others. Facilities to put machine understandable data on the Web are becoming a necessity. The Semantic Web is targeted to address this need. The idea is of having data on the Web defined and linked in a way that it can be used by machines not just for display, but for automation, security, filtering, integration and reuse of data across various applications.

Semantic Web technologies are still very much in their infancy. It is believed that a large number of Semantic Web applications can be used for a variety of different tasks, increasing the modularity of applications on the Web. The Semantic Web is generally built on syntaxes which use URIs to represent data, usually in tuple-based structures, i.e., many tuples of URI data that can be held in databases, or interchanged on the World Wide Web using a set of particular syntaxes developed especially for the task. These syntaxes are called RDF (Resource Description Framework) syntaxes.

Security Manager

The Security Manager provides a secure connection between the client device and the origin server. Depending on the security policies of an organization, if the security requirements are not met or some content is not be viewable the security manager will ensure security with respect to:

- *Confidentiality*: The message being transacted needs to be confidential. Nobody will be able to see it.
- *Integrity*: The message being transacted needs to be tamper-resistant. Nobody will be able to change any part of the message.
- *Availability*: The system will be available. Nobody will be able to stop the service.
- *Non-repudiation*: Users of the system can be identified. Nobody after using the system can claim otherwise.
- *Trust*: There are complex issues of knowing what resources, services or agents to trust. The system will be trusted.

Confidentiality is managed by encryption. Using encryption techniques we change the message to some other message so that it cannot be understood. There are different types of encryption algorithms and standards. In a defined environment like enterprise LAN or a VPN (Virtual Private Network), we can standardize some encryption algorithm like 128 bits AES to be used. However,

in a ubiquitous environment, the environment is unpredictable with ad-hoc groups of devices. Also, the networks and their security level cannot be guaranteed all the time. Integrity can be managed using different hashing algorithms. Availability relates to peripheral security related to Web server, firewall, etc. Non-repudiation can be managed with digital signatures. For trust we may need to establish some sort of third-party recommendation system. Third-party rating system can also help establish trust. The security manager needs to manage all these aspects.

Platform for Privacy Preference Project (P3P)

The Platform for Privacy Preference Project (P3P) is an emerging standard defined by W3C. P3P enables web sites to express their privacy practices in a standardized format so that they can be retrieved and interpreted by user agents. With P3P, users need not read the privacy policies they visit; instead, key information about the content of the web site can be conveyed to the user. Any discrepancies between a site's practices and the user's preferences can be flagged as well. The goal of P3P is to increase user trust and confidence in the Web.

P3P provides a technical mechanism to inform users about privacy policies about the site. This will help users to decide whether to release personal information or not. However, P3P does not provide any mechanism for ensuring that sites act according to their policies. P3P is intended to be complementary to both legislative and self-regulatory programs that can help enforce web site policies.

Adaptability Manager

The Adaptability Manager is responsible for adapting content, behavior and other aspects according to context and policy. The adaptability manager may take any number of actions depending on the information passed to it by the context manager. This information may or may not be in the form of RDF. The most obvious action to perform is to transcode content so that it may be viewed on a particular device. Other actions might include appending location-specific information to documents.

Content Adaptation and Transcoding

In a ubiquitous situation, services are used from any device through any network. Therefore, the content should be able to adapt to these dynamic situations. The adaptation may be static or dynamic.

Content adaptation can be performed either at the content level at the server end or at the agent level in the client device. Content adaptation can be done at an intermediate level in a middleware framework as well. To do a good job of content adaptation, we need to go beyond the header. We need to consider the requirements of the entire Web page or relationships between its various components in different media. It also needs to look at adaptation within the scope of the same and a different modality. Modes can be audio, video, voice, image or text. We are differentiating between audio and voice by the characteristics that audio is a sound clip as an object like the audio part of a multimedia lecture, whereas voice is real-time and synthesized from some other form or representation. Content adaptation needs to consider the following attributes.

1. **Physical capabilities of the device:** Screen size, i.e., width and height in pixels, color and bits/pixel.
2. **Logical capabilities of the device:** Required for displaying video, image and playing audio.

3. Effective network bandwidth.

4. Payload: The total amounts of bits that can be delivered to the agent for the static parts. For streaming media this will be the initial buffer space required before the media starts playing. For storage constrained devices, the payload will be defined as the storage space.

Transcoding can be classified as the following:

- *Spatial transcoding* is transcoding in space or dimension. In this transcoding technique a standard frame is downscaled and reduced. The frame is changed from one size to a different size to suit the target device.
- *Temporal transcoding* copes with a reduction of number of frames in the time scale. This technique downscales the number of transferred frames to suit the target device and network bandwidth.
- *Color transcoding* is sometimes requested for monochrome clients. Using less bits for pixel can reduce bandwidth and sometimes modify the perception of images.
- *Code transcoding* is used to change coding from one standard to another. One such example could be compression of the data or transcode a BMP file to WBMP for wireless device.
- *Object or semantic transcoding* comprises some different techniques based on computer vision techniques. The goal is to extract semantically valuable objects from the scene and transfer them with the lower amount of compression in order to maintain both details and speed.

Server side content adaptation can be achieved through the concept of InfoPyramid. InfoPyramid creates context-aware content through static transcoding. The transcoding is done off-line at the content creation time. InfoPyramid is used to store multiple resolutions and modalities of the transcoded content, along with any associated meta-data. For server side adaptation, each atomic item of the document is analysed to determine its resource requirements. The types of resources considered are those that may differentiate different client devices. The resource requirement is determined by the following attributes.

1. Static content size in bits.
2. Display size such as height, width and area.
3. Streaming bit-rate.
4. Color requirements.
5. Compression formats.
6. Hardware requirements, such as display for images, support for audio and video.

This is very useful for enterprises whose users are likely to use the service from different networks and devices. For example, a bank or a courier company which has its customer base across the world and is likely to use the service from any device from any network. When the Web server receives a user request, it determines the capabilities of the requesting client device. A customization module (context-sensitive content switch) dynamically selects the page from the InfoPyramids. The selection is based on the resolutions or modalities that best meet the client capabilities. This selected content is then rendered in a suitable delivery format for delivery to the client. This type of transcoding is most suitable for enterprises where the content type is known.

In case of client-side adaptation, the adaptation is done by the agent application. The agent application does the adaptation based on its capabilities. For example, let us assume that the client device does not support color; therefore, a color image received by the agent will be displayed as a black and white image. Client-side adaptation can be quite effective for static images. However, it may not be very effective for streaming payload delivery.

The other technique of transcoding is through a middleware. One big benefit of the middleware approach is that it is totally transparent to the device and the content. Content providers do not have to change the way they author or serve content. However, there are a number of drawbacks to this approach:

1. Content providers have no control over how their content will appear to different clients.
2. There may be legal issues arising from copyright that may preclude or severely limit the transcoding by proxies.
3. HTML tags mainly provide formatting information rather than semantic information.
4. Transcoding sometimes could be difficult to apply to many media types such as video and audio.
5. Developing a general purpose transcoding engine is very difficult if not impossible.

Transcoding through middleware is transparent to both device and content. Therefore, this transcoding technique has to be very robust and universal. That is why this transcoding technique is the most difficult to engineer. It is most desirable for content aggregators and value-added service providers.

Content Rating and Filtering

Any city in the world has regions well marked like business district, residential area, shopping complex, so on and so forth. In Bangalore, for example, Commercial Street, Koramangala, and Shivaji Market signify commercial/shopping area, residential area and market place respectively. By looking at the name of a web site or the document header, can we make some judgement about the content? This is necessary for content filtering and personalization. If we want to make sure that children at home are not accessing some restricted material, how do we do this? In a bookstore, adult magazines are displayed on the topmost shelf so that children cannot reach them. Children below 18 are not allowed to buy cigarettes or alcohol from a shop. In Internet, everything is freely accessible. How do we enforce such social discipline in the electronic world?

W3C has proposed a standard called PICS (Platform for Internet Content Selection) for rating of web content. Filtering of the content can take place depending on this rating. PICS specification is a set of technical specifications for labels (meta-data) that help software and rating services to work together. Rating and labeling services choose their own criteria for proper identification and filtering of the content. Since rating will always involve some amount of subjective judgement, it is left to the service provider to define the ratings. Rating can be through self-labeling or third-party labeling of content. In third-party labeling some independent rating agency can be used. The rating of Internet sites was originally designed to help parents and teachers control what children access on the Internet, but it also facilitates other uses for labels, including code signing and privacy.

The RSACI (Recreational Software Advisory Council Internet) has a PICS-compliant rating system called Resaca. Web pages that have been rated with the Resaca system contain labels recognized by many popular browsers like Netscape and Internet Explorer. Resaca uses four categories—violence, nudity, sex, and language—and a number for each category indicating the

degree or level of potentially offensive content. Each number can range from 0, meaning the page contains no potentially offensive content, to 4, meaning the page contains the highest levels of potentially offensive content. For example, a page with a Resaca language level of 0 contains no offensive language or slangs. A page with a language level of 4 contains crude, vulgar language or extreme hate speech. When an end-user asks to see a particular URL, the software filter fetches the document but also makes an inquiry to the label bureau to ask for labels that describe that URL. Depending on what the labels say, the filter may block access to that URL. PICS labels can describe anything that can be named with a URL. That includes FTP and Gopher. E-mail messages do not normally have URLs, but messages from discussion lists that are archived on the Web do have URLs and can thus be labeled. A label can include a cryptographic signature. This mechanism lets the user check that the label was authorized by the service provider.

While the motivation for PICS was concern over children accessing inappropriate materials, it is a general “meta-data” system, meaning that labels can provide any kind of descriptive information about Internet material. For example, a labeling vocabulary could indicate the literary quality of an item rather than its appropriateness for children. Most immediately, PICS labels could help in finding particularly desirable materials, and this is the main motivation for the ongoing work on a next generation label format that can include arbitrary text strings. More generally, the W3C is working to extend Web meta-data capabilities generally and is applying them specifically in the following areas:

1. Digital Signature: Coupling the ability to make assertions with a cryptographic signature block that ensures integrity and authenticity.
2. Intellectual Property Rights Management: Using a meta-data system to label Web resources with respect to their authors, owners and rights management information.
3. Privacy (P3): Using a meta-data system to allow sites to make assertions about their privacy practices and for users to express their preferences for the type of interaction they want to have with those sites.
4. Personalization: Based on some policy, the content can be personalized to suit the need of the user and the service.

Regardless of content control, meta-data systems such as PICS are going to be an important part of the Web, because they enable more sophisticated commerce (build and manage trust relationships), communication, indexing, and searching services. Content filtering can take place either at the client end or at the middleware proxy end.

Content Aggregation

Over a period, the dynamics associated with the content has changed considerably. Earlier, there was a requester requesting for content and a responder responding to the content requested. The game was simple with only two players, the requester and the responder. These contents were corporate content or content for the mass (primarily web sites). There was no concept of charging for the content. Today there is a concept of OEM (Original Equipment Manufacturer) in content. There are some organizations which create content like an OEM. There are other ASPs (Application Service Providers), MVNOs (Mobile Virtual Network Operators), and content aggregators who source content from these OEMs and provide the content as a value added service to different individuals, content providers, and network operators.

In the current scenario, there are primarily four parties involved; they are end user (EU), the content provider (CP), the content aggregator (CA), and the ISP (Internet Service Provider) or the wireless or wireline network operator (NO). The network operator will have routers, cache, gateways and other nodes to offer the service. In this scheme anybody can become a requester or a responder. There could be different parameters, which will determine the content. These parameters are of two types, static and dynamic. The static adaptation parameters are those which can be received before the service begins. The content is adapted, based on this parameter. The dynamic adaptation parameters are those which are required with every request. For example, a user may initiate a request for a MPEG stream. The NO will transcode the stream to suit the bandwidth of the end user and delivers the same to the user. However, through a dynamic parameter, the user can specify a different parameter for transcoding.

From the content aggregator's perspective we may classify the service into two categories:

1. Single service request: This works at the user level and works for only one user. For example, a user may request the proxy server at the NO to translate the page into Hindi and then deliver the same to the user. In this case, the end user buys the content and the translation service.
2. Group service request: This works for a group of users. This type of request is initiated either at the CA level or the NO level. For example, the content aggregator has some arrangement for advertisement. The content aggregator examines all the HTML pages and inserts an advertisement at an appropriate place.

Seamless Communication

The basic premise of a ubiquitous system is that the system will be available and accessible from anywhere, anytime and through any network or device. A user will be able to access the system after moving from one place to another place (foreign place). The user will also be able to access the system while on the move (traveling mode). Mobile healthcare professionals, for example, may need to seamlessly switch between different modes of communication when they move from indoors to outdoors. A corporate user requires a similar kind of facility as well. Also, what is necessary is, during the movement, the session needs to continue. If we take the example of healthcare sector, some data and information are exchanged between the patient and the hospital. While the patient is moved from home, to ambulance, to a helicopter, to the hospital, the information exchange has to continue without any interruption.

Seamless communication will combine seamless handoffs and seamless roaming. Handoff is the process by which the connection to the network (point of attachment) is moved from one base station (access point) to another base station within the same network. Whereas, roaming will involve the point of attachment moving from one base station of one network to another base station of another network. The basic challenge in handoff is that it has to work while a session is in progress. Cellular technology with respect to voice has reached a level of maturity where a seamless voice communication is possible through handoff and roaming. The data technology is yet to mature to provide a similar level of service. In some parts of the world, handoff is termed as handover.

Seamless communication offers users freedom to roam across different wireless networks. Roaming works within homogeneous networks, like GSM to GSM or CDMA2000 to CDMA2000.

Nowadays, roaming is also possible from GSM to CDMA2000 network and vice-versa provided the user device is dual band and can connect to both these networks. True seamless roaming will include handoff and roaming in a heterogeneous hybrid network. The user will move from a WiFi to 3G to wired LAN to GSM while the session is in progress. Users will be able to communicate using whatever wireless device is currently at hand. Thus, GPRS-enabled cell phones, PDAs and laptops will be able to roam and communicate freely and access the Internet across both WLANs and WWANs.

In seamless roaming, the following aspects need to be maintained and managed in a seamless fashion without any disruption of service:

1. Authentication across network boundaries.
2. Authorization across network boundaries.
3. Billing and charging data collection.
4. End-to-end data security across roaming.
5. Handoff between wireless access points.
6. Roaming between networks.
7. Session migration.
8. IP mobility.

The task of managing authentication between client devices and networks, often involving multiple login names and passwords, will become automatic and invisible to the user, as will the configuration of various settings and preferences that accumulate with client devices.

Autonomous Computing

The world is heading for a software complexity crisis. Software systems are becoming bigger and more complex. Systems and applications cover millions of lines of code and require skilled IT professionals to install, configure, tune and maintain. New approaches are needed to provide flexible and adaptable software and hardware, both for mobile devices and the intelligent environment. Ease of use will have some effect on acceptance of a ubiquitous system. The scale of these ubiquitous systems necessitates “autonomic” systems. The purpose of autonomous system is to free users and system administrators from the details of system operation and maintenance complexity. Also, the system will run 24×7 . The essence of autonomous system is self-management, which is a combination of the following functions:

1. **Self-configurable:** An autonomous system will configure itself automatically in accordance with high-level policies. This will suit the functional requirement of the user.
2. **Self-optimizing:** An autonomous system will continuously look for ways to improve its operation with respect to resource, cost and performance. This will mean that an autonomous system will keep on tuning hundreds of tunable parameters to suit the user and the environment.
3. **Self-healing:** An autonomous system will detect, diagnose and repair localized problems resulting from bugs or failures. These failures could be the result of either software or hardware failure.
4. **Self-protecting:** An autonomous system will be self-protecting. This will be from two aspects. It will defend itself from external attacks; also, it will not propagate or cascade failure to other parts of the system.

5. **Self-upgradable:** An autonomous system will be able to grow and upgrade itself within the control of the above properties.

Design tools and theories may be needed to support large-scale autonomic computing for small devices.

2.6.2 Context Aware Systems

The role of a context manager is to maintain information pertaining to location, mobile devices, network, users, the environment around each mobile device and any other context information deemed relevant. Following is a description of these information and relevance in the mobile computing environment.

- *Location information:* This feature helps us to identify the location of the user/device. This can be achieved in either of the two ways. One is through the device and the other is through the network. From the device, the best way to find the location is through GPS (Global Positioning Systems). GPS-based systems can offer location information to a precision of 10 feet radius. Also, the location of the base station with which the device is associated can help us to get the location information. In certain networks, GSM for example, the base station location can be obtained from the device through the CID (Cell ID) value. From the network side the location of the device can be determined through timing advance technology. However, this information relates to a point when a successful call was made. Base-station-based location information is likely to be correct to the precision of 100 feet radius.
- *Device information:* This feature helps us to know the characteristics of the device. This is required to determine the resource capability and the user interface capability. In a mobile computing environment the user will move from device to device. Therefore, it is essential to know the device context. Device information can be obtained from the device and from the network. Through the User-Agent parameter of HTTP protocol we can get some information about the device. As this information is provided by the browser in the device, the information is very generic. This does not give the device properties like color, pixel capability, display size, etc. From the network side, the information about the device can be obtained from the EIR (Equipment Identity Register) database of the network. In all the wireless networks (GSM, GPRS, UMTS, 3G) we have the EIR. However, we do not have any concept of EIR in wireless LAN or WiFi.
- *Network information:* In a mobile computing environment, the user moves from network to network. Sometime they are even heterogeneous in nature. Network information is required to identify the capability of the network. Capability information will include security infrastructure, services offered by the networks, etc. For example, while roaming a user moves from a GPRS network to a GSM network. Therefore, the rendering may need an adaptation from WAP to SMS. In the future, some of these will be done through programmable networks.
- *User information:* This information is required to identify the user correctly. From the security point of view, the system needs to ensure that the user is genuine and is who he claims to be. We need to ensure that nobody else is impersonating. This information can be validated

through authentication independent of device or network. However, user preferences' information need to be obtained from the network. For charging the user properly we need to refer to some subscriber information available in the network.

- *Environment information:* This includes ambient surrounding awareness. We need to know the temperature, elevation, moisture, and other ambient-related information which are necessary for sensor-based networks.

For a general mobile-computing environment we need information related to location, network, user, and device. We also notice that for a majority of the parameters we need to access the information available in different databases within the network. These information are being available through different network interfaces of intelligent networks. These interfaces are Softswitch (<http://www.softswitch.org>), JAIN (Java API for IN <http://java.sun.com/products/jain>), Parlay (<http://www.parlay.org>), and TINA (www.tinac.com). These are explained in Chapter 11.

GPS

Global Positioning System (GPS) is a system that gives us the exact position on the Earth. GPS is funded by and controlled by the US Department of Defense. There are GPS satellites orbiting the Earth, which transmit signals that can be detected by anyone with a GPS receiver. Using the receiver, we can determine the location of the receiver. GPS has three parts: the space segment, the user segment, and the control segment.

The space segment consists of 24 satellites, each in its own orbit 11,000 nautical miles above the Earth. Each GPS satellite takes 12 hours to orbit the Earth. Each satellite is equipped with an accurate clock to let it broadcast signals coupled with a precise time message.

The user segment consists of receivers, which can be in the users' hand, embedded in a mobile device or mounted in a vehicle. The user segment receives the satellite signal which travels at the speed of light. Even at this speed, the signal takes a measurable amount of time to reach the receiver. The difference between the time the signal is sent and the time it is received, multiplied by the speed of light, enables the receiver to calculate the distance to the satellite. To measure precise latitude, longitude and altitude, the receiver measures the time it took for the signals from four separate satellites to get to the receiver. If we know our exact distance from a satellite in space, we know we are somewhere on the surface of an imaginary sphere with radius equal to the distance to the satellite radius. If we know our exact distance from four satellites, we know precisely where we are on the surface of the earth.

2.7 MOBILE COMPUTING THROUGH INTERNET

We discussed that a network can be divided into three major functional areas, namely, core, edge and access. Likewise, we can divide a ubiquitous network into three functional areas. Out of the three, the core and the edge are likely to be Internet and internet. By internet we define a network which is a combination of various networks and interworks with one another, whereas Internet with the uppercase I is the Internet we know. For mobile and ubiquitous computing, the access network will be both wireless and wired networks. In the case of wireless access network, it could range from infrared, Bluetooth, WiFi, GSM, GPRS, IS-95, CDMA, etc. For wired, it is expected to

be some kind of LAN. In the case of wired network the bandwidth is higher, stable and the device is likely to be a workstation with a large memory and display. Also, such devices are not constrained by the limited battery power.

When the user-facing device is a wired device, the complexity and challenges are far less. However, some of the constraints for wireless can still apply in the case of wired devices and networks. Therefore, from the mobile computing client point of view, consideration for a wired device will be the same as a wireless client.

2.8 MAKING EXISTING APPLICATIONS MOBILE-ENABLED

There are many applications that are now being used within the intranet or the corporate network, that need to be made ubiquitous. These are different productivity tools like e-mail or messaging applications, workflow systems, etc. Information systems for partners and vendors and employees like sales force automation, etc. will also fall within this category. These applications need to be made ubiquitous and mobile-computing capable. There are many ways by which this can be achieved.

1. **Enhance existing application:** Take the current application and enhance it to support mobile computing.
2. **Rent an application from an ASP:** There are many organizations which develop ubiquitous application and rent the same at a fee.
3. **Write a new application:** Develop a new application to meet the new business requirement of mobile computing.
4. **Buy a packaged solution:** There are many companies which are offering packaged solutions for various business areas starting from manufacturing to sales and marketing. Buy and install one of these which will also address the mobile computing needs of the enterprise.
5. **Bridge the gap through middleware:** Use different middleware techniques to face-lift and mobile-computing-enable the existing application.

One of these techniques, or any combinations can be used to make an application ubiquitous. If the enterprise has a source code for the application, enhancement of the existing application may be a choice. Writing a new application by taking care of all the aspects described above may also be a possibility. Buying a package or renting a solution from an ASP can also be a preferred path for some business situations.

Many of these applications might have been developed in-house, but may not be in a position to be enhanced. Some might have been purchased as products. A product developed by an outside agency cannot be enhanced or changed as desired. In many such situations, mobile computing enabling can be done through middleware. The combination of communication and application middleware can be used to make an application mobile. Let us assume that the enterprise has its sales and distribution application running in SAP in IBM AS/400 system. The enterprise wants this system to be wireless-enabled for its mobile sales force. Using TN5250 communication middleware, the application can be abstracted as an object. Through a transaction processing middleware and APIs, the SAP application can be used as a document. By using a transcoding middleware, the application can be wireless-enabled and used through WAP, J2ME or even SMS (Short Message Service). Through middleware, some additional security features can be added.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

- (c) Policy Manager
- (d) Security Manager
- (e) Semantic Web
- (f) P3P

Q7: What is content adaptation? What are the various classifications of transcoding? How can the two be helpful for various device classes?

Q8: How is content rating and filtering helpful in classifying content? What is the role of RSACI and PICS in classifying content?

Q9: You have been asked to develop a location aware restaurant guide system for the Restaurant Foundation of India. Describe four main functions of this system. Describe how will you implement these four functions?

Q10: What is seamless communication? How can seamless communication help in an emergency service rescue operation?

Q11: What is a context aware system? What all can be the types of information needed for developing a fully context aware system?

Q12: Write brief notes on:

- (a) GPS
- (b) Mobile Computing through Internet

Q13: Discuss with examples how existing applications can be made mobile.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

- finds the right way to connect the caller's line to the line being called.
- checks if the desired line is free.
- makes the connection, and
- notes down the call details: time of call, duration of call, calling number and called number.

Having removed the need for an operator in the automated exchange, a system was necessary to indicate progress of the call to the caller. A series of distinct tones were generated by a machine called Ring Generator. The tones produced were as follows:

- *Dial Tone (DT)*: This is a signal applied to the line after the calling party (A party) has lifted his handset and the switching equipment has allocated him an available outlet (a circuit) for this call to proceed.
- *Busy Tone (BT)*: Busy tone indicated either that the called subscriber (B party) is already off-hook (busy) or that the route to the called subscriber is congested.
- *Ring Tone (RT)*: When a circuit between A party and the B party is established, the telephone rings at B party's end and a ring tone is generated for the A party.

A normal telephone system is called Public Switched Telephone Network (PSTN). PSTN nodes can be subdivided into three main categories: local exchanges (also known as end office), transit exchanges (also known as local access tandem) and international exchanges (also known as interexchange carrier). Local exchanges are used for the connection of subscribers. Transit exchanges switch traffic within and between different geographical areas. International exchanges, and other gateway-type exchanges switch traffic to telecommunication networks in foreign countries and other networks. A physical wire (also known as local loop) is laid from the local exchange to the telephone device at each subscriber's place. This is traditionally also known as the last mile. In case of a wireless network like GSM or WiLL (Wireless in Local Loop), there is no wire from the local exchange to the telephone. The communication between the local exchange and the telephone device is managed over the wireless radio interface. In India, there are network operators who are offering basic or fixed telephone, WiLL, and GSM.

3.2 MULTIPLE ACCESS PROCEDURES

In a PSTN network, a separate physical wire is used to connect the subscriber's telephone with the switch. Therefore, multiple users can have speech communication at the same time without causing any interference to each other. The scene is different in the case of wireless communication. Radio channel, used in a wireless network, is shared by multiple subscribers. Unless we control simultaneous access of the radio channel (by multiple users), collisions can occur. In a connection-oriented communication, a collision is undesirable. Therefore, every mobile subscriber must be assigned a dedicated communication channel on demand. This is achieved by using different multiplexing techniques (Fig. 3.1).

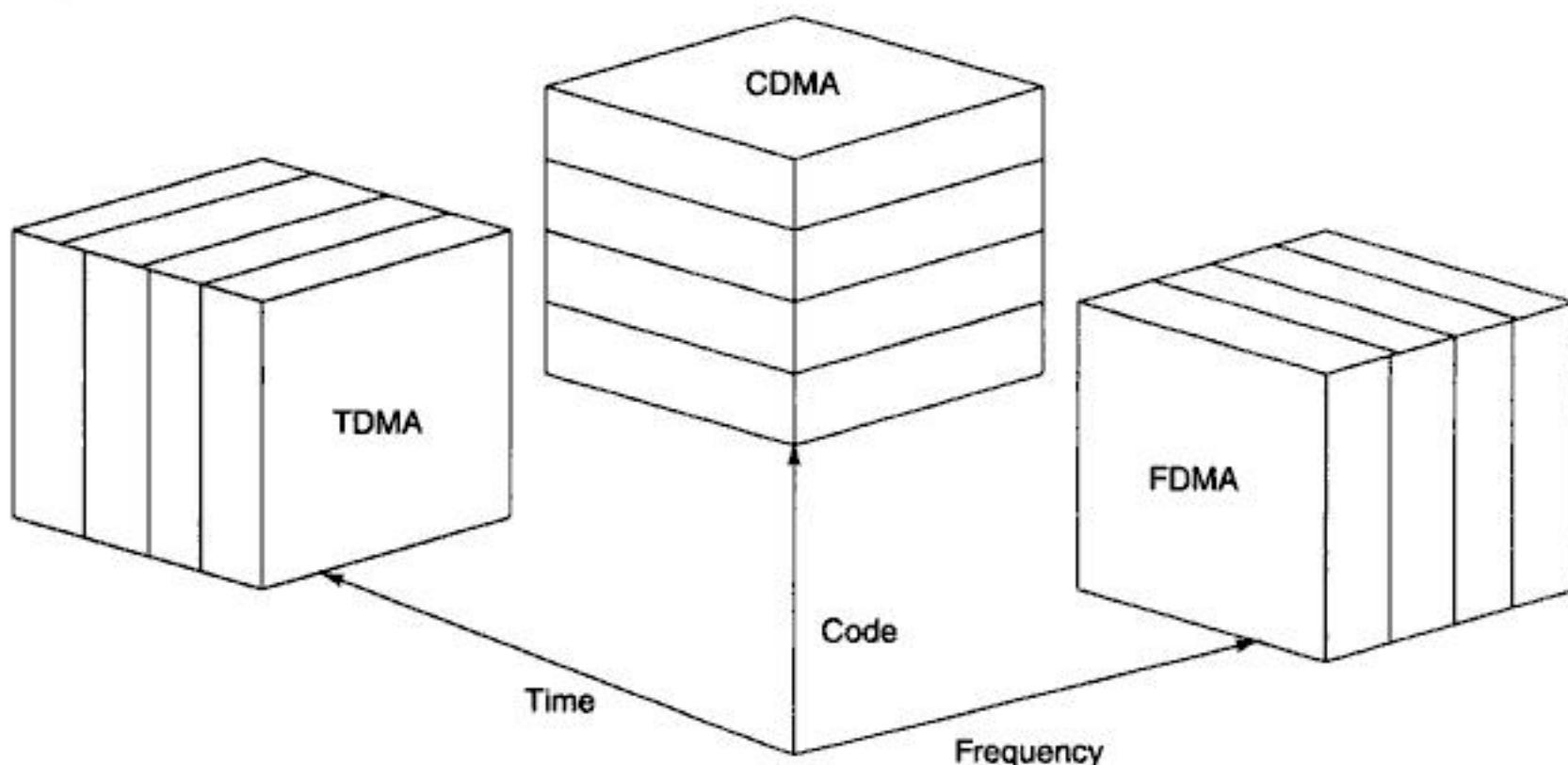


Figure 3.1 Multiple Access Procedures

3.2.1 Frequency Division Multiple Access

Frequency Division Multiple Access (FDMA) is one of the most common multiplexing procedures. The available frequency band is divided into channels of equal bandwidth so that each communication is carried on a different frequency. This multiplexing technique is used in all the first generation analog mobile networks like Advanced Mobile Phone System (AMPS) in the US and Total Access Communication System (TACS) in the UK.

3.2.2 TDMA Variants

Time Division Multiple Access (TDMA) is a multiplexing technique where multiple channels are multiplexed over time. Assuming that we have a 64Kbps channel to transmit one voice channel; but we are having a high speed carrier of 2Mbps ($32 * 64\text{Kbps}$), we can transmit this voice channel in $1/32$ second. This implies that we can theoretically divide the 2Mbps channel into a 32 time-slot and use one of them for transmission of our voice channel. In TDMA, several users share the same frequency channel of higher bandwidth by dividing the signal into different time slots. Users transmit their data using their own respective time slots in rapid succession; to synchronize, the transmitter and the receiver need to synchronize using a global clock.

Figure 3.2 shows that a TDMA system divides its transmission medium into frames which are repeated indefinitely (one after another). Each TDMA frame is then divided into time slots of same temporal width that are allotted to individual users. TDMA is a very common multiplexing technique and used in many digital transmissions like GSM, IS-136, SS7, satellite systems, etc.

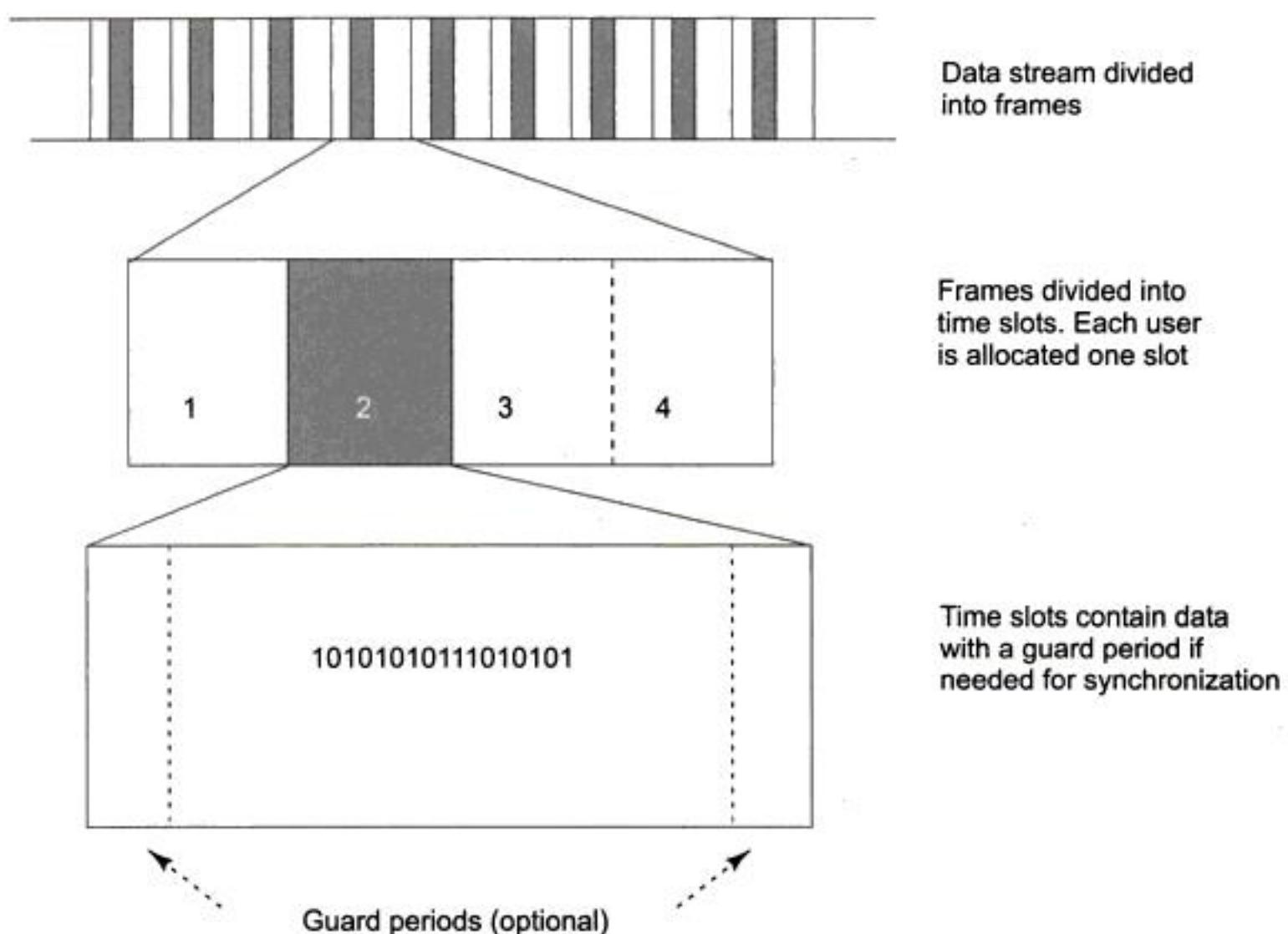


Figure 3.2 TDMA Frames and Time Slots

Fixed TDMA

In Fixed TDMA, connections between time slots in each frame and data streams assigned to a user remain static and switched only when large variations in traffic are required. In this variant of TDMA, the slot sizes are fixed at T/N (where T is time in seconds and N is the number of users). If a station does not transmit during its assigned slot, then the corresponding bandwidth is wasted. This variant is simple to implement but performs poorly since the entire bandwidth is not used.

Dynamic TDMA

In Dynamic TDMA or Dynamic Reservation TDMA (DR TDMA), a scheduling algorithm is used to dynamically reserve a variable number of time slots in each frame to variable bit-rate data streams. This reservation algorithm is based on the traffic demand of each data stream. The fixed length DR TDMA frame is time-duplexed into an uplink and downlink channel and the boundary between these two parts is dynamically adjusted as a function of the traffic load.

Packet Reservation Multiple Access

Packet Reservation Multiple Access (PRMA) is a packet based TDMA where the users contend for the time slots. In PRMA, a user can reserve a time slot in advance for future use and optimize the bandwidth in radio transmission. The two prominent variants of PRMA are Dynamic PRMA (DPRMA) and PRMA Hindering States (PRMA HS). In DPRMA, each mobile station is responsible

for making a reasonable estimate of its bandwidth requirements and then request for resource allocation to the base station. It aims to closely match each user's transmission rate with its packet generation rate. PRMA HS in contrast allows a terminal to transmit during the time interval needed to receive the outcome of a reservation attempt. PRMA HS is used for the uplink of Low Earth Orbit (LEO) satellite mobile communications.

3.2.3 Code Division Multiple Access

Code Division Multiple Access (CDMA) is a broadband system. CDMA uses spread spectrum technique where each subscriber uses the whole system bandwidth. Unlike the FDMA or TDMA where a frequency or time slot is assigned exclusively to a subscriber, in CDMA all subscribers in a cell use the same frequency band simultaneously. To separate the signals, each subscriber is assigned an orthogonal code called "chip".

3.2.4 Space Division Multiple Access

Along with TDMA, FDMA, and CDMA, we need to make use of the space effectively. Space division multiple access (SDMA) is a technique where we use different parts of the space for multiplexing. SDMA is used in radio transmission and is more useful in satellite communications to optimize the use of radio spectrum by using directional properties of antennas. In SDMA, antennas are highly directional, allowing duplicate frequencies to be used at the same time for multiple surface zones on earth. SDMA requires careful choice of zones for each transmitter, and also requires precise antenna alignment.

3.3 SATELLITE COMMUNICATION SYSTEMS

On October 4, 1957 Union of Soviet Socialist Republics (USSR) scientists placed the first manmade artificial satellite name **Sputnik** in earth's orbit. Four months later, the US matched it by sending **Explorer 1** into earth's orbit. Because a satellite orbits around the earth, part of the earth is always within the satellite's range; therefore, technically it is possible to use satellites for communications, military, or even spying functions.

In 1960, the world's first communication satellite **Echo 1** was launched by the US. Echo 1 was a passive communication satellite to communicate across the US and across the Atlantic Ocean by reflecting signals using a large aluminized plastic balloon (100 feet in diameter). It reflected Radio and TV signals transmitted to the satellite back to the earth station within view of the satellite. Being a low orbit satellite, Echo 1 circled the earth every 90 minutes; therefore, everybody on earth could eventually see it sometime, but, no single person, ever saw it for more than 10 minutes out of every 90 minute orbit—this means, it could not be used for long communication. In 1958, the **Score** satellite was put into earth's orbit that worked as a relay agent—it carried a tape recorder that would record messages as it passed over an originating station and then rebroadcast them as it passed over the destination station.

The major limitation of a passive satellite was that it needed high transmission power to overcome transmission loss. **Telstar 1** launched on July 10, 1962 was the first active communication satellite. It was also a low orbit satellite but it could see Europe and the US simultaneously during one part of its orbit and Japan and the US during another part of its orbit; as a result, it provided real-time communications between the US and those two regions—for a few minutes out of every hour.

3.3.1 Communicating through Satellite

Every communications satellite involves the transmission of information from an originating ground station to the satellite followed by a retransmission of the information from the satellite back to the ground called the uplink and the downlink respectively (Fig. 3.3). Hence, the satellite must have a receiver with receive antennas, and a transmitter with transmit antennas. It must also have some methods for connecting the uplink to the downlink for retransmission with amplification; also, it must have electrical power through solar energy to run all of the electronics. The downlink may either be to a select number of ground stations or may be broadcast to everyone over a large area.

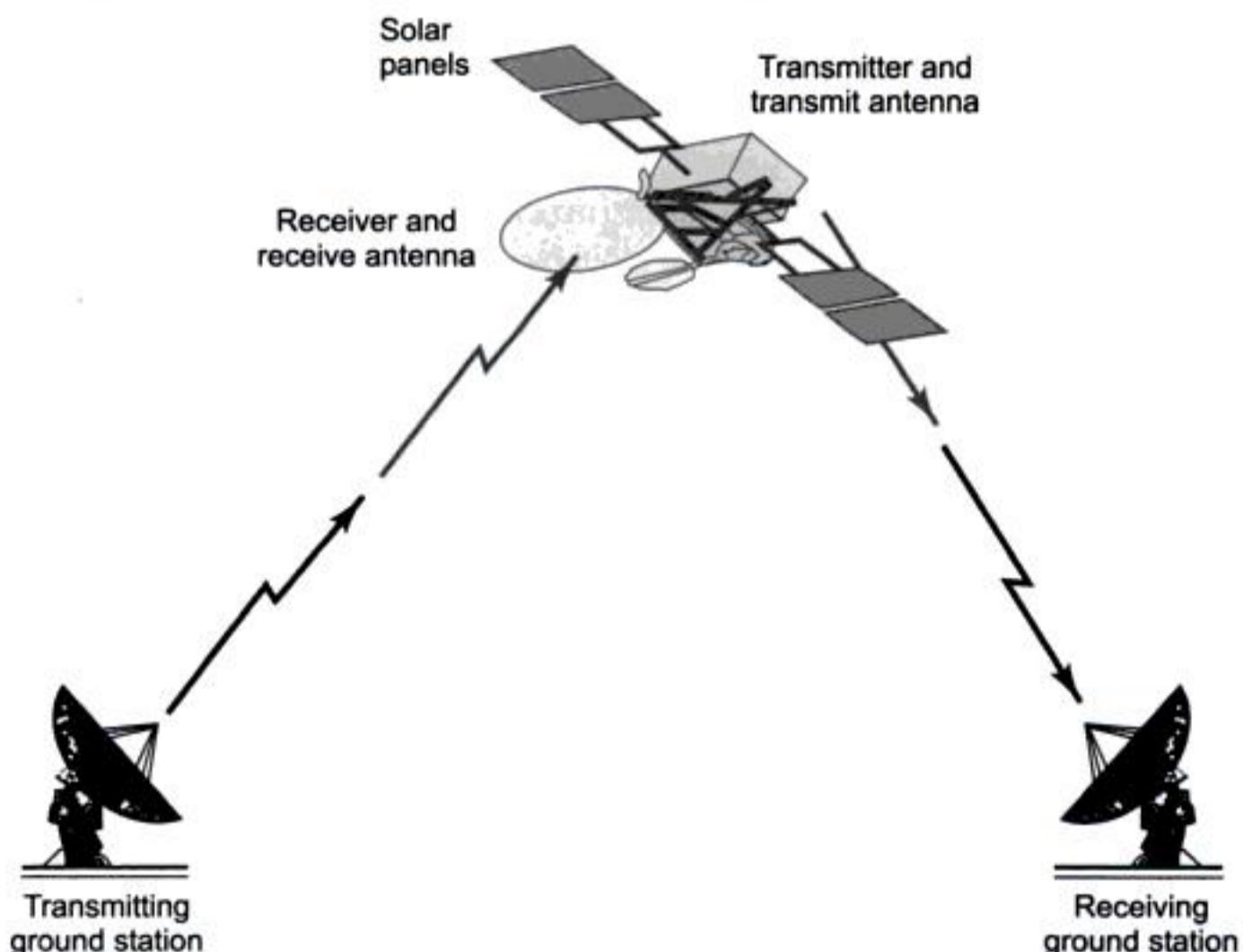


Figure 3.3 Satellite Communications System

A properly designed satellite antenna will concentrate most of the transmitter power within a designated area using space division multiplexing. One of the biggest differences between a low earth satellite and a geosynchronous satellite is in their antennas. All antennas in use today radiate energy preferentially in some direction. The most important application for communication satellites was in intercontinental long distance telephony. The fixed Public Switched Telephone Network relays telephone calls from land line telephones to an earth station, where they are then transmitted to a geostationary satellite. The downlink follows an analogous path.

3.3.2 Low Orbit Satellite

A Low Earth Orbit (LEO) satellite typically orbits around the earth about 400 kilometers above the earth's surface with a time period of about 90 minutes. These satellites are only visible from within a radius of roughly 1000 kilometers from the sub-satellite point. Sub-satellite point is the point of intersection of earth's surface with the straight line from the satellite to the center of earth. The greatest advantage of LEO satellite is that it does not need high powered rockets—making it less expensive to launch. Also, due to its proximity to the ground, LEO does not require high signal strength.

For uninterrupted communication services a large number of satellites are needed so that they communicate with each other and one of the satellites is in touch with the user. Unlike in a mobile telephone system where the user is mobile and transceivers are static, in LEO satellite system, user is relatively static compared to the transceiver, which is mobile.

3.3.3 Medium Orbit Satellite

Medium Earth Orbit (MEO), sometimes called Intermediate Circular Orbit (ICO), is the region of space around the earth above low earth orbit of 2,000 kilometres and below geostationary orbit of 35,786 kilometers. The most common use for satellites in this region is for navigation, such as the GPS (with an altitude of 20,200 kilometers). Communications satellites that cover the North and South Pole are also put in MEO. The orbital periods of MEO satellites range from about 2 to 24 hours. The MEO orbit has a moderate number of satellites.

3.3.4 Geostationary Satellite

In geostationary satellite the orbit of the artificial satellite is such that the orbital speed of the satellite is same as the speed of earth's rotation. Though the satellite is moving at a high speed, from earth it will always appear to be stationary—this is the reason for calling it geo-stationary. A Geostationary Earth Orbit (GEO) can be achieved only very close to the ring 35,786 km directly above the equator. This equates to an orbital velocity of 3.07 km/s or a period of 1436 minutes, which equates to almost exactly one sidereal day or 23.934461223 hours. The idea of a geostationary orbit was first proposed by Arthur C. Clarke in 1945; therefore, a geostationary orbit is also known as the Clarke Orbit. The GEO satellite could view approximately 42% of the earth. Therefore, a system of three GEO satellites, with the ability to relay messages from one GEO to the other could interconnect virtually all of the earth except the polar regions.

Unlike LEO or MEO, the GEO orbit is much higher—demanding high power rockets. In 1963, the necessary rocket booster power was available for the first time and the first geosynchronous satellite, **Syncom 2** was launched by the US into earth's orbit. Geosynchronous orbit is so far that the time to transmit a signal from earth to the satellite and back is approximately $\frac{1}{4}$ of a second—the time required to travel 36,000 km up and 36,000 km down at the speed of light. For telephone conversations, this delay can sometimes be annoying.

3.3.5 Satellite Phones

Initially satellite communication was being used for broadcast to stationary TV receivers, and transmission of telephone channels. However, demand on mobile phone made some companies to look into satellite phones that will connect a subscriber directly through the communication satellite, where the satellite will function as the transceiver station connecting the mobile phone. There are few companies that offer such facility; we describe some of them as case study.

- *Iridium*: Iridium comprises a group satellites working in concert as a satellite constellation. The Iridium constellation is used to provide voice and data communication to satellite phones, pagers and integrated transceivers over the entire surface of the earth. The constellation uses 66 active satellites in orbit along with spare in-orbit satellites to serve in case of failure. The satellites orbit the earth in roughly 100 minutes. Each satellite can support up to 1100 concurrent phone calls. Iridium satellites are in low earth orbit at a height of approximately 780 km with spare satellites at 667 km storage orbit. Spare satellites will be boosted to the correct altitude and put into service in case of failure of active the satellite. Satellites communicate with neighboring satellites via Ka band inter-satellite links. For more information on Iridium, please refer to www.iridium.com and www.satphoneusa.com/iridium/network.html.
- *Globalstar*: Globalstar is another mobile satellite voice and data services provider offering services to subscribers around the world. Globalstar uses 52 LEO satellites—48 satellites for communication with four satellites as spare. Globalstar's products include mobile and fixed satellite telephones, simplex and duplex satellite data modems and satellite airtime packages. Many land based and maritime industries make use of the various Globalstar products and services from remote areas beyond the reach of cellular and landline telephone service. For more information on Globalstar, please refer to www.globalstar.com.
- *Thuraya*: Thuraya is another satellite phone company that mainly services in Asia and Africa. Unlike Globalstar or Iridium that uses LEO, Thuraya uses three geostationary satellites. In all practical purpose Thuraya is a GSM (see Chapter 5) cellular telephone network with a satellite BTS (Base Transceiver System). All Thuraya phones use the same GSM SIM cards and can roam in any terrestrial GSM network around the world. Thuraya phones have a dual-mode feature that allows them to operate in the Thuraya satellite network or GSM terrestrial mobile networks while outside the satellite coverage. Thuraya subscribers can also switch to roaming GSM network if it is available. For more information on Thuraya, please refer to www.thuraya.com.

3.4 MOBILE COMPUTING THROUGH TELEPHONE

One of the early examples of mobile computing was accessing applications and services through voice interface. This technology was generally referred to as Computer Telephony Interface (CTI). Different banks around the world were offering telephone banking for quite sometime using this technology. In a telephone banking application, the user calls a number and then does his banking



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
35     tpt[0].tp_flags = TF_MAXDTMF; /* terminate if already in buf. */
36     tpt[1].tp_type = IO_CONT;
37     tpt[1].tp_termno = DX_LCOFF; /* LC off termination */
38     tpt[1].tp_length = 3; /* Use 30 ms (10 ms resolution * timer) */
39     tpt[1].tp_flags = TF_LCOFF|TF_10MS; /* level triggered, clear
40         history, * 10 ms resolution */
41     tpt[2].tp_type = IO_EOT;
42     tpt[2].tp_termno = DX_MAXTIME; /* Function Time */
43     tpt[2].tp_length = 100; /* 10 seconds (100 ms resolution * timer) */
44     /* clear previously entered digits */
45     if (dx_clrdigbuf(chdev) == -1)
46     {
47         /* process error */
48     }
49     /* Now play the file */
50     if (dx_play(chdev,&iott,&tpt,EV_SYNC) == -1)
51     {
52         /* process error */
53     }
54     /* get digit using dx_getdig( ) and continue processing. */
55     /* Set up the DV_TPT and get the digits */
56     if ((numdigs = dx_getdig(chdev,tpt, &digp, EV_SYNC)) == -1)
57     {
58         /* process error */
59     }
60     for (cnt=0; cnt < numdigs; cnt++)
61     {
62         printf("\nDigit received = %c, digit type = %d",
63             digp.dg_value[cnt], digp.dg_type[cnt]);
64     }
65     /* go to next state */
66     .
67     .
68     .
69 }
```

Line 16 is to open a channel for use in a Dialogic card. It is necessary to open the channel before any type of access of the same.

Line 50 is to play the voice file, which was pre-recorded with voice "Hello World". Pre-recorded voice files are recordings of normal voice and stored in digitized form. This can be done using normal telephone speaker and Dialogic card. However, in a majority of cases, this is done in a professional studio using professional people with a good voice.

In line 56 we read the digits entered through the telephone keypad.

3.6. VOICE XML

In mobile computing through telephone, the IVR is connected to the server through client/server architecture. It is also possible to host the IVR and the application on the same system. In the last few years, mobile computing through voice has come a long way. Today Internet (HTTP) is used in addition to client/server interface between the IVR and the server. This increases the flexibility in the whole mobile-computing architecture. HTTP is used for voice portals as well. In the case of a voice portal, a user uses an Internet site through voice interface. For all these advanced features, VoiceXML has been introduced. Recent IVRs are equipped with DSP (Digital Signal Processing) and are capable of recognizing voice. The output is synthesized voice through TTS (Text to Speech).

The Voice eXtensible Markup Language (VoiceXML) is an XML-based markup language for creating distributed voice applications. VoiceXML is designed for creating audio dialogs that feature synthesized speech, digitized audio, recognition of spoken voice and DTMF key input. Using VoiceXML, we can create Web-based voice applications that users can access through telephone.

VoiceXML supports dialogs that feature:

- Spoken input
- DTMF (telephone key) input
- Recording of spoken input
- Synthesized speech output (text-to-speech)
- Recorded audio output
- Dialog flow control
- Scoping of input

Architectural Model

The architectural model for VoiceXML is depicted in Figure 3.7. It has the following components:

A **Document Server** (e.g., a Web server) services requests from a client application. The client side of the application runs on a **VoiceXML Interpreter**, and is accessed through the **VoiceXML interpreter context**. The server delivers VoiceXML documents, which are processed by the VoiceXML Interpreter. The VoiceXML Interpreter Context is responsible for special actions on voice escape phrases.

For instance, in an interactive voice response application, the VoiceXML interpreter context may be responsible for detecting an incoming call, acquiring the initial VoiceXML document, and answering the call, while the VoiceXML interpreter manages the dialog after answer. The implementation platform generates events in response to user actions (e.g., spoken or character input received, disconnect) and system events (e.g., timer expiration).

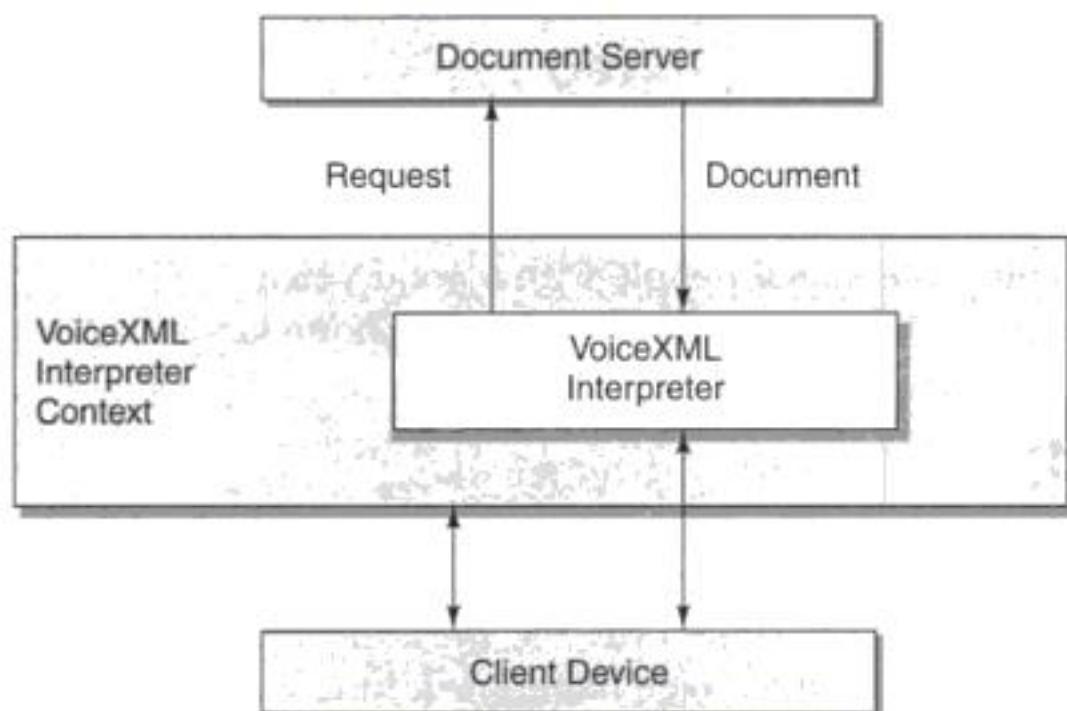


Figure 3.7 Voice XML Architectural Model

3.6.1 How Voice XML Fits into Web Environment

All of us are familiar with the web as it works today. We use a visual GUI web browser (such as Netscape Communicator or Internet Explorer), which renders and interprets HTTP requests to present information to the user (text, graphics, audio, multimedia, etc.). When the user makes a selection (for example, a click on a hyperlink), the web browser sends an HTTP request to the web server. The web server responds by locating the new page and returns the page to the user. The content server may also have to interact with a back-end infrastructure (database, servlets, etc.) to obtain and return the requested information.

The Voice Browser extends this paradigm. In Figure 3.8, a telephone and a Voice Server have been added to the web environment. The Voice Server manages several Voice Browser sessions. Each Voice Browser session includes one instance of the Voice Browser, the speech recognition engine, and the text-to-speech engine.

VoiceXML introduces a new way of presenting the web information. Instead of presenting the information visually (through HTML, graphics and text), the Voice Browser presents the information to the caller in audio using VoiceXML. When the caller says something (which is the voice equivalent of clicking on something to make a selection), the Voice Browser sends an HTTP request to the web server, which accesses the same back-end infrastructure, to return information this time in audio. This type of portal is known as voice portal. Voice portal is very useful in a hands-free situation like when you are driving.

The Voice Browser

An audio Voice Browser is similar to a visual web browser like Netscape Communicator or Microsoft Internet Explorer. Through voice browser, we interact with a web server using our voice and a telephone. Instead of rendering and interpreting a HTML document (like a GUI browser), the

Voice Browser renders and interprets VoiceXML documents. Instead of clicking a mouse and using keyboard, we use our voice and a telephone (and even the phone keypad) to access web information and services.

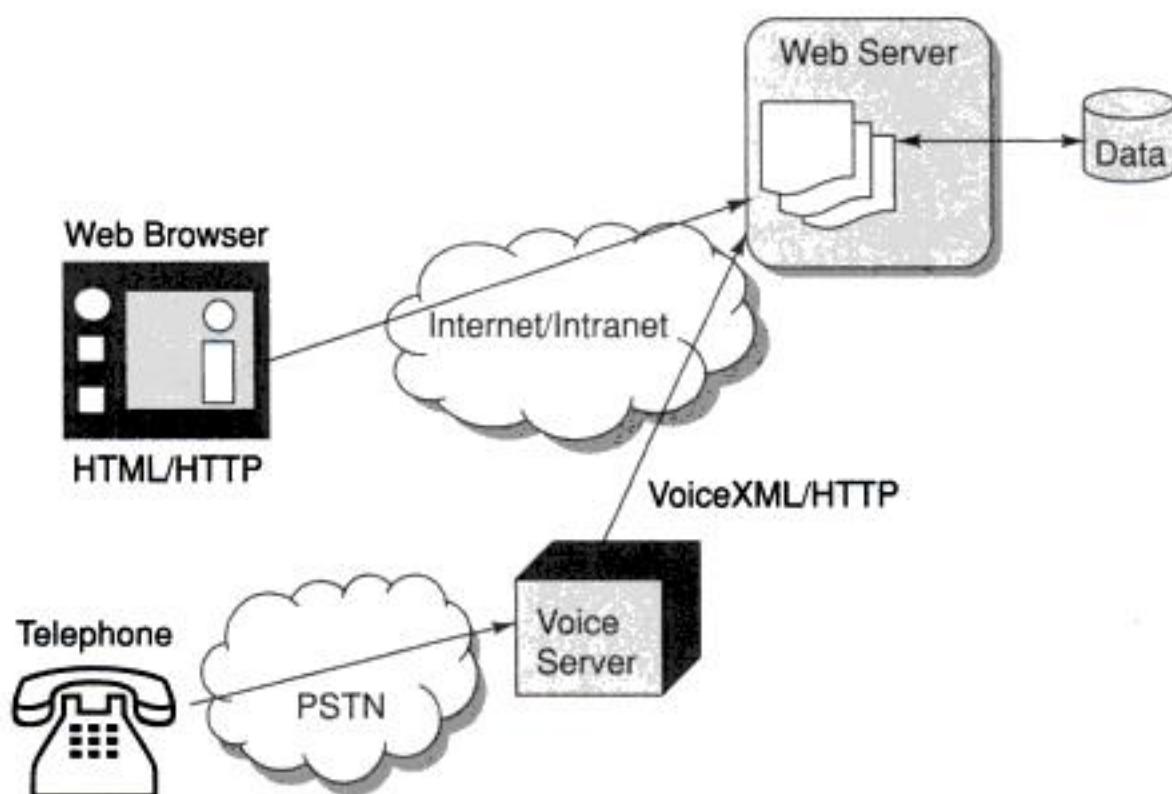


Figure 3.8 Voice Browser and Voice Portal over VoiceXML Architecture

Dialogs

A VoiceXML application defines a series of dialogs between a user and a computer. Each VoiceXML document forms a conversational finite state machine. The user is always in one conversational state, or dialog, at a time. Each dialog determines the next dialog to which to transition. Transitions are specified using URIs, which define the next document and dialog to use.

There are two types of dialogs that can be implemented in VoiceXML:

- forms
- menus

Forms define an interaction that collects values for a set of fields. Menus, on the other hand, present the user with choices or options and then transition to another dialog based on the choice.

Essential Elements of Voice XML Documents

The first line of any VoiceXML application must contain the `<?xml version="1.0"?>` element. The second line must contain the `<vxml version="1.0">` element. And each VoiceXML `<tag>`, must have an associated `</tag>`. The very last line of VoiceXML document must be the `</vxml>` tag. So, at a minimum, a VoiceXML document looks like this:

```

<?xml version="1.0"?>
<vxml version="1.0">
    .
    .

```



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Form

Form is one of the ways of developing a dialog with the caller in VoiceXML. Forms are central to VoiceXML. A VoiceXML form is a process to present information and gather input from the caller. A form is, basically, a collection of one or more fields that the caller fills in by saying something. A VoiceXML form is a very similar concept to a paper or online form, except that in the case of VoiceXML, we cannot see the field and instead of typing or writing in a field, we say something to fill it in.

In VoiceXML, we define a form using the `<form>` element and fields within the form using the `<field>` element. Here is a simple Voice Form.

```
<?xml version="1.0"?>
<vxml version="1.0">
<form id="add_funds">
  <field name="amount" type="currency">
    <prompt>How much?</prompt>
  </field>
  <field>
    <prompt>Charge to credit card or tuition
    bill?</prompt>
    <grammar> credit card | credit | tuition | tuition
    bill</grammar>
  </field>
</form>
</vxml>
```

This form has an ID of “add_funds”, and it contains two fields. The first field asks the user how much money to add to the meal account “How much” and is expecting the user to say an amount as currency (e.g., “one thousand rupees”). The second field asks for the type of transaction (“charge to credit card or tuition bill”) and is expecting the caller to say either “credit card”, “credit”, “tuition”, or “tuition bill”.

As we can see, fields define the information the application needs from the caller. Fields tell the caller what to say, and they also define the words and phrases that the caller can say (or the keys that can be pressed). Based on the caller’s input—in other words, what the caller says or which keys were pressed—the application takes an appropriate action. When the user provides a valid response, the field is considered FILLED and the application can then do something with this information.

Events

VoiceXML provides a form-filling mechanism for handling “normal” user input. In addition, VoiceXML defines a mechanism for handling events not covered by the form mechanism. Events are thrown by the platform under a variety of circumstances, such as when the user does not respond, doesn’t respond intelligibly, requests help, etc.

Links

A `link` supports mixed initiative. It specifies a grammar that is active whenever the user is in the scope of the link. If user input matches the link’s grammar, control transfers to the link’s destination URI. A `<link>` can be used to throw an event to go to a destination URI.

VoiceXML Elements

Element	Purpose Page
<assign>	Assign a variable a value.
<audio>	Play an audio clip within a prompt.
<block>	A container of (non-interactive) executable code.
<break>	JSML element to insert a pause in output.
<catch>	Catch an event.
<choice>	Define a menu item.
<clear>	Clear one or more form item variables.
<disconnect>	Disconnect a session.
<div>	JSML element to classify a region of text as a particular type.
<dtmf>	Specify a touch-tone key grammar.
<else>	Used in <if> elements.
<elseif>	Used in <if> elements.
<emp>	JSML element to change the emphasis of speech output.
<enumerate>	Shorthand for enumerating the choices in a menu.
<error>	Catch an error event.
<exit>	Exit a session.
<field>	Declares an input field in a form.
<filled>	An action executed when fields are filled.
<form>	A dialog for presenting information and collecting data.
<goto>	Go to another dialog in the same or different document.
<grammar>	Specify a speech recognition grammar.
<help>	Catch a help event.
<if>	Simple conditional logic.
<initial>	Declares initial logic upon entry into a (mixed-initiative) form.
<link>	Specify a transition common to all dialogs in the link's scope.
<menu>	A dialog for choosing amongst alternative destinations.
<meta>	Define a meta data item as a name/value pair.
<noinput>	Catch a no input event.
<nomatch>	Catch a no match event.
<object>	Interact with a custom extension.
<option>	Specify an option in a <field>.
<param>	Parameter in <object> or <subdialog>.
<prompt>	Queue TTS and audio output to the user.
<property>	Control implementation platform settings.
<pros>	JSML element to change the prosody of speech output.
<record>	Record an audio sample.

<reprompt>	Play a field prompt when a field is re-visited after an event.
<return>	Return from a subdialog.
<sayas>	JXML element to modify how a word or phrase is spoken.
<script>	Specify a block of ECMAScript client-side scripting logic.
<subdialog>	Invoke another dialog as a subdialog of the current.
<submit>	Submit values to a document server.
<throw>	Throw an event.
<transfer>	Transfer the caller to another destination.
<value>	Insert the value of a expression in a prompt.
<var>	Declare a variable.
<vxml>	Top-level element in each VoiceXML document.

3.7 TELEPHONY APPLICATION PROGRAMMING INTERFACE (TAPI)

In the previous sections we have discussed how to program a Dialogic card and develop voice-based applications and services. However, there are quite a few higher level frameworks available where a developer can develop voice-based services without going too deep into it. TAPI (Telephony Application Programming Interface) is one such example. There is another related standard for speech called Speech Application Programming Interface (SAPI). Developed jointly by Intel and Microsoft, TAPI and SAPI are two standards that can be used when developing voice telephony applications. Using TAPI, programmers can take advantage of different telephone systems, including ordinary PSTN, ISDN, and PBX (Private Branch Exchange) without having to understand all their details. Use of these API will save the programmer the pain of trying to program hardware directly. Through TAPI and SAPI a program can “talk” over telephones or video phones to people or phone-connected resources. Through TAPI one will be able to:

- Use simple user interface to set up calls. This can be calling someone by clicking on their picture or other images.
- Use simple graphical interface to set up a conference call and then attend the call at the scheduled time.
- See who the user is talking to.
- Attach voice greeting with an email. This will allow the receiver to listen to this greeting while opening the email.
- Set groups and security measures such that a service can receive phone calls from certain numbers (but not from others).
- Send and receive faxes.
- Use same set of TAPI APIs which are available in many smart phones. This facilitates accessing telephony interfaces from a mobile phone and a desktop computer.

In addition to the interface for applications, TAPI includes an interface for convergence of both traditional PSTN telephony and IP telephony. IP telephony or VoIP (Voice over IP) is an emerging set of technologies that enables voice, data, and video collaboration over Internet protocol. VoIP is discussed in detail in Chapter 17.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

CHAPTER 4

Emerging Technologies

4.1 INTRODUCTION

The mainstream wireless technologies have been discussed in Chapters 5 through 10. We will discuss wireless networks and application development using cellular networks like GSM, SMS, GPRS, WAP, CDMA, and 3G in Chapters 5 through 9. We will also discuss wireless local area networks (WLAN or WiFi) in Chapter 10. In this chapter, however, will we discuss some technologies which are not yet in the mainstream but are potential candidates for the same. These technologies are included here to make the mobile computing story complete. These include technologies like Bluetooth (802.15.1a), Radio frequency identifier (RFID), Wireless metropolitan area network or wireless broadband (WiMax-802.16), Mobile IP, IPv6, and Java Card. Bluetooth is a technology in the personal area network (PAN). RFID is emerging as a leading technology in the logistics, manufacturing, and retail industry. Wireless broadband is expected to be a mainstream technology very soon. Mobile IP allows data hand-off over different sub-networks. IPv6 is the next generation Internet protocol. Java Card technology is emerging as a forerunner in the security and personal identity domain. Therefore, we introduce all these technologies in this chapter.

4.2 BLUETOOTH

Bluetooth was the nickname of a Danish king Harald Blåtand, who unified Denmark and Norway in the 10th century. The concept behind Bluetooth wireless technology was unifying the telecom and computing industries. Bluetooth technology allows users to make ad hoc wireless connections between devices like mobile phones, desktop or notebook computers without any cable. Devices carrying Bluetooth-enabled chips can easily transfer data at a speed of about 1 Mbps in basic mode within a 50 m (150 feet) range or beyond through walls, clothing and even luggage bags.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

- **Adopted Protocols:** This has many protocol stacks like Point-to-Point Protocol (PPP), TCP/IP Protocol, OBEX (Object Exchange Protocol), Wireless Application Protocol (WAP), vCard, vCalendar, Infrared Mobile Communication (IrMC), etc.
 - **PPP Bluetooth:** This offers PPP over RFCOMM to accomplish point-to-point connections. Point-to-Point Protocol is the means of taking IP packets to/from the PPP layer and placing them onto the LAN.
 - **TCP/IP:** This protocol is used for communication across the Internet. TCP/IP stacks are used in numerous devices including printers, handheld computers, and mobile handsets. Access to these protocols is operating system independent, although traditionally realized using a socket programming interface model. TCP/IP/PPP is used for all Internet Bridge usage scenarios. UDP/IP/PPP is also available as transport for WAP.
 - **OBEX Protocol:** OBEX is a session protocol developed by the Infrared Data Association (IrDA) to exchange objects. OBEX, provides the functionality of HTTP in a much lighter fashion. The OBEX protocol defines a folderlisting object, which can be used to browse the contents of folders on remote devices.
 - **Content Formats:** vCard and vCalendar specifications define the format of an electronic business card and personal calendar entries developed by the Versit consortium. These are now maintained by the Internet Mail Consortium. Other content formats, supported by OBEX, are vMessage and vNote. These content formats are used to exchange messages and notes. They are defined in the IrMC (IrDA Mobile Communication) specification. IrMC also defines a format for synchronization of data between devices.

4.2.3 Bluetooth Security

In a wireless environment where every bit is on the air, security concerns are high. Bluetooth offers security infrastructure starting from authentication, key exchange, to encryption. In addition to encryption, a frequency-hopping scheme with 1600 hops/sec is employed. All of this make the system difficult to eavesdrop. At the lowest levels of the protocol stack, Bluetooth uses the publicly available cipher algorithm known as SAFER+ to authenticate a device's identity. In addition to these basic security functions, different application verticals use their own security infrastructure at the application layer.

4.2.4 Bluetooth Application Models

Each application model in Bluetooth is realized through a profile. Profiles define the protocols and protocol features supporting a particular usage model.

- **File Transfer:** The file transfer usage model offers the ability to transfer data objects from one device (e.g., PC, smart-phone, or PDA) to another. Object types include .xls, .ppt, .wav, .jpg, .doc files, folders or directories or streaming media formats. Also, this model offers a possibility to browse the contents of the folders on a remote device.
- **Internet Bridge:** In this usage model, a mobile phone or cordless modem acts as modem to the PC, providing dial-up networking and fax capabilities without need for physical connection to the PC.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

a convergence of voice, data and video. This convergence will demand interoperability and high data rate. Keeping this in mind, the IEEE 802 committee set up the 802.16 working group in 1999 to develop wireless broadband or WirelessMAN (wireless metropolitan area network) standards. WirelessMAN offers an alternative to high bandwidth wired access networks like fiber optic, cable modems and DSL (Digital Subscriber Line). WirelessMAN is popularly known as WiMAX (Worldwide Interoperability for Microwave Access). WiMAX provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile Internet access. This technology provides up to 10 Mbps bandwidth without the need for cables. Figure 4.4 illustrates the WiMAX Architecture; whereas, Fig. 4.5 illustrates a typical WirelessMAN deployment scenario.

The release of WirelessMAN (IEEE 802.16) standards in April 2002 has paved the way for the entry of broadband wireless access as a new bearer to link homes and businesses with core telecommunications networks. WirelessMAN provides network access to buildings through exterior antennas communicating with radio base stations. The technology is expected to provide less expensive access with more ubiquitous broadband access with integrated data, voice and video services. One of the most attractive aspects of wireless broadband technology is that networks can be created in just weeks by deploying a small number of base stations on buildings or poles to create high-capacity wireless access systems. In a wired set up, one physical wire will connect the device with the network. Also, we need to keep many wires reserved for future growth. Therefore, the initial investment in wired infrastructure is very high. Wireless network can grow as the demand increases. At any point in time the number of active users are always a fraction of the number of subscribers. In a wireless environment the number of channels is always low compared to the number of subscribers. This makes wireless technologies very attractive to the service providers.

IEEE 802.16 standardizes the air interface and related functions associated with WLL. Three working groups have been chartered to produce the following standards:

- IEEE 802.16.1—Air interface for 10 to 66 GHz.
- IEEE 802.16.2—Coexistence of broadband wireless access systems.
- IEEE 802.16.3—Air interface for licensed frequencies, 2 to 11 GHz.
- Extensive radio spectrum is available in frequency bands from 10 to 66 GHz worldwide. In a business scenario, 802.16 can serve as a backbone for 802.11 networks. Other possibilities are using 802.16 within the enterprise along with 802.11a, 802.11b or 802.11g.

IEEE 802.16 standards are concerned with the air interface between a subscriber's transceiver station and a base transceiver station. The 802.16 standards are organized into a three-layer architecture.

- The physical layer: This layer specifies the frequency band, the modulation scheme, error-correction techniques, synchronization between transmitter and receiver, data rate and the multiplexing structure.
- The MAC (Media Access Control) layer: This layer is responsible for transmitting data in frames and controlling access to the shared wireless medium through media access control (MAC) layer. The MAC protocol defines how and when a base station or subscriber station may initiate transmission on the channel.
- Above the MAC layer is a convergence layer that provides functions specific to the service being provided. For IEEE 802.16.1, bearer services include digital audio/video multicast, digital telephony, ATM, Internet access, wireless trunks in telephone networks and frame relay.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

while I am in office with my laptop computer, I use the company Ethernet LAN; and, when I am back home, I use the broadband at home. In this portable computing environment I use the network only when stationary and disconnect from one network before movement. Mobile computing on the other hand offers seamless computing and data networking facility even if the user is in a state of mobility and changes the network. Mobility Management (MM) deals with a situation where the user is at a vehicular state and accessing the network. Vehicular state generally means moving at a speed 60 kmph or higher. We will discuss the mobility management for voice network in Chapter 5. Here in Mobile IP, we will discuss the mobility management in TCP/IP data networks; Mobile IP standards are specified in RFC3344.

A data connection between two end-points through TCP/IP network requires a source IP address, source TCP port and a target IP address with a target TCP port. The combination of the IP address of the node (client or server device) system combined with the TCP port as the identification of a service becomes a point of attachment for an end-point. TCP port number is application-specific and remains constant. IP address, on the other hand, is network-specific and varies from network to network. IP addresses are assigned to a node from a set of addresses assigned to a network. This structure works well as long as the client is static and is using a desktop computer where the point of attachment is fixed. Let us assume that the user is mobile and is using a laptop with WiFi. As the user moves, the point of attachment will change from one subnet to another resulting in a change of IP address. This will force the connection to terminate. Therefore, the question is how do we allow mobility while a data connection is alive. The technology to do so is "Mobile IP". The term "mobile" in "Mobile IP" signifies that, while a user is connected to applications across the Internet and the user's point of attachment changes dynamically, all connections are maintained despite the change in underlying network properties including the point of attachments. This is similar to the handoff/roaming scenario in cellular networks. In a cellular network, when a user is mobile, the point of attachment (base station) changes. However, in spite of such changes the user is able to continue the conversation without any break in service.

4.5.1 How does Mobile IP Work?

IP routes packets from a source endpoint to a destination endpoint through various routers. An IP address of a node can be considered to be a combination of network address (most significant 24 bits) and the node address (least significant 8 bits). Let us assume a "C" class IP address 75.126.113.230 to be the mail server of Geschickten (mail.geschickten.com). We can assume that the first 24 bits 75.126.113 is the address of the network and the last 8 bits containing 230 is the address of the node. The network portion of an IP address is used by routers to deliver the packet to the last router in the chain to which the target computer is attached. This last router then uses the host portion (230 in this example) of the IP address to deliver the IP packet to the destination computer. In addition to the IP addresses of the nodes, for meaningful communication we need the TCP or UDP (User Datagram Protocol) port of the applications. The port number is used by the host to deliver the packet to the appropriate application.

A TCP connection is identified by a quadruplet that contains the IP address and port number of the sender endpoint along with the IP address and port number of the receiving endpoint. To ensure that an active TCP connection is not terminated while the user is mobile, it is essential that all of these four identities remain constant—physically or virtually. The TCP ports are application specific and generally constant—they do not change after an end-to-end connection is established.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

We have assumed that the foreign agent will allocate the care-of address. However, it is possible that a mobile node moves to a network that has no foreign agents or on which all foreign agents are busy. It is also possible that the care-of address is dynamically acquired as a temporary address by the mobile node such as through DHCP (Dynamic Host Configuration Protocol) as explained in RFC2131, or may be owned by the mobile node as a long-term address for its use only while visiting some foreign network. As an alternative therefore, the mobile node may act as its own foreign agent by using a co-located care-of address. A co-located care-of address is an IP address obtained by the mobile node that is associated with the foreign network. If the mobile node is using a co-located care-of address, then the registration happens directly with its home agent.

4.5.4 Tunneling

Figure 4.7 shows the tunneling operations in Mobile IP. In the mobile IP, an IP-within-IP encapsulation mechanism is used. Using IP-within-IP, the home agent, adds a new IP header called tunnel header. The new tunnel header uses the mobile node's care-of address as the tunnel destination IP address. The tunnel source IP address is the home agent's IP address. The tunnel header uses 4 as the protocol number (Fig. 4.8), indicating that the next protocol header is again an

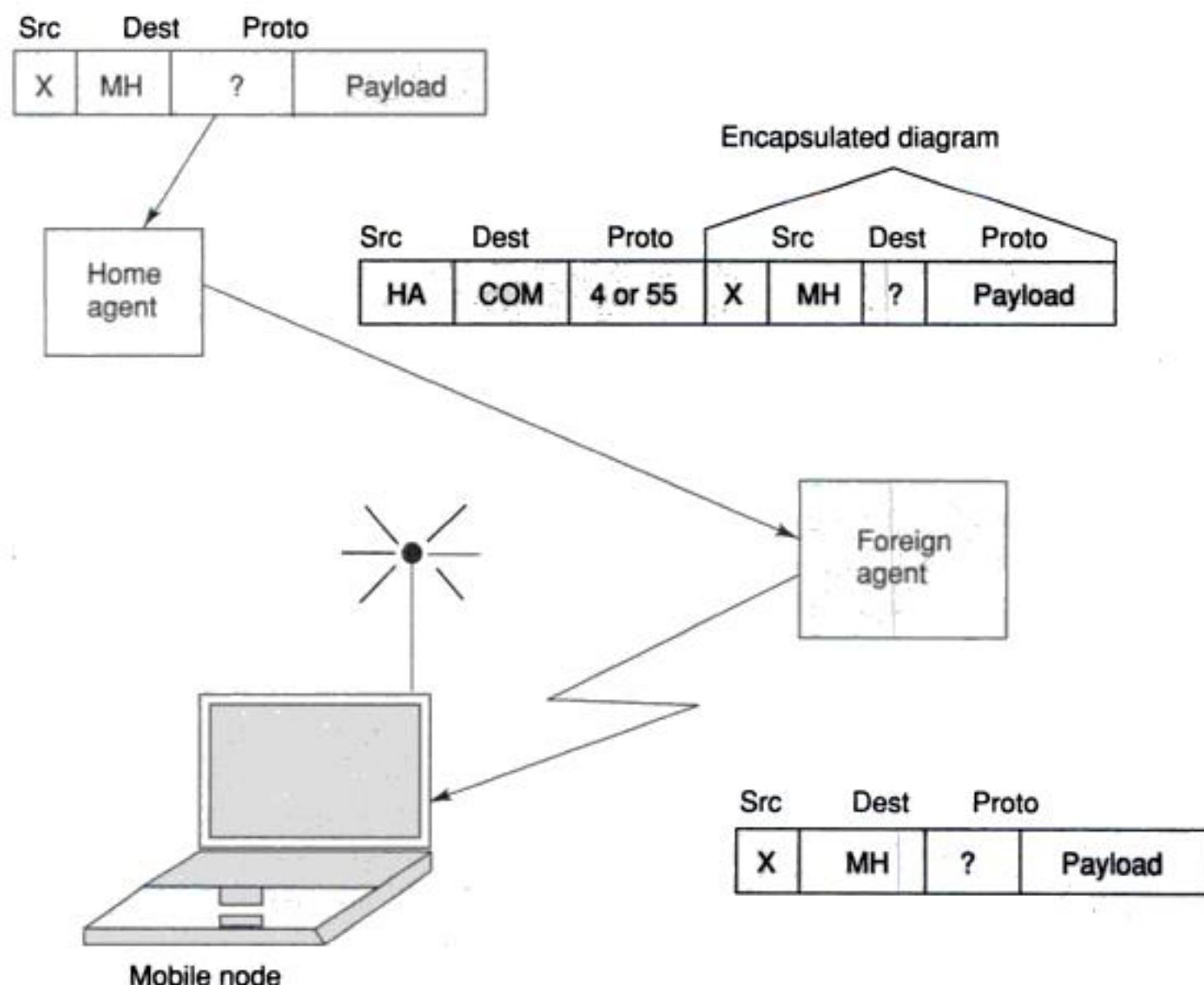


Figure 4.7 Tunneling Operations in Mobile IP



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

and digital cellular phones. The explosion in the number of devices connected to the Internet, combined with projections for the future, made scientists think seriously whether the 32-bit address space of TCP/IP is sufficient. IP version 6 (IPv6), the successor to today's IP version 4 protocol (IPv4), dramatically expands the available address space. Internet Engineering Task Force (IETF) has produced a comprehensive set of specifications (RFC 1287, 1752, 1886, 1971, 1993, 2292, 2373, 2460, 2473, etc.) that define the next-generation IP protocol originally known as "IPNg," now renamed as "IPv6". IPv6 addresses both a short-term and long-term concern for network owners, service providers and users.

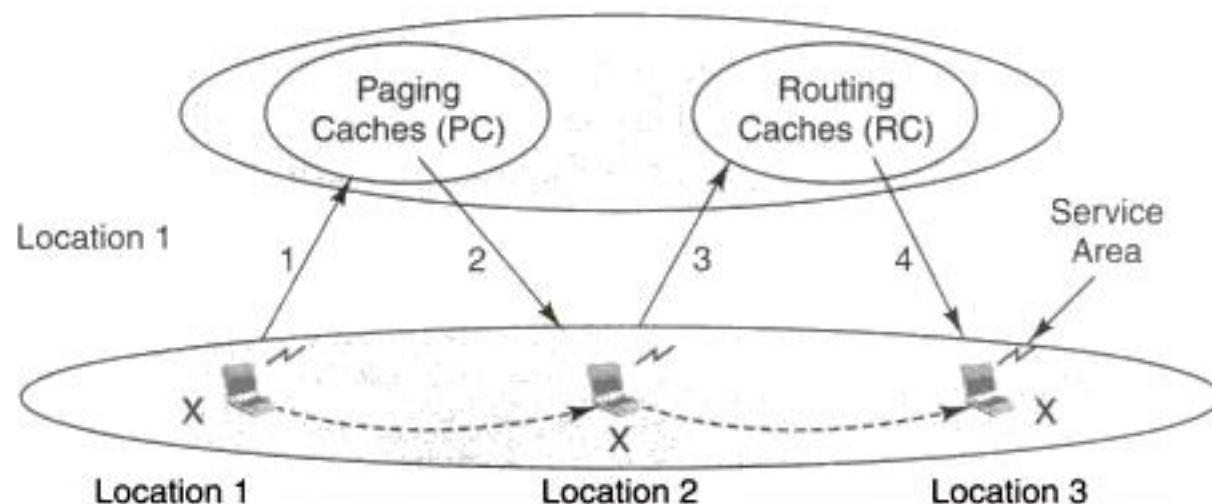


Figure 4.10 Cellular IP Paging and Routing

4.6.1 Address Space

IPv6 uses 128 bit addresses for each packet, creating a virtually infinite number of IP addresses (approximately 3.4×10^{38} IP addresses), as opposed to 3758096384 IPv4 addresses (2^{31} A Class address + 2^{30} B Class + 2^{29} C Class address). This also means that if we set the world population at 10 billion in 2050, there will be 3.4×10^{27} addresses available per person.

In IPv6, there are global addresses and local addresses. Global addresses are used for routing of global Internet. Link local addresses are available within a subnet. IPv6 uses hierarchical addressing with three-level of addresses (Fig. 4.11). This includes a Public Topology (the 48 bit external routing prefix), a Site Topology (typically a 16 bit subnet number), and an Interface Identifier (typically an automatically generated 64 bit number unique on the local LAN segment).

End-user-sites get their address prefix from an ISP that provides them the IPv6 service. General IPv6 host is given a linklocal address such as fe80::EUI-64 and more than one global address such as global-prefix::EUI-64. It has 64 bit length and made by IEEE EUI-64 format. Interface ID is used to specific Interface in the same link. Interface ID is generated to use Interface's link layer address. An Ethernet MAC address for a device is 48 bits long, Interface ID is created by adding 2 octet "0xffff" in it's center. Like 02:60:8c:de:7:79 becomes 260:8cff:fede:779.

4.6.2 IPv6 Security

One of the biggest differences between IPv6 and IPv4 is that all IPv6 nodes are expected to implement strong authentication and encryption features to improve Internet security. IPv6 comes



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

TSi	Traffic Selector-Initiator
TSr	Traffic Selector-Responder
V	Vendor ID

Figure 4.13 IPsec IKEv2 Procedure

In the protocol above, HDR contains the Security Parameter Indexes (SPIs), version numbers, and flags of various sorts. The SAi1 payload states the cryptographic algorithms the initiator supports. The KE payload sends the initiator's Diffie-Hellman value. Ni is the initiator's nonce. Payloads such as [CERTREQ] that may optionally appear are shown in brackets, indicate that optionally a certificate request payload can be included. At this point in the negotiation, each party can generate SKEYSEED, from which all keys are derived for that IKE_SA. Everything except the headers of all the messages that follow are encrypted and integrity protected.

4.6.3 Packet Payload

Each IPv6 packet payload is attached a tag which can be customized to enable a better quality in the packet flow, or by a price of other class, such as non-real-time quality of service or "real-time" service. This feature does not exist natively in IPv4, although a part of payload could be used for the same, reducing unique information amount carried by the packet.

Information is packetized into IPv6 packets, with the corresponding levels of control. A neighbor discovery feature (care-of address, and stateless Prefix or Stateful DHCPv6) will in principle allow the device carrying these packets to configure itself for a consistent dialogue with other devices or software interfaces. The same can be done with IPv4 packets, but with the intervention of humans or specific tools and services and only for selected information and software architectures.

4.6.4 Migrating from IPv4 to IPv6

The migration from IPv4 to IPv6 is quite an involved task. This includes the following:

1. Migration of the network components to be able to support IPv6 packets. As there is no change at the physical layer between IPv4 and IPv6, network components like hub or switch need not change. As there is a change in the packet header the routers need to be upgraded. However, using IP tunneling IPv6 packets can propagate over an IPv4 envelope. Existing routers can support IP tunneling.
2. Migration of the computing nodes in the network: this will need the operating system upgrades so that they support IPv6 along with IPv4. Upgraded systems will have both IPv4 and IPv6 stacks. Therefore, both the IPv4 and IPv6 applications can run without any difficulty.
3. Migration of networking applications in both client and server systems: this requires porting of the applications from IPv4 to IPv6 environment.

Migration of Windows System

The Microsoft Windows 9x families do not support IPv6. Windows XP and Windows Server 2003 support IPv6 natively. Windows 2000 Professional can be upgraded to support IPv6. IPv6 in Windows support different tools and dlls. These are:

wship6.dll: The Winsock helper dynamically linked library for the INET6 address family.

wininet.dll: Winsock INET6 libraries.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

4.7 JAVA CARD

Java Card is a smart card with Java framework. Smart card was developed in 1974, by Roland Moreno. Smart card is a plastic card with intelligence and memory. Smart cards are becoming popular as identity module and wireless security devices. In many countries driving licenses are being issued on smart cards. The SIM card on a GSM mobile phone is a smart card as well. The importance of smart card made ISO standardize all its interfaces. These are done through ISO 7816 standards. These ISO standards define the physical characteristic of the card (ISO 7816-1:: Physical Characteristics), locations and dimensions of the contacts (7816-2:: Dimensions and Locations of the Contacts), signals and transmission interfaces (7816-3:: Electronic Signals and Transmission Protocols), and command interfaces (7816-4:: Interindustry Commands for Interchange). A smart card is embedded with either (i) a microprocessor and a memory chip or (ii) only a memory chip with non-programmable logic. A microprocessor card can have an intelligent program resident within the card which can add, delete, and otherwise manipulate information on the card. A memory card on contrast, can store some information for some pre-defined operation. Smart cards are capable of carrying data, functions, and information on the card. Therefore, unlike memory strip cards, they do not require access to remote databases at the time of the transaction.

Microprocessor based smart cards which were used for some specific application areas are becoming quite common. Smart cards have now emerged as multi-function cards. To allow interoperability, Java was chosen. All the microprocessor based smart cards now offer Java API framework on them. This is why smart cards with Java framework are also called Java Cards. 3GPP has decided to use Java Card as the standard for USIM and ICC (Integrated Circuit cards). Java Card technology preserves many of the benefits of the Java programming languages such as: productivity, security, robustness, tools, and portability. For Java card, the Java Virtual Machine (JVM), the language definition, and the core packages have been made more compact to bring Java technology to the resource constrained smart cards.

A smart card of a GSM SIM card supporting Java Card functionalities may typically have an 8 or 16 bit microprocessor running at speeds between 5 MHz to 40 MHz with 32K to 128K bytes of EEPROM (Electronically Erasable Programmable Read Only Memory). Though Java card works in a master/slave mode, using the proactive SIM technology of GSM Phase 2+, it is possible for the application on the SIM card to get activated in an automated fashion. Also, Java card technology supports OTA (Over the Air) downloads. In OTA download, a Java applet (through SMS) can be downloaded by the network operator proactively or by the user interactively over the wireless media. Applications written for the Java Card platform are referred to as applets.

The development framework in Java card is different from that on a desktop computer. The major challenge of Java Card technology on smart card is to fit Java system software in a resource constraint smart card while conserving enough space for applications. Java Card supports a subset of the features of Java language available on desktop computers. The Java Card virtual machine on a smart card is split into two parts (Fig. 4.15): one that runs off-card and the other that runs on-card. Many processing tasks that are not constrained to execute at runtime, such as class loading, bytecode verification, resolution and linking, and optimization, are dedicated to the virtual machine that is running off-card where resources are usually not a concern. The on-card components of Java Card include components like the Java Card virtual machine (JCVM), the Java Card Runtime Environment (JCRE), and the Java API. Task of the compiler is to convert a Java source into Java

class files. The converter will convert class files into a format downloadable into the smart card. Converter ensures the byte code validity before the application is installed into the card. The converter checks the classes off-card for,

- How well it is formed?
- Java Card subset violations.
- Static variable initialization.
- Reference resolution.
- Byte code optimization.
- Storage allocation.
- The Java Card interpreter.
- Applet execution.
- Controls run time resources.
- Enforces runtime security.

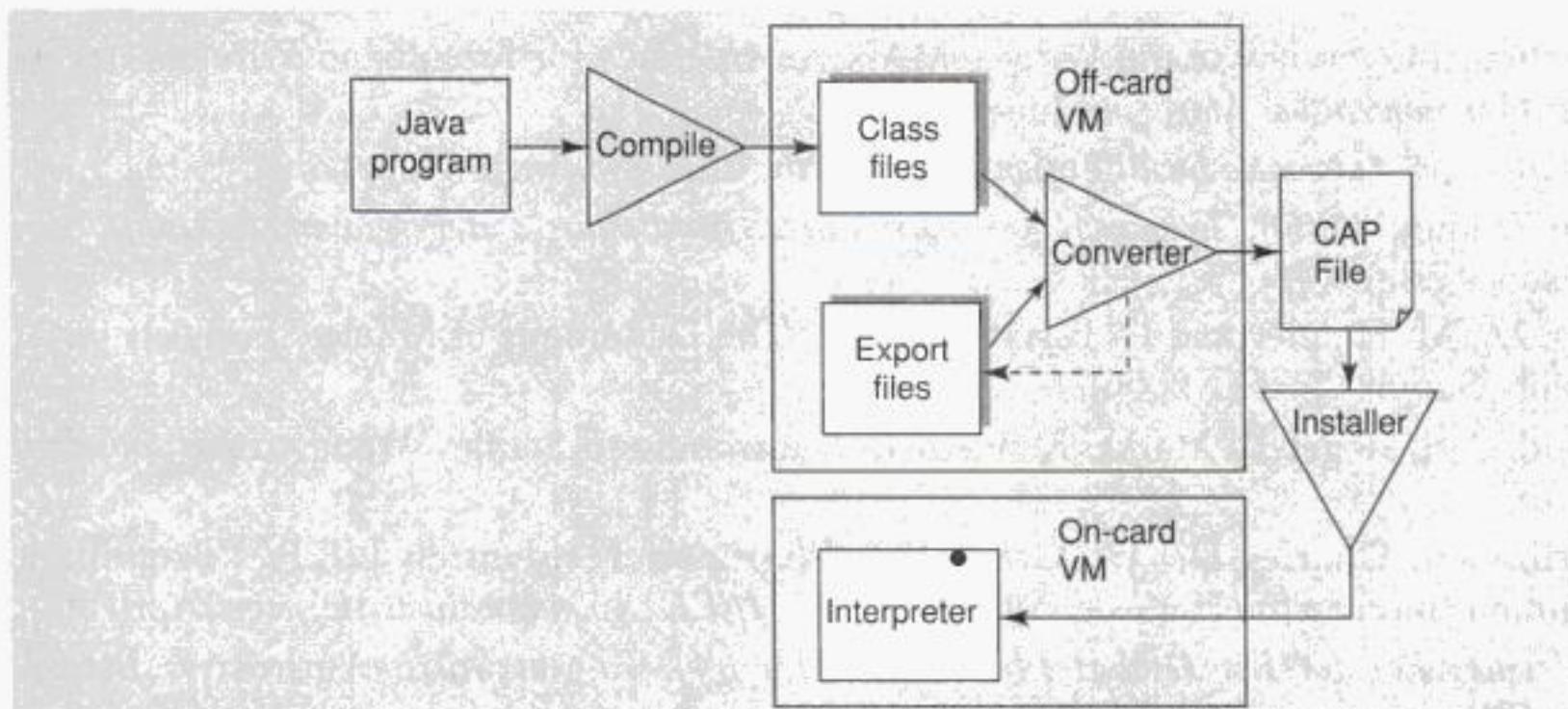


Figure 4.15 Architecture of Java Card Applications Development Process

Following conversion by the off-card VM into CAP (Converted APlet) format, the applet is transferred into the card using the installer. The applet is selected for execution by the JCRC. JCRC is made up of the on-card virtual machine and the Java Card API classes. JCRC performs additional runtime security checks through the applet firewall. Applet firewall partitions the objects stored into separate protected object spaces, called contexts. Applet firewall controls the access to shareable interfaces of these objects. The JCVM is a scaled down version of standard JVM (Java Virtual Machine). Elements of standard Java not supported in JCVM are,

- Security manager.
- Dynamic class loading.
- Bytecode verifier.
- Threads.
- Garbage collection.
- Multi-dimensional arrays.

- Char and strings.
- Floating point operation.
- Object serialization.
- Object cloning.

As mentioned above, Java applications for Java Cards are called Applets. Java Card applets should not be confused with Java applets on the Internet. A Java Card applet is not intended to run within an Internet browser environment. The reason for choosing the name applet is that Java Card applets can be loaded into the Java Card runtime environment after the card has been manufactured. That is, unlike applications in many embedded systems, Java Card applets do not need to be burned into the ROM during manufacture.

REFERENCES/FURTHER READING

1. A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access, *IEEE Communications Magazine*, June 2002.
2. Association for Automatic Identification and Mobility: <http://www.aimglobal.org>.
3. Chen Zhiqun, (2000), *Technology for Smart Cards: Architecture and Programmer's Guide*, Sun, Addison-Wesley.
4. Cong, D., M. Hamler and C. Perkins, (2006), 'The Definitions of Managed objects for IP Mobility Support', *RFC*: 2006.
5. Eklund Carl, Roger B. Marks, Kenneth L. Stanwood and Stanley Wang, *IEEE Standard*, 802.16:
6. Gavrilovich, Charles D. Jr., Gray Cary Ware and Freidenrich L.L.P., "Broadband Communication on the Highways of Tomorrow", *IEEE Communications Magazine*, April 2001.
7. Guidelines For 64-Bit Global Identifier (EUI-64). Registration Authority: <http://standards.ieee.org/regauth/oui/tutorials/EUI64.html>.
8. Held Gil, (2001), *Data Over Wireless Networks Bluetooth, WAP, & Wireless LANs*, McGraw-Hill.
9. IEEE 802.16 for Broadband: <http://www.nwfusion.com/news/tech/2001/0903-tech.html>.
10. Java card Forum: <http://www.javacardforum.org/>.
11. Karagiannis Georgios, 'Mobile IP', *Ericsson Open Report # 3/0362-FCP NB 102 88 Uen*, 13 July, 1999.
12. Karagiannis Georgios, (1999), 'Mobile IP,' *Ericsson State of the Art Report # 3/0362-FCP NB 102 88 Uen*.
13. Muller Nathan J., (2001), *Bluetooth Demystified*, Tata McGraw-Hill.
14. Official Bluetooth site: <http://www.bluetooth.com>.
15. Perkins, C., 'Mobile IP,' *IEEE Communications Magazine*, May 1997.
16. Perkins, C., 'Mobile Networking through Mobile IP,' *IEEE Internet Computing*, January-February 1998, p 58.
17. Perkins, C., (1998), *Mobile IP: Design Principles and Practices*, Prentice-Hall PTR.

18. Prabhu, C.S.R. and A. Prathap Reddi, (2004), *Bluetooth Technology and Its Applications with Java and J2ME*, Prentice-Hall of India.
19. RFC 2002: IP Mobility Support—<http://www.faqs.org/rfcs/rfc2002.html>.
20. RFC 2005, Applicability Statement for IP Mobility Support.
21. Stallings William, IEEE 802.16 for broadband wireless, Network World, 09/03/01, RFC1825: Security.
22. Andras G. Valko, “Cellular IP: A New Approach to Internet Host Mobility,” *ACM SIGCOMM Computer Communication Review*, pp 50–65.

REVIEW QUESTIONS

- Q1: Describe the protocol stack of Bluetooth.
- Q2: How does a new Bluetooth device discover a Bluetooth network? Describe the security principles in Bluetooth.
- Q3: What is active RFID? Describe two applications of active RFID. How is active RFID different from passive RFID? Describe two applications of passive RFID.
- Q4: What is WiMax (Wireless broadband)? How is it different from WiFi? Explain the WiMax physical layer.
- Q5: What is Mobile IP? Explain tunneling in the context of Mobile IP.
- Q6: How does Mobile IP work? What are the challenges with mobile IP with respect to high speed mobility? How does Cellular IP solve some of these challenges?
- Q7: What is Cellular IP?
- Q8: In what ways is IPv6 better than IPv4? Briefly enunciate the migration issues from IPv4 to IPv6 in the context of different operating systems.
- Q9: You have a communication application that uses sockets in IPv4, what are the steps you need to follow to port this application from IPv4 to IPv6?
- Q10: Write short notes on:
 - (a) Java Card
 - (b) Security Association in IPv6
 - (c) IPsec
- Q11: You need to develop a secured healthcare application. What information will you keep in the Java card and what will be in the backend server? How will you secure such information on the Java Card?



CHAPTER 5

Global System for Mobile Communications (GSM)

5.1 GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

GSM is much more than just an acronym for Global System for Mobile Communication. It signifies an extremely successful technology and bearer for mobile communication system. GSM today covers 71% of all the digital wireless market. The mobile telephone has graduated from being a status symbol to a useful appliance. People use it not only in business but also in personal life. Its principal use is for wireless telephony, and messaging through SMS. It also supports facsimile and data communication.

GSM is based on a set of standards, formulated in the early 1980s (see Table 5.1 for the GSM timeline). In 1982, the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Groupe Spécial Mobile (GSM) to study and develop a pan-European mobile system, which was later rechristened as Global System for Mobile Communication. See Chapter 1 for cellular network evolution and standards. The proposed GSM system had to meet certain business objectives. These are:

- Support for international roaming.
- Good speech quality.
- Ability to support handheld terminals.
- Low terminal and service cost.
- Spectral efficiency.
- Support for a range of new services and facilities.
- ISDN compatibility.

Due to its innovative technologies and strengths, GSM rapidly became truly global. Many of the new standardization initiatives came from outside Europe. Depending on locally available frequency bands, different air interfaces were defined. Of these prominent ones are 900 MHz, 1800 MHz and 1900 MHz. However, architecture, protocols, signaling and roaming are identical in all networks independent of the operating frequency bands.

Table 5.1 GSM history timeline

<i>Year</i>	<i>Event</i>
1982	Groupe Spécial Mobile (GSM) established
1987	Essential elements of wireless transmission specified
1989	GSM becomes an ETSI technical committee
1990	Phase 1 GSM 900 specification (designed 1987 through 1990) frozen
1991	First GSM network launched
1993	First roaming agreement came into effect
1994	Data transmission capability launched
1995	Phase 2 launched. Fax and SMS roaming services offered
2002	SMS volume crosses 24 billion/year, 750 million subscribers

GSM uses a combination of FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access). See Section 3.2 for definition of these multiple access procedures. The GSM system has an allocation of 50 MHz (890–915 MHz and 935–960 MHz) bandwidth in the 900 MHz frequency band. Using FDMA, this band is divided into 124 (125 channels, 1 not used) channels each with a carrier bandwidth of 200 KHz. Using TDMA, each of these channels is then further divided into eight time slots. Therefore, with the combination of FDMA and TDMA we can realize a maximum of 992 channels for transmitting and receiving. In order to be able to serve hundreds of thousands of users, the frequency must be reused. This is done through cells.

The frequency reuse concept led to the development of cellular technology as originally conceived by AT&T and Bell Labs way back in 1947. The essential characteristics of this reuse are as follows:

- The area to be covered is subdivided into radio zones or cells (Fig. 5.1). Though in reality these cells could be of any shape, for convenient modeling purposes these are modeled as hexagons. Base stations are positioned at the center of these cells.
- Each cell i receives a subset of frequencies fbi from the total set assigned to the respective mobile network. To avoid any type of co-channel interference, two neighboring cells never use the same frequencies.
- Only at a distance of D (known as frequency reuse distance), the same frequency from the set fbi can be reused. Cells with distance D from cell i , can be assigned one or all the frequencies from the set fbi belonging to cell i .
- When moving from one cell to another during an ongoing conversation, an automatic channel change occurs. This phenomenon is called handover. Handover maintains an active speech and data connection over cell boundaries.

The regular repetition of frequencies in cells result in a clustering of cells. The clusters generated in this way can consume the whole frequency band. The size of a cluster is defined by k , the number of cells in the cluster. This also defines the frequency reuse distance D . Figure 5.1 shows an example of a cluster size of 4.

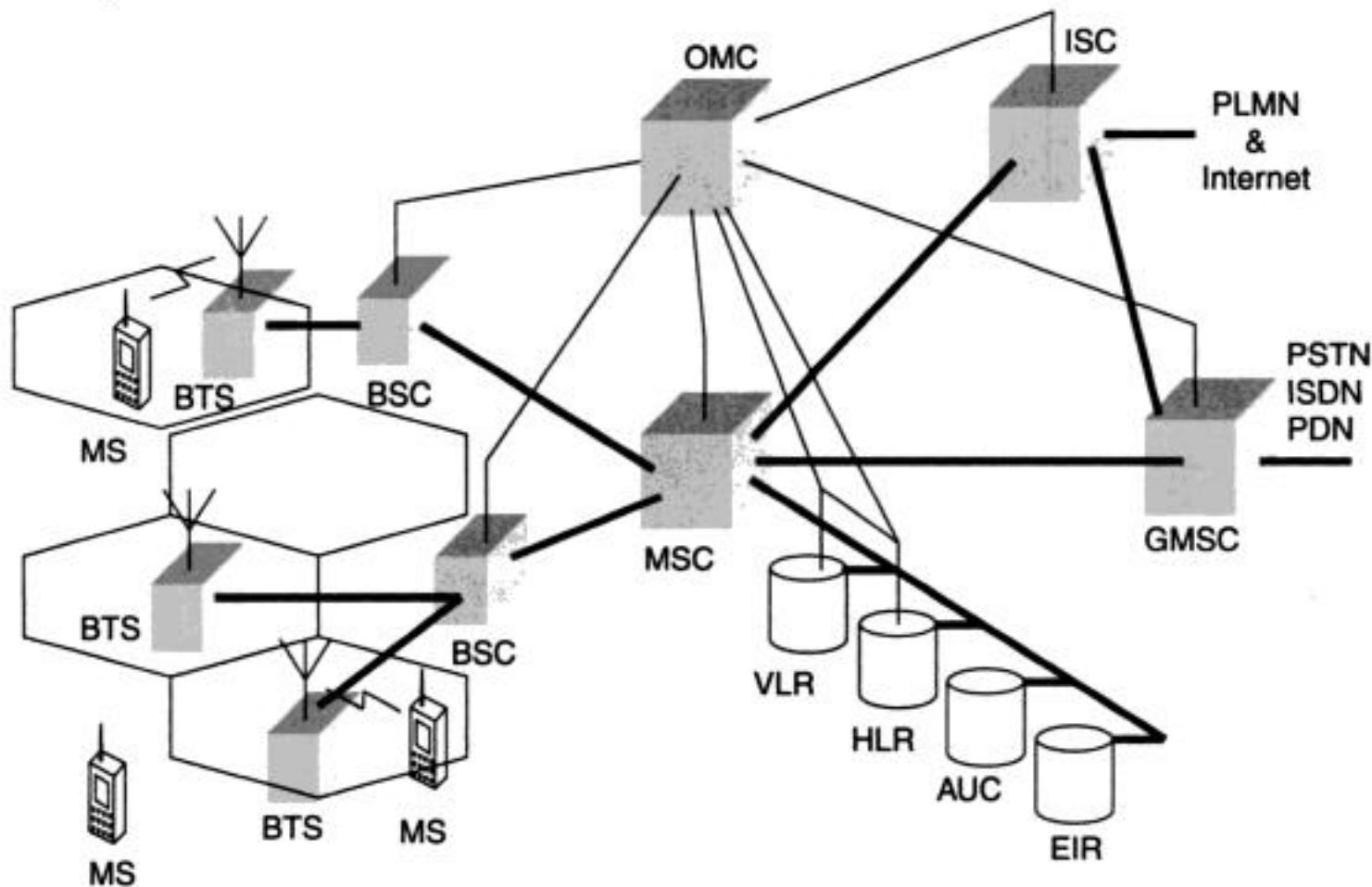


You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

- The Mobile Station (MS). This includes the Mobile Equipment (ME) and the Subscriber Identity Module (SIM).



AUC	Authentication Center	ISDN	Integrated System Digital Network
BSC	Base Station Controller	MS	Mobile Station
BTS	Base Transceiver Station	MSC	Mobile Switching Center
EIR	Equipment Identity Register	OMC	Operation and Maintenance Center
GMSC	Gateway MSC	PDN	Packet Data Network
HLR	Home Location Register	PLMN	Public Land Mobile Network
ISC	International Switching Center	PSTN	Public Switched Telephone Network
		VLR	Visitor Location Register

Figure 5.3 Architecture of GSM

- The Base Station Subsystem (BSS). This includes the Base Transceiver Station (BTS) and the Base Station Controller (BSC).
- The Network and Switching Subsystem (NSS). This includes Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), and the Authentication Center (AUC).
- The Operation and Support Subsystem (OSS). This includes the Operation and Maintenance Center (OMC).
- The data infrastructure that includes Public Switched Telephone Network (PSTN), Integrated System Digital Network (ISDN), and the Public Data Network (PDN).

5.3.1 Mobile Station

Mobile Station is the technical name of the mobile or the cellular phone. In early days mobile phones were a little bulky and were sometimes installed in cars like other equipment. Even the



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

5.3.4 The Operation and Support Subsystem (OSS)

As the name suggests, Operations and Support Subsystem (OSS) controls and monitors the GSM system. The OSS is connected to different components of the NSS and to the BSC. It is also in charge of controlling the traffic load of the BSS. However, the increasing number of base stations, due to the development of cellular radio networks, has resulted in some of the maintenance tasks being transferred to the BTS. This transfer decreases considerably the costs of maintenance of the system. Provisioning information for different services is managed in this subsystem.

Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment within the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). EIR contains a list of IMEIs of all valid terminals. An IMEI is marked as invalid if it has been reported stolen or is not type approved. The EIR allows the MSC to forbid calls from this stolen or unauthorized terminals.

Authentication Center (AUC) is responsible for the authentication of a subscriber. This is a protected database and stores a copy of the secret key stored in each subscriber's SIM card. These data help to verify the user's identity.

5.3.5 Message Centre

Short Message Service or SMS is one of the most popular services within GSM. SMS is a data service and allows a user to enter text message up to 160 characters in length when 7-bit English characters are used. It is 140 octets when 8-bit characters (some European alphabets or binary data) are used, and 70 characters in length when non-Latin alphabets such as Arabic, Chinese or Hindi are used (70 characters of 16-bit Unicode). SMS is a proactive bearer and is an always ON network. Message center is also referred to as Service Centre (SC) or SMS Controller (SMSC). SMSC is a system within the core GSM network, which works as a store and forward system for SMS messages. Refer to Figure 5.5 for SMS architecture.

There are two types of SMS, SMMT (Short Message Mobile Terminated Point-to-Point), and SMMO (Short Message Mobile Originated Point-to-Point). SMMT is an incoming short message from the network and is terminated in the MS (phone or Mobile Station). SMMO is an outgoing message, originated in the MS, and forwarded to the network for delivery. For an outgoing message, the SMS is sent from the phone to SC via the VLR and the Interworking MSC (IWMSC). For incoming SMS message the path is from SC to the MS via the HLR and the Gateway MSC (GMSC). Please see Chapter 6 for SMS and related technologies.

5.4 CALL ROUTING IN GSM

Human interface is analog. However, the advancement in digital technology makes it very convenient to handle information in digital fashion. In GSM there are many complex technologies used between the human analog interface in the mobile and the digital network (Fig. 5.6).

Digitizer and source coding: The user speech is digitized at 8 KHz sampling rate using Regular Pulse Excited–Linear Predictive Coder (RPE–LPC) with a Long Term Predictor loop. In this technique, information from previous samples is used to predict the current sample. Each sample



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



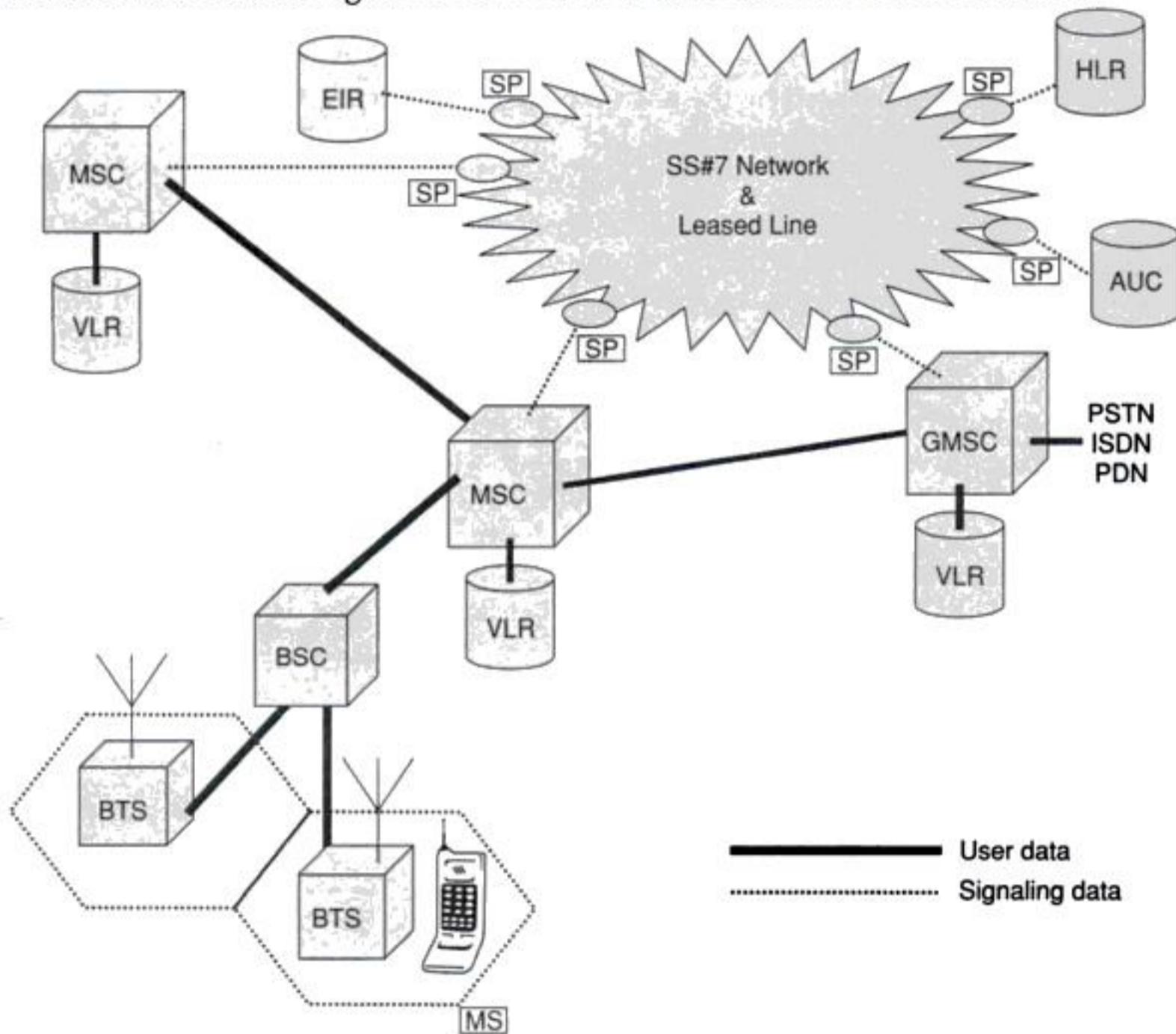
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

5.5 PLMN INTERFACES

The basic configuration of a GSM network contains a central HLR and a central VLR. HLR contains all security, provisioning and subscriber-related information. VLR stores the location information and other transient data. MSC needs subscriber parameter for successful call set-up. Figure 5.8 shows a basic configuration of a GSM mobile communication network.



AUC	Authentication Center
BSC	Base Station Controller
BTS	Base Transceiver Station
EIR	Equipment Identity Register
GMSC	Gateway MSC
HLR	Home Location Register

ISDN	Integrated System Digital Network
MS	Mobile Station
MSC	Mobile Switching Center
PDN	Public Data Network
PSTN	Public Switched Telephone Network
SP	Signaling Point
VLR	Visitor Location Register

Figure 5.8 Configuration of a GSM PLMN

Within the switching and management system, the transmission rate is 2 Mbits/s. This 2 Mbits/ interface is called E1 interface in India and in Europe. These are realized typically through



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Management (MM) solves all these challenges. Using MM one can make outgoing calls and receive incoming calls while in motion; even at the vehicular state where the speed is higher than 60 kmph. The MM function handles all functions that arise from the mobility of the subscriber.

In a wired network where the device is stationary, the point of attachment to the network is fixed; here, address of the device is sufficient to locate the device in the routing table and establish a connection. However, in a wireless or mobile environment the point of attachment constantly changes, the device moves from one location to another location making the old routing table invalid; therefore, establishing and maintaining a connection is complex. As long as there is a wireless network with available channels, mobile originated outgoing calls are relatively easy to handle; for mobile terminated incoming calls, however, Paging and Location Updates are necessary. Also, Handover and Roaming are two important aspects in mobility. We will discuss mobility management in the following sections.

5.8.1 Paging

For a mobile terminated call, the MS needs to be traced, located, and then the call connected. The MS is traced through the Paging process within a location. Using the BSS signaling channel the Paging message for an MS is sent that includes the IMSI as the identifier of the MS. The message may also include an indication of which combination of channels will be needed for the subsequent transaction related to the paging. A single paging message across the MSC to BSS interface contains information of the cells in which the page shall be broadcast.

In Paging, the most difficult part of the decision is—which cell to start the paging from; because a cellular network may be spread over thousands of square-kilometres with thousands of cells. If we cannot locate the mobile quickly, the call cannot be connected resulting in lost revenue. For example, it can start at the center of the network and keep on searching each and every cell for a long time. However, such global paging is very expensive in terms of backbone and radio signaling channels. Also, global paging will take enormous amount of time. To optimize the cost and response time, paging starts at the location where the MS was present last. The location of the MS is recorded in the HLR and updated through Location Update. The MS is searched in these cells where it has the highest probability of being present. There are various algorithms for paging so that the MS can be located quickly with minimum effort and cost.

5.8.2 Location Update

Location update is concerned with the procedures that enable the network to know the current location of a powered-on MS so that the mobile terminated call routing can be completed. If the location of the MS is not known, tracking the MS through paging costs in terms of radio and backbone SS7 signalling (see Chapter 11) bandwidth. To optimize this, location information is regularly updated within the core network. Through location update, the presence and location information is kept up-to-date within the VLR and the HLR. Presence deals with willingness and availability of an MS for communication. Assuming that the MS is willing to communicate, the MS must be powered-on and attached to the network. If the MS is attached to the network, it must be located through Paging before a successful communication can take place for mobile terminated calls and mobile terminated SMS.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



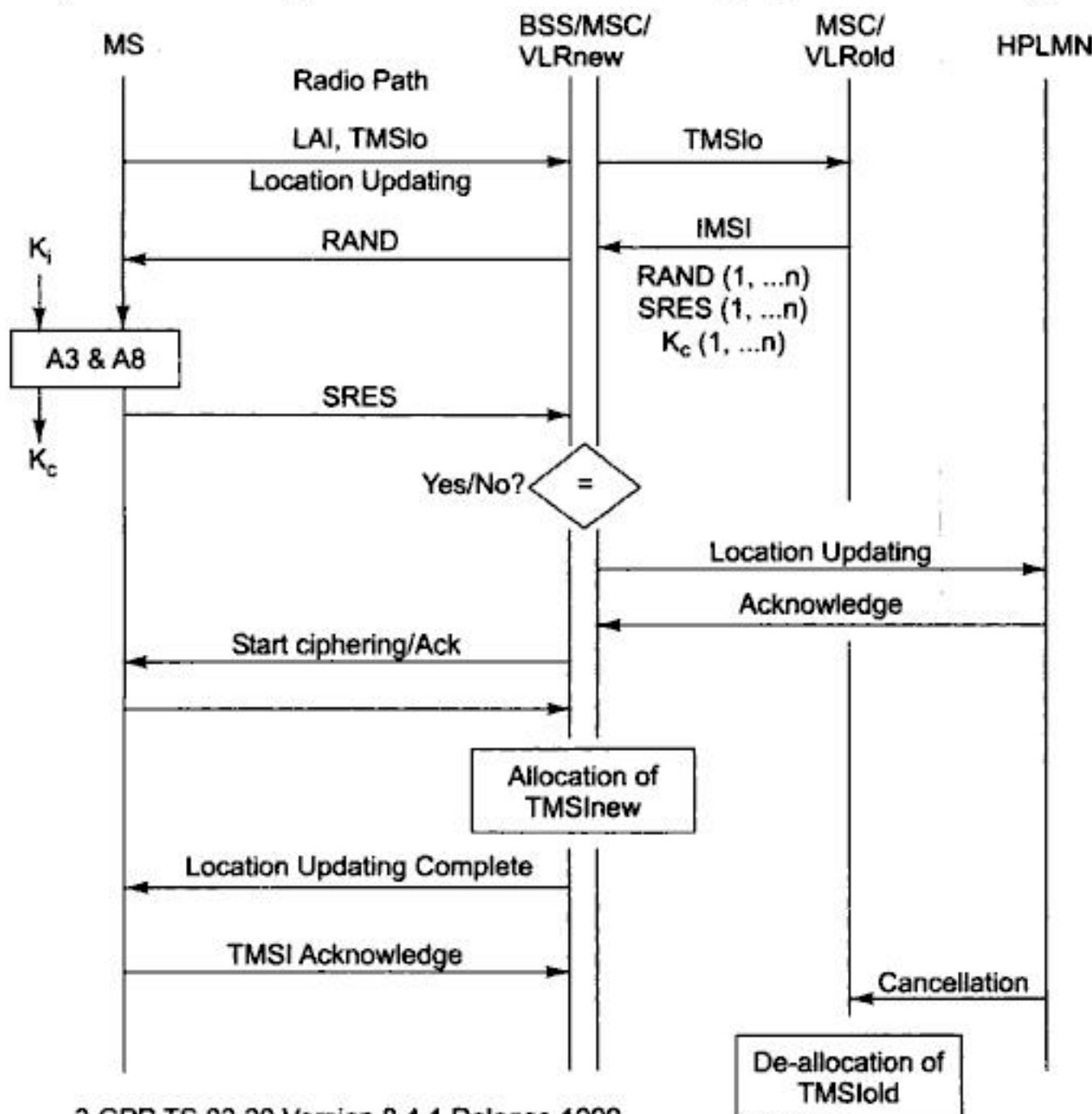
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

procedure. The MSC in this case will terminate the procedure with the old BSS by sending a Clear_Command with cause “Handover successful”. When the MS is successfully in communication with the network, i.e., the RR message Handover_Complete has been received from the MS, then the new BSS will immediately send a BSSMAP message Handover_Complete to the MSC and terminate the procedure. The MSC in this case will terminate the procedure with the old BSS by sending a Clear_Command with cause “Handover successful”.

5.8.4 Authentication and Security Issues during Handover

GSM uses A3, A8, and A5 algorithms (see Section 5.10) for security. A3 algorithm is used to authenticate the subscriber; A8 algorithm is used to generate the ciphering key K_c ; and, A5 algorithm is used to cipher everything that is transmitted over the air that include both signal and traffic. Security issues in GSM network are covered in detail in GSM standard 03.20.

When a handover occurs, the necessary information (e.g., key K_c , initialization data) is transmitted within the system infrastructure to enable the communication to proceed from the old BSS to the new BSS, and the synchronization procedure is resumed. The key K_c remains unchanged at handover.



3 GPP TS 03.20 Version 8.4.1 Release 1999

Figure 5.11 Normal Location Updating Procedure (Fig. 5.1)

Figure 5.11 illustrates the normal location updating procedure with all elements pertaining to security functions, i.e., TMSI (Temporary Mobile Subscriber Identity) management, authentication and K_c management. Here it is assumed that during the handover the MSC/VLR is changed from old VLR₀ to new VLR_n. During the Location Update the MS sends the LAI (Location Area Identifier) and the old TMSI₀ to the old VLR₀. The VLR₀ sends the series of challenges RAND (1, ..., n), and their respective answers SRES (1, ..., n) of challenges, and the respective ciphering keys K_c (1, ..., n) with the IMSI of the MS. VLR₀ receives all these RAND challenges from the HPLMN (Home Public Land Mobile Network). If the authentication is successful, the HLR is updated with new location; the ciphering starts with new K_c and a new TMSI is allocated. As part of housekeeping, the new VLR_n is registered in the HLR; the HLR also informs the VLR₀ to de-register the IMSI. The VLR₀ deletes all entries related to this IMSI including the TMSI₀.

5.8.5 Roaming

Handover relates to moving from one point of attachment to another point of attachment within the same network operator; when this movement happens between two different networks it is called roaming. Different networks imply two separate billing and charging domains.

When a mobile station is powered-off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected. When a mobile station is switched on in a new network (for example, the user has disembarked from an aircraft in a new country) or the subscriber moves to a different operator's PLMN (Public Land Mobile Network), the subscriber must register with the new network to indicate its current location. The first location update procedure is called the IMSI attach procedure where the MS indicates its IMSI to the new network. Normally, a location update message is sent to the new MSC/VLR, which records the location area information, and then sends the location information to the subscriber's HLR. If the mobile station is authenticated and authorized in the new MSC/VLR, the subscriber's HLR cancels the registration of the mobile station with the old MSC/VLR. A location update is also performed periodically. If after the updating time period, the mobile station has not registered, it is then deregistered.

Roaming is a killer application in GSM that allows users to seamlessly move around nationally and internationally and remain connected. Unlike routing in the fixed network, where a terminal is semi-permanently wired to a central office, GSM allows roaming around the world. When there is an incoming call for a subscriber, the mobile phone needs to be located, a channel needs to be allocated and the call connected. A powered-on mobile is informed of an incoming call by a paging message sent over the paging channel of the cells within the current location area. The location updating procedures, and subsequent call routing, use the MSC and both HLR and the VLR. The information sent to the HLR is normally the SS7 address of the new VLR. If the subscriber is entitled to service, the HLR sends a subset of the subscriber information needed for call control to the new MSC/VLR, and sends a message to the old MSC/VLR to cancel the old registration.

An incoming mobile terminating call is directed to the Gateway MSC (GMSC) function. The GMSC is basically a switch, which is able to interrogate the subscriber's HLR to obtain routing information and thus contains a table linking MSISDNs to their corresponding HLR. A simplification is to have a GMSC handle one specific PLMN. Though the GMSC function is distinct from the MSC function, it is usually implemented within an MSC. The routing information that is returned to the GMSC is the Mobile Station Roaming Number (MSRN), which is also

defined in the E.164 numbering plan that includes CC (Country Code), NDC (National Destination Code), and SN (Subscriber Number) (Fig. 5.7).

MSRN is a temporary location-dependent MSISDN number. It is assigned by the serving VLR for each MS in its area. MSRNs are numbers reserved by a PLMN only for roaming use; and, not assigned to subscribers, nor are they visible to subscribers. The allocation of MSRN is done in such a fashion that the currently responsible MSC in the visited network (CC+NDC) can do routing of the call quite easily.

The most general routing procedure begins with the GMSC querying the called subscriber's HLR for an MSRN (Fig. 5.7). The HLR typically stores only the SS7 address of the subscriber's current VLR. The VLR temporarily allocates an MSRN from its pool for the call. This MSRN is returned to the HLR and back to the GMSC, which can then route the call to the new MSC. At the new MSC, the IMSI corresponding to the MSRN is looked up, and the mobile is paged in its current location area. As a rule of thumb, HLR is referred for incoming call; whereas VLR is referred for outgoing call.

Roaming is of two types. These are:

- *Horizontal Roaming*: Horizontal roaming is between two networks from same family. For example, GSM to GSM roaming or GSM to UMTS roaming will be considered horizontal roaming.
- *Vertical Roaming*: Vertical roaming is between two networks from different families. For example, GSM to CDMA roaming or GPRS to WiFi will be considered vertical roaming. When vertical roaming happens without any disruption of session or service, it is called Seamless Roaming.

5.8.6 Roaming Example

Let us assume that the user's mobile number is +919844012345. This is a number in Spice network in Bangalore. The mobile subscriber is roaming in Mumbai. Somebody from a fixed phone in Mumbai wants to talk to this Spice subscriber. The caller (also known as 'A' party) dials 09844012345 from Mumbai. This call will be switched at the PSTN network in Mumbai and will be routed to Spice network in Bangalore. The Spice MSC will look at the HLR and know that the subscriber (called 'B' party) is now within the coverage of a mobile operator (Vodafone) in Mumbai—this is done using the MSRN. The call will be routed to the Mumbai MSC at Vodafone. The Vodafone MSC at Mumbai will look at its VLR to locate the Spice subscriber and route the call. Also, when the call is over, the charging information will be forwarded to the Spice network. Please note that for the incoming call, the routing always happens via the home network resulting in the call routing from Mumbai PSTN to Bangalore PLMN to Mumbai PLMN. The calling party (person in Mumbai) pays long distance tariff for Mumbai PSTN to Bangalore PLMN; the called party (Spice subscriber) pays for Bangalore PLMN to Mumbai PLMN long distance tariff in addition to roaming airtime charges. For outgoing call, the home network is not referred (other than the first time authentication), resulting in the call being directly routed by the visiting network. Let us consider the opposite scenario; the Spice subscriber from Bangalore is still roaming in Mumbai and wants to call someone in Mumbai. The Spice subscriber dials the Mumbai number, the Vodafone MSC looks at the VLR and routes the call directly to the Mumbai number. In this case, the Spice subscriber pays a local Mumbai to Mumbai call charge in addition to the airtime charges.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

5.10 PERSONAL COMMUNICATIONS SERVICE

Personal Communications Service (PCS) technology is a flavor of GSM technology for digital cellular phone services that use frequency bands of 1800 and 1900 MHz; though, PCS is also used to signify one-to-one personal communications over the wireless media. PCS is used to denote Digital Enhanced Cordless Telecommunications (DECT) in the 1920 MHz to 1930 MHz Satellite Personal Communications. In general, PCS signifies the 1900 MHz radio band digital cellular mobile phone system in North American countries like Canada, Mexico and the United States. In Hong Kong, however, PCS is used to refer to GSM-1800. Like the GSM, PCS offers services like voice, data, SMS and roaming.

5.10.1 PCS Switching Center

Like the GSM, the PCS switching center represents a collection of network elements. It is a service which supports access technology independent call control/service control and a connection control switching functions. It also facilitates interconnection of access and network systems to support end-to-end services.

5.10.2 Supportability for PCS Frequencies

As such, CDMA, GSM and D-AMPS systems can also be used on PCS frequencies. In spite of the fact that Dual-band GSM phones can work in both the 850 and 1900 MHz bands, they are incompatible with 900 and 1800 MHz European and Asian variants. However, GSM tri-band and quad-band phones offered by North American carriers usually support both European and other domestic frequencies.

5.11 AUTHENTICATION AND SECURITY

The radio medium is open to everybody and anybody. Anybody who can get hold of a radio receiver can access GSM signal or data. Therefore, it is necessary and important that the communication over the wireless radio media is secured. The first step to GSM security is the authentication. Authentication of a user is done to ensure that the user is really the person he claims to be. Authentication involves two functional entities, the SIM card in the mobile phone, and the Authentication Center (AUC). Authentication is done by using an algorithm by name A3. Following the authentication, a key is generated for encryption. An algorithm by the name A8 is used to generate the key. A different algorithm called A5 is used for both ciphering and deciphering procedures. The ciphering is done on both signaling, voice and data. This in other words means that SS7 signal, voice, data, and SMS within GSM are ciphered over the wireless radio interface.

The GSM specifications for security were designed by the GSM Consortium in secrecy and are distributed only on a need-to-know basis to hardware and software manufacturers and to GSM network operators. The specifications were never exposed to the public. The GSM Consortium relied on Security by Obscurity, i.e., the algorithms would be harder to crack if they were not publicly available.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

- www.gsmworld.com
 - www.wikipedia.org
17. 3GPP TS 08.06, Digital cellular telecommunications system (Phase 2+); Signalling Transport Mechanism Specification for the Base Station System - Mobile Services Switching Centre (BSS-MSC) Interface.
18. 3GPP TS 08.08, Digital cellular telecommunications system (Phase 2+); Mobile-services Switching Centre–Base Station System (MSC-BSS) interface; Layer 3 specification.
19. 3GPP TS 09.02 Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification.
20. 3GPP TS 23.122, 3rd Generation Partnership Project; Technical Specification Group Core Network; NAS Functions related to Mobile Station (MS) in idle mode.
21. 3GPP TR 23.908, Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Technical Report on Pre-paging.
22. 3GPP TS 29.018: 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); Serving GPRS Support Node (SGSN) - Visitors Location Register (VLR) Gs interface layer 3 specification.
23. 3GPP TS 29.198-14, Universal Mobile Telecommunications System (UMTS); Open Service Access (OSA) Application Programming Interface (API); Part 14: Presence and Availability Management (PAM) Service Capability Feature (SCF).

REVIEW QUESTIONS

- Q1: Describe the GSM architecture with its constituent elements.
- Q2: In GSM network, there are some databases used for various purposes. What are they? What are their functions?
- Q3: Explain the following in brief in the context of GSM networks:
- | | |
|--------------------|----------|
| (a) Mobile Station | (b) BSS |
| (c) NSS | (d) OSS |
| (e) IMSI | (f) IMEI |
| (g) TMSI | (h) MSRN |
- Q4: Explain mobile terminating call in the context of GSM networks.
- Q5: What is handover/handoff? How is handoff different from roaming?
- Q6: What is the role of AuC? How is authentication done in a GSM network?
- Q7: What are the different algorithms used for security in GSM?
- Q8: What are HLR and VLR? Describe the functions of HLR and VLR in call routing and roaming?
- Q9: What is a PLMN? How is PLMN connected to PSTN and PDN?
- Q10: What is PCS? Which areas of the world is it presently used in?
- Q11: What is the role of PCS switching center?
- Q12: Discuss the supportability for PCS frequencies.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

network is never used. This implies that an SMS message can be sent from any SC in any network to a GSM phone anywhere in the world. This makes any SM MT message mobile operator independent.

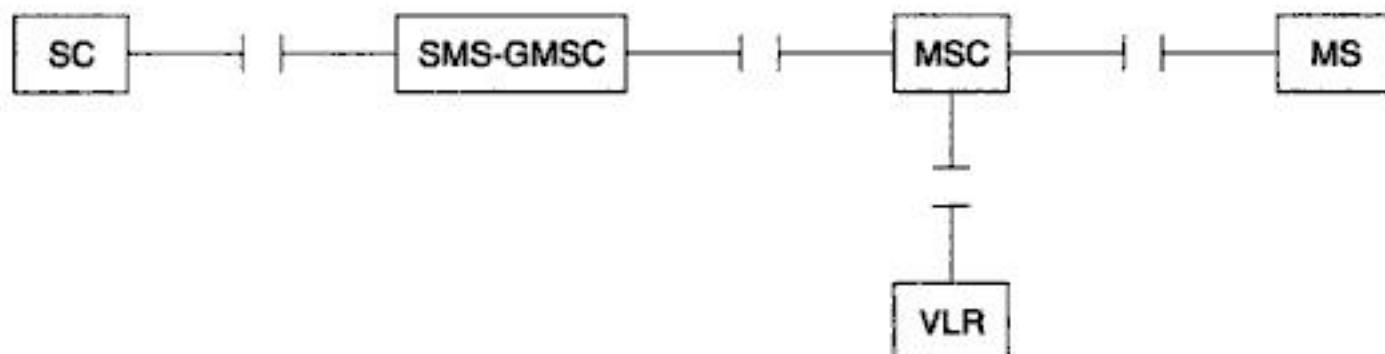


Figure 6.2 Interface Involved in the SM MT Procedure

6.2.4 Short Message Mobile Originated (SM MO)

SM MO is an outgoing message originated in the MS where generally the user types in a message and sends it to another MSISDN number or an application. For an MO message, the MSC forwards the message to the home SC of the sender. The SC is an independent computer in the network and works as a store and forward node with a large database. The database is used to store the SMSs. In SS7 terminology SC is an SCP (Service Control Point) within the SS7 cloud. MO message works in two asynchronous phases. In the first phase, the message is sent from the MS to the home SC as an MO message (Fig. 6.3). In the second phase, the message is sent from the home SC to the receiving MS as an MT message (Fig. 6.2). It is possible to attempt to send an SMS message to an invalid MSISDN number. In such a case, the message will be sent successfully from the MS to the SC. However, it will fail during the SC to the MS transfer. The user will see SM MO message sent successfully but SM MT message delivery would fail.

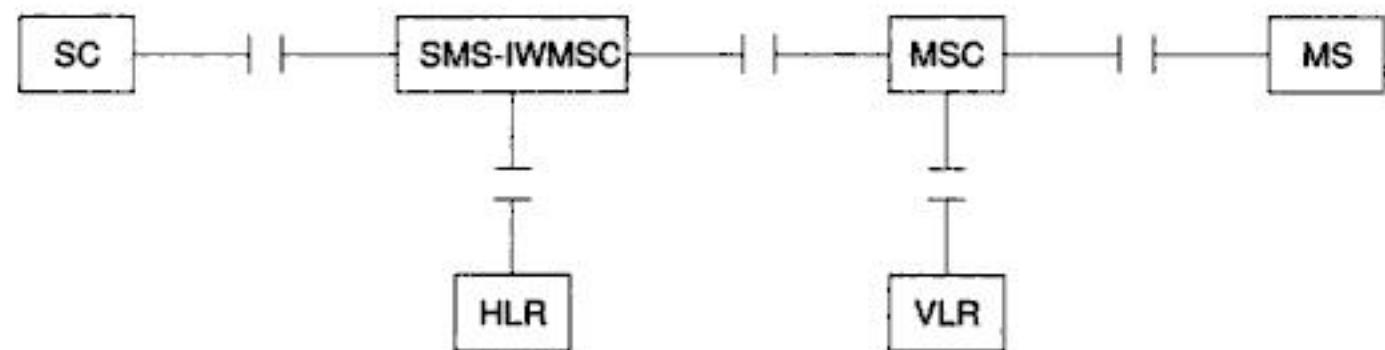


Figure 6.3 Interface Involved in the Short Message Mobile Originated (SM MO) Procedure

6.2.5 SMS as an Information Bearer

SMS is a very popular bearer in the person-to-person, mobile-to-mobile or point to point messaging domain. However, it is gaining popularity in other verticals like enterprise applications, services provided by independent service providers as ASP (Application Service Provider), and notification services, where one endpoint is a mobile phone but the other endpoint is a mobile application. Here SMS functions as an input-output media for information exchange for a mobile application (Fig. 6.4).

To use SMS as a bearer for any information service, we need to connect the services running on the Enterprise Origin server to the SC through an SME (Short Message Entity) or ESME (External Short Message Entity). SME in any network is generally a SMS gateway. With respect to SMS, a GSM subscriber is always in control of the SC in the home network irrespective of the serving network. Thus, if there is any SMS-based data service in the home network, it will be available to the subscriber from any foreign network.

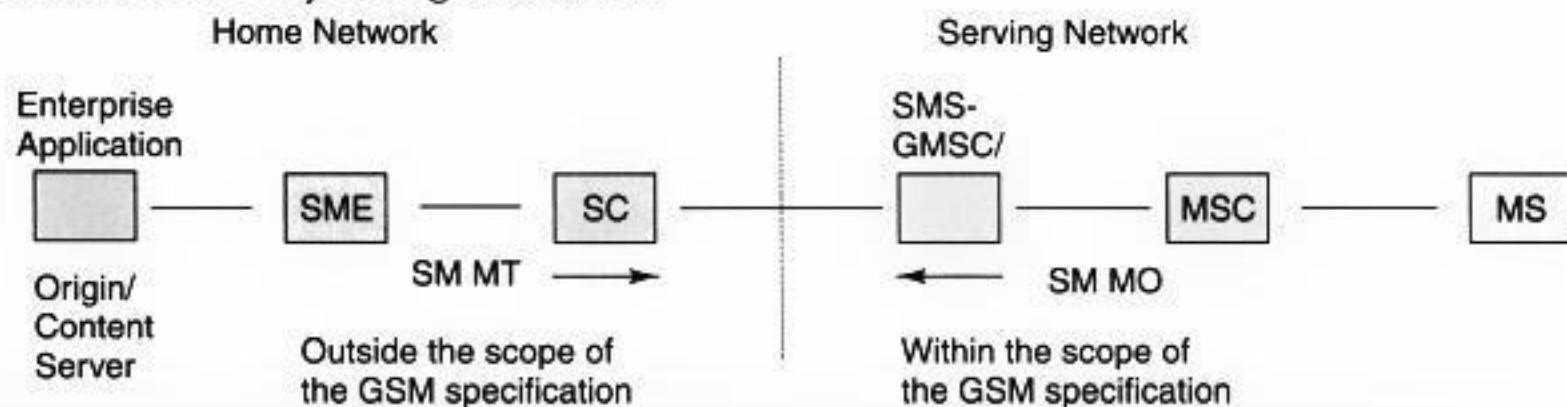


Figure 6.4 SMS as an Information Bearer/Medium for Mobile Applications

6.2.6 Operator-centric Pull

For an SMMO to work it is mandatory that an SC is used. As a part of SMS value added services, operators offer different information on demand and entertainment services. These are done through connecting an Origin server to the SC via an SMS gateway. In different parts of the world a new industry vertical has emerged to address this market. These service providers are known as MVNO (Mobile Virtual Network Operators). Virtual operators develop different systems, services, and applications to offer data services using SMS. Many enterprises use these MVNOs to make their services available to mobile phone users. There are quite a few banks in India which offer balance enquiry and other low security banking services over SMS. For example, if a HDFC customer wants to use these services, he needs to register for the service. During the registration, the HDFC customer needs to mention the MSISDN of the phone which will be used for this service. Once a user is registered for the service, he enters “HDFCBAL” and sends the message to a service number (like 333 for example in the case of Escotel) as an MO message. SC delivers this MO message to the SMS gateway (technically known as SME—Short Message Entity) connected to this service number. The SMS gateway then forwards this message to the enterprise application. The response from the enterprise application is delivered to the MS as an MT message from the SME. Even if the subscriber is in some remote region of a foreign network within GSM coverage, he can send the same SMS to the same service number in his home network. This makes the home services available in the foreign network. This also implies that an operator-centric SMS pull service is completely ubiquitous.

The connectivity between SC to SME and SME to Enterprise Origin server is not defined by GSM. However, there are a few de facto standard protocols for this communication. The most popular protocol is Short Message Peer to Peer (SMPP). There are certain other protocols like CIMD from Nokia as well. The connectivity between SME and Origin server could be anything like SOAP (Simple Object Access Protocol), or direct connection through TCP socket. However, common practice is through HTTP. HTTP helps user to get information from the Internet via SMS. There is an open source for SMS gateway called Kannel, which supports a multitude of

protocols and forwards the SMS enquiry as an HTTP request and gets information from the Internet. This is how an SMS can be converted into a simple Internet access. Conventionally SMS queries are keywords driven like “CRI” for live cricket score, or “RSK 2627 3 03” to get the availability of seat/berth in Indian Railways train number 2627 (Karnataka Express) for March 3. There are applications where SMS is used in session-oriented transactions. Applications like “SMS chat” and “SMS contests” need to remember the user context over multiple transactions.

6.2.7 Operator-independent Push

We have seen that it is possible to send an SMS to any phone in any network. For example, an MT message can be delivered from a network in India to an MS of UK roaming in Germany (Fig. 6.5). Which in other words means that any push, which may be an alert, notification or even response from a pull message generated by an application, can be serviced by any network and delivered to any GSM phone in any network without any difficulty.

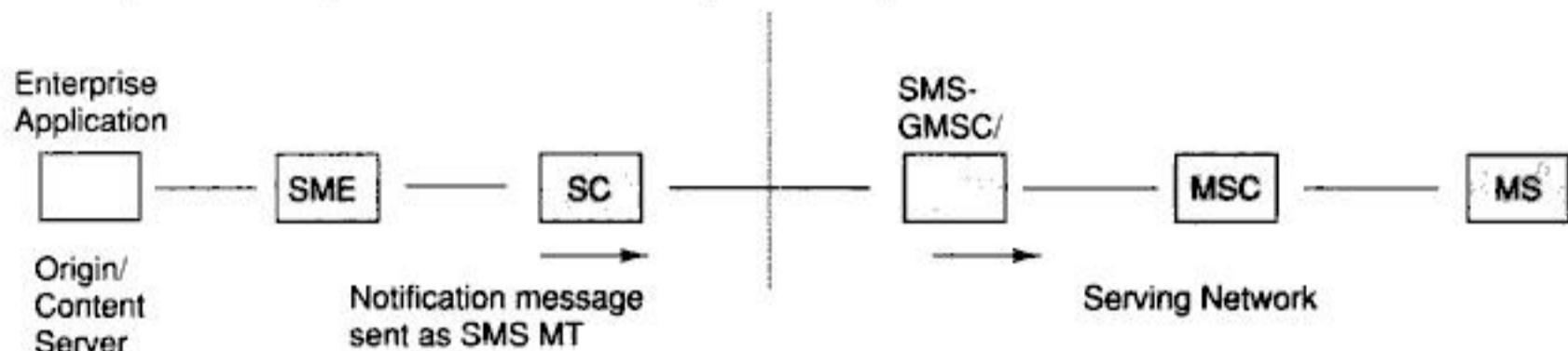


Figure 6.5 The Basic Network Structure of the SMS Push

Assuming that appropriate roaming tie-ups are in place, an enterprise can use SMS to send business alerts or proactive notifications to its customer anywhere, anytime on any GSM phone. With roaming tie-ups, operators reach an agreement on revenue share and call forwarding mechanism. Roaming tie-ups are a commercial issue rather than technical. Some credit card companies in India send SMS notifications to its cardholders in different networks using operator-independent push.

6.2.8 Challenge for SMS as a Mobile Computing Bearer

When it comes to offering enterprise services using SMS, the scene becomes difficult to manage. Let us take the example of Indian Bank. In Delhi, a customer of this bank who is a subscriber of operator “A” (Airtel) sends “HDFCBAL” to 300 to know the balance in his account. In the same city of Delhi another customer of the same bank who happens to be a subscriber of a different operator “B” (Essar) sends “HDFCBAL” to 1234 to get the balance information. HDFC bank has a sizable population of customers in the Middle East. The same banking services, which are available in India, are not available in the Middle East. The reason being both cellular operators “A” and “B” connect to the bank’s application through their private SC and SME, whereas the operators in Middle East do not have an SME to connect to the bank’s application. This is like in the early days of telephony when an enterprise used to announce different customer care numbers for different cities. If the enterprise did not have an office in a city, the customers had to make long distance

calls to customer care in some other city. All these changed with the introduction of the 1-800 service. Enterprises need something similar to 1-800 in SMS. Also, this gives some identity to the enterprise. My Inc for example may like to publish a number like +9198375MYINC for any of its customer anywhere in the world.

The major challenge for implementing ubiquitous service through SMS requires operator independent SM MO messages or operator independent pull services. The SMS routing needs to work exactly in the same fashion as 1-800 services.

6.2.9 Operator-independent Pull

As the SME is always connected to the home network's SC, with the conventional framework, it is not possible to route mobile originated SMS messages to any application or any SME of choice. There are ways by which an SMS message can be routed to some enterprise SME connected to external SC. This is achieved through SAT, where the SAT application running on the SIM card changes the SC number during the transmission of the SMS and forces the SMS to recognize a different SC of a different network as its home SC. In this case also, technically the SMS is sent to the SME connected to the home SC. SMS has always been considered a revenue generating tool for cellular operators. Therefore, the current framework suits a cellular operator very well. If a SMS service is operator dependent, the cellular operator can use this to its advantage. In today's global scenario an enterprise or a MVNO has its customers around the world subscribing to different GSM networks. To make this possible, enterprises need operator-independent pull as well. Operator-independent pull services can be achieved using GSM modem technology described in the following sections. Also, the same can be done using Intelligent Network Technologies.

6.3 VALUE ADDED SERVICES THROUGH SMS

Value Added Services (VAS) can be defined as services, which share one or more of the following characteristics:

- Supplementary service (not a part of basic service) but adds value to total service offering.
- Stimulates incremental demand for core services offering.
- Stands alone in terms of profitability and revenue generation potential.
- Can sometimes stand-alone operationally.
- Does not cannibalize basic service unless clearly favorable.
- Can be an add-on to basic service, and as such, may be sold at a premium price.
- May provide operational and/or administrative synergy between or among other services and not merely for diversification.

A GSM operator's primary business goal is to offer the network infrastructure. Voice, SMS are basic services provided by a GSM operator. However, offering different other services using SMS as a bearer will be a VAS. There are various flavors and variations of VAS over SMS. We will give some examples and discuss how to develop them. The most popular VAS over SMS are entertainment and information on demand. Information on demand has three categories as described below.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```

Recv: OK
Sent: AT+CMGS="9810080856"
> This SMS message is being sent from a computer using
    hyper-terminal and my Nokia phone<ctrl-Z>
Recv: +CMGS: 122
OK

```

In this example, we use the standard Hayes Modem command sets. We send the AT (In Hayes terminology this is known as attention) command to the modem from the computer. The GSM modem responds by saying "OK". This means that the modem is ready and can take instructions. We then set the message format to text mode through CMGF command. In the next request we send AT+CMGS="9810080856". This is to send a SMS message to a mobile with MSISDN 9810080856. The GSM modem accepts the request and responds with a '>' sign. This is a prompt from the modem requesting for the user input. The user enters the data followed by a control "Z". "^Z" (control z, 0x1A) is used to indicate the end of message. When the message is sent, the GSM modem responds with a number 122. This number is the message identifier of the message successfully sent.

AT command can also be used for other functions of the phone. Most of the functions available as a part of MMI (Man Machine Interface), are available through AT command. Examples could be sending an SMS, read an SMS; check battery power or write a phone book entry. Following is a list of the AT commands supported for SMS.

SMS Text Mode

AT+CSMS	Select Message Service
AT+CPMS	Preferred Message Storage
AT+CMGF	Message Format
AT+CSCA	Service Center Address
AT+CSMP	Set Text Mode Parameters
AT+CSDH	Show Text Mode Parameters
AT+CSCB	Select Cell Broadcast Message Types
AT+CSAS	Save Settings
AT+CRES	Restore Settings
AT+CNMI	New Message Indications to TE
AT+CMGL	List Messages
AT+CMGR	Read Message
AT+CMGS	Send Message
AT+CMSS	Send Message from Storage
AT+CMGW	Write Message to Memory
AT+CMGD	Delete Message

SMS PDU Mode

AT+CMGL	List Messages
---------	---------------



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

<i>TPDU Octet 3</i>	<i>Value</i>	<i>Description</i>	<i>Status</i>
	0B	Address length	Length of the address is 11 in decimal.
<i>TPDU Octet 4</i>	<i>Value</i>	<i>Description</i>	<i>Status</i>
	91	Type of address	International address using ISDN telephone number plan.
<i>TPDU Octets 5-10</i>	<i>Value</i>	<i>Description</i>	<i>Status</i>
	72 38 88 09 00 F1	TP-Destination-Address	The destination telephone number +27838890001 is encoded as 72 38 88 09 00 F1. In this case the address is 11 digit, therefore a F is added to make it occupy 6 octets. The address field can be anywhere between 2 to 12 octets long.
<i>TPDU Octet 11</i>	<i>Value</i>	<i>Description</i>	<i>Status</i>
	00	TP-Protocol-Identifier, consists of one octet.	Short Message Type 0. This means that the ME must acknowledge receipt of the short message but may discard its contents.
<i>TPDU Octet 12 bits</i>	<i>Value (hex 15)</i>	<i>Description</i>	<i>Status</i>
7	0	TP-Data-Coding-Scheme used in TPUser-Data, consists of one octet. See GSM 3.38	Functionality (bits 7 and 6) related to usage of bits 4-0.
6	0		Functionality (bits 7 and 6) related to usage of bits 4-0.
5	0		Indicates that text is uncompressed
4	0		Indicated that bits 1 and 0 have message class meaning.
3	0	Alphabet being used (bits 3 and 2)	8-bit data
2	0	Alphabet being used (bits 3 and 2)	8-bit data
1	0	Message class (bits 1 and 0)	Class 1, Default meaning: MEspecific
0	0	Message class (bits 1 and 0)	Class 1, Default meaning: MEspecific

(Contd)



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

These network nodes are called GPRS support nodes (GSN). GPRS support nodes are responsible for the delivery and routing of data packets between the mobile stations and the external packet data networks (PDN). There are two types of support nodes, viz., SGSN (Serving GSN) and GGSN (Gateway GSN). Figure 7.1 depicts GPRS system components for data services.

Serving GPRS Support Node (SGSN): A serving GPRS support node (SGSN) is at the same hierarchical level as the MSC. Whatever functions MSC does for voice, SGSN does the same for packet data. SGSN's tasks include packet switching, routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions. SGSN processes registration of new mobile subscribers and keeps a record of their location inside a given service area. The location register of the SGSN stores location information (e.g., current cell, current VLR) and user profiles of all GPRS users registered with this SGSN. SGSN sends queries to Home Location Register (HLR) to obtain profile data of GPRS subscribers. The SGSN is connected to the base station system with Frame Relay.

Gateway GPRS Support Node (GGSN): A gateway GPRS support node (GGSN) acts as an interface between the GPRS backbone network and the external packet data networks. GGSN's function is similar to that of a router in a LAN. GGSN maintains routing information that is necessary to tunnel the Protocol Data Units (PDUs) to the SGSNs that service particular mobile stations. It converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format for the data networks like Internet or X.25. PDP sends these packets out on the corresponding packet data network. In the other direction, PDP receives incoming data packets from data networks and converts them to the GSM address of the destination user. The readdressed packets are sent to the responsible SGSN. For this purpose, the GGSN stores the current SGSN address of the user and his or her profile in its location register. The GGSN also performs authentication and charging functions related to data transfer.

7.3.1 GPRS Network Enhancements

In addition to the new GPRS components (SGSN and GGSN), some existing GSM network elements must also be enhanced in order to support packet data. These are:

Base Station System (BSS): BSS system needs enhancement to recognize and send packet data. This includes BTS upgrade to allow transportation of user data to the SGSN. Also, the BTS needs to be upgraded to support packet data transportation between the BTS and the MS (Mobile Station) over the radio.

Home Location Register (HLR): HLR needs enhancement to register GPRS user profiles and respond to queries originating from GSNs regarding these profiles.

Mobile Station (MS): The mobile station or the mobile phone for GPRS is different from that of GSM.

SMS Nodes: SMS-GMSCs and SMS-IWMSCs are upgraded to support SMS transmission via the SGSN. Optionally, the MSC/VLR can be enhanced for more efficient coordination of GPRS and non-GPRS services and functionality.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Medium Access Control (MAC): The medium access control (MAC) layer controls the access attempts of an MS on the radio channel shared by several MSs. It employs algorithms for contention resolution, multiuser multiplexing on a packet data traffic channel (PDTCH), and scheduling and prioritizing based on the negotiated QoS.

Physical Layer

The physical layer between MS and BSS is divided into two sublayers: the physical link layer (PLL) and the physical RF Layer (RFL).

Physical Link Layer (PLL): This layer provides services for information transfer over a physical channel between the MS and the network. These functions include data unit framing, data coding, and the detection and correction of physical medium transmission errors. The Physical Link layer uses the services of the Physical RF layer.

Physical RF Layer (RFL): This layer performs the modulation of the physical waveforms based on the sequence of bits received from the Physical Link layer above. The Physical RF layer also demodulates received wave forms into a sequence of bits that are transferred to the Physical Link layer for interpretation.

Multiple Access Radio Resource Management

On the radio interface, GPRS uses a combination of FDMA and TDMA. As in GSM (Fig. 5.10), GPRS uses two frequency bands at 45 MHz apart; viz., 890–915 MHz for uplink (MS to BTS), and 935–960 MHz for downlink (BTS to MS). Each of these bands of 25 MHz width is divided into 124 single carrier channels of 200 kHz width. Each of these 200 kHz frequency channels is divided into eight time slots. Each time slot of a TDMA frame lasts for a duration of 156.25 bit times and contains a data burst.

On top of the physical channels, a series of logical channels are defined to perform functions like signaling, broadcast of general system information, synchronization, channel assignment, paging or payload transport. As with GSM, these channels can be divided into two categories: traffic channels and signaling channels. Traffic channel allocation in GPRS is different from that of GSM. In GSM, a traffic channel is permanently allocated for a particular user during the entire call period (whether any data is transmitted or not). In contrast, in GPRS traffic, channels are only allocated when data packets are sent or received. They are released after the transmission of data. GPRS allows a single mobile station to use multiple time slots of the same TDMA frame for data transmission. This is known as multislot operation and uses a very flexible channel allocation. One to eight time slots per TDMA frame can be allocated for one mobile station. Moreover, uplink and downlink are allocated separately, which efficiently supports asymmetric data traffic like Internet where the bandwidth requirements in uplink and downlink are different.

In GPRS, physical channels to transport user data packet is called data traffic channel (PDTCH). The PDTCHs are taken from a common pool of all channels available in a cell. Thus, the radio resources of a cell are shared by all GPRS and non-GPRS mobile stations located within the cell. The mapping of physical channels to either packet switched data (in GPRS mode) or circuit switched data (in GSM mode) services are performed dynamically depending on demand. This is done depending on the current traffic load, the priority of the service and the multislot class. A load supervision procedure monitors the load of the PDTCHs in the cell. According to the demand, the



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

GSNs of the same PLMN or the same network operator. These are private packet-based networks of the GPRS network provider; for example, Airtel GSNs in Bangalore connecting to Airtel GSNs in Delhi through a private data network. In the diagram, these intra-PLMN networks are connected with an inter-PLMN backbone. An inter-PLMN backbone network connects GSNs of different PLMNs and operators. To install such a backbone, a roaming agreement is necessary between two GPRS network providers. For example, Airtel GSNs in Bangalore connect to Vodafone GSNs in Delhi. The gateways between the PLMNs and the external inter-PLMN backbone are called border gateways. Among other things, they perform security functions to protect the private intra-PLMN backbones against unauthorized users and attacks.

We assume that the packet data network is an IP network. A GPRS mobile station located in PLMN1 sends IP packets to a host connected to the IP network, e.g., to a Web server connected to the Internet. The SGSN that the mobile station is registered with encapsulates the IP packets coming from the mobile station, examines the PDP context and routes them through the intra-PLMN GPRS backbone to the appropriate GGSN. The GGSN decapsulates the packets and sends them out on the IP network, where IP routing mechanisms are used to transfer the packets to the access router of the destination network. The latter delivers the IP packets to the host.

Let us assume the home-PLMN of the mobile station is PLMN2. An IP address has been assigned to the mobile by the GGSN of PLMN2. Thus, the MS's IP address has the same network prefix as the IP address of the GGSN in PLMN2. The correspondent host is now sending IP packets to the MS. The packets are sent out onto the IP network and are routed to the GGSN of PLMN2 (the home-GGSN of the MS). The latter queries the HLR and obtains the information that the MS is currently located in PLMN1. It encapsulates the incoming IP packets and tunnels them through the inter-PLMN GPRS backbone to the appropriate SGSN in PLMN1. The SGSN decapsulates the packets and delivers them to the MS.

The HLR stores the user profile, the current SGSN address, and the PDP addresses for every GPRS user in the PLMN. For example, the SGSN informs the HLR about the current location of the MS. When the MS registers with a new SGSN, the HLR will send the user profile to the new SGSN. The signaling path between GGSN and HLR may be used by the GGSN to query a user's location and profile in order to update its location register.

7.4.5 Communicating with the IP Networks

A GPRS network can be interconnected with Internet or a corporate intranet. GPRS supports both IPv4 and IPv6. From an external IP network's point of view, the GPRS network looks like any other IP sub-network, and the GGSN looks like a usual IP router. Figure 7.5 shows an example of how a GPRS network may be connected to the Internet. Each registered user who wants to exchange data packets with the IP network gets an IP address. The IP address is taken from the address space of the GPRS operator maintained by a DHCP server (Dynamic Host Configuration Protocol). The address resolution between IP address and GSM address is performed by the GGSN, using the appropriate PDP context.

Moreover, a domain name server (DNS) managed by the GPRS operator or the external IP network operator is used to resolve host names. To protect the PLMN from unauthorized access, a firewall is installed between the private GPRS network and the external IP network. With this



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

- TDMA IS-136
- i-mode
- 3G systems—IMT-2000, UMTS, W-CDMA, Wideband IS-95.

WAP can be used through 2G, 2.5G, and 3G networks. There is a perception that WAP or MMS requires GPRS networks. This is not correct. WAP and MMS can be accessed technically from a 2G network using CSD. However, high-speed data networks like GPRS are more suitable for WAP and MMS applications.

8.2 WAP

WAP forum develops standards for application deployment over wireless devices like PDAs and mobile phones. WAP is based on layered architecture. The WAP Protocol Stack is similar to the OSI network model (Fig. 8.1). These layers consist (from top to bottom) of:

- Wireless Application Environment (WAE).
- Wireless Session Protocol (WSP).
- Wireless Transaction Protocol (WTP).
- Wireless Transport Layer Security (WTLS).
- Wireless Datagram Protocol (WDP).

The application environment of WAE comprises multiple components to provide facilities like:

- User agent: the browser or a client program.
- Wireless Markup Language (WML): a lightweight markup language, similar to HTML, but optimized for use in wireless devices.

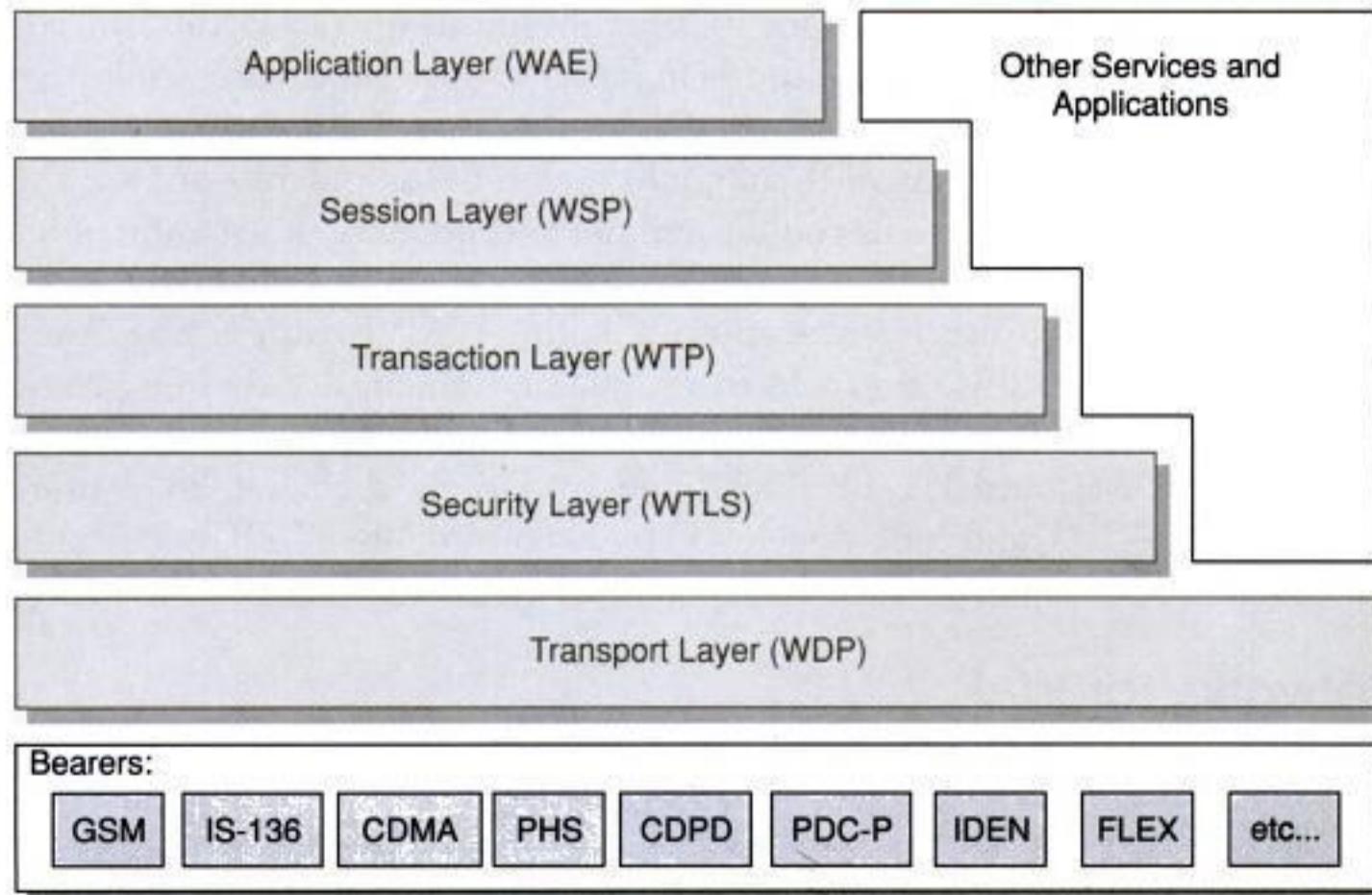


Figure 8.1 WAP Layered Architecture and Protocol Stack



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

8.2.5 WMLScript

WMLScript is an extended subset of JavaScript and forms a standard means for adding procedural logic to WML decks. WMLScript is used to do client side processing. Therefore, it can be used very effectively to add intelligence to the client and enhance the user interface. Using WMLScript, it is possible to access the device resources. WMLScript provides the application programmer with a variety of interesting capabilities. These are as follows:

- The ability to do local validation of user input before it is sent to the content server.
- The ability to access device resources, functions, and peripherals.
- The ability to interact with the user without reference to the origin server.

Key WMLScript features include:

- *JavaScript-based scripting language*: WMLScript is based on industry standard JavaScript solution and adapts it to the narrow-band environment.
- *Procedural Logic*: WMLScript adds the power of procedural logic to WML.
- *Compiled implementation*: WMLScript can be compiled to a more space efficient bytecode that is transported to the client.
- *Event-based*: WMLScript may be invoked in response to certain user or environmental events.
- *Integrated into WAE*: WMLScript is fully integrated with the WML browser. WMLScript has access to the WML state model and can set and get WML variables.
- *International Support*: WMLScript supports Unicode 2.0.
- *Efficient extensible library support*: WMLScript can be used to expose and extend device functionality without changes to the device software.
- *Data types*: Following basic data types are supported in WMLScript: *boolean*, *integer*, *floating-point*, *string* and *invalid*. WMLScript attempts to automatically convert between the different types as needed.

8.2.6 Wireless Telephony Application (WTA, WTAI)

WAP offers WTAI (Wireless Telephony Application Interface) functions to create Telephony Applications. This is achieved through a wireless telephony application (WTA) user-agent using the appropriate WTAI function. For example, let us say that we want to book a table for a lunch meeting in a restaurant. From the WAP application, we go to the restaurant site and get the telephone number. In normal case we note down the telephone number on a piece of paper, exit from the browser session, and then make a voice call to book the table. In case of WTAI that is not required. We can display an action item call in the WAP screen and make a call straight from the WAP page. The WTAI function libraries are accessed from server side using URL's; or at the client side through WMLScript.

There are different library functions to do different telephony functions:

- *Voice Call Control*: This library handles call set-up and control of device during an ongoing Call. The call may be either outgoing or incoming.
- *Network Text*: Using this library, SMS text messages can be integrated with the WML, WMLScript functions.
- *Phonebook*: Using this library, the phonebook entries in the device can be manipulated.
- *Call Logs*: Using this library, call logs in the device can be accessed.

8.2.7 WAP Push Architecture

The WAP Push framework allows information to be sent to a client device without a previous user action. In a normal client/server model, a client requests for a service or information from a server. The server then responds to this request by transmitting information back to the client. This is referred to as pull technology (Fig. 8.4), where the client pulls information from the server. In addition to this type of synchronized request response transaction, WAP offers push technology (Fig. 8.5). Push is also based on the client/server model, but there is no explicit request from the client before the server transmits its content. This can be termed as unsolicited response. In other words, “pull” transactions are always initiated from the client, whereas, “push” transactions are server-initiated. Push technology is helpful to implement alerts and notification.

8.2.8 The Push Framework

The push content generally is originated in a server in the Internet that needs to be delivered to a mobile phone. The Push Initiator contacts the Push Proxy Gateway (PPG) from the Internet side, delivering content for the destination client (Fig. 8.6). The PPG then forwards the content to the mobile network to be delivered to the destination client over-the-air. In addition to providing simple proxy gateway services, the PPG is capable of notifying the Push Initiator about the final outcome of the push operation. It may even wait for the client to accept or reject the content in two-way mobile networks (MMS uses this function).

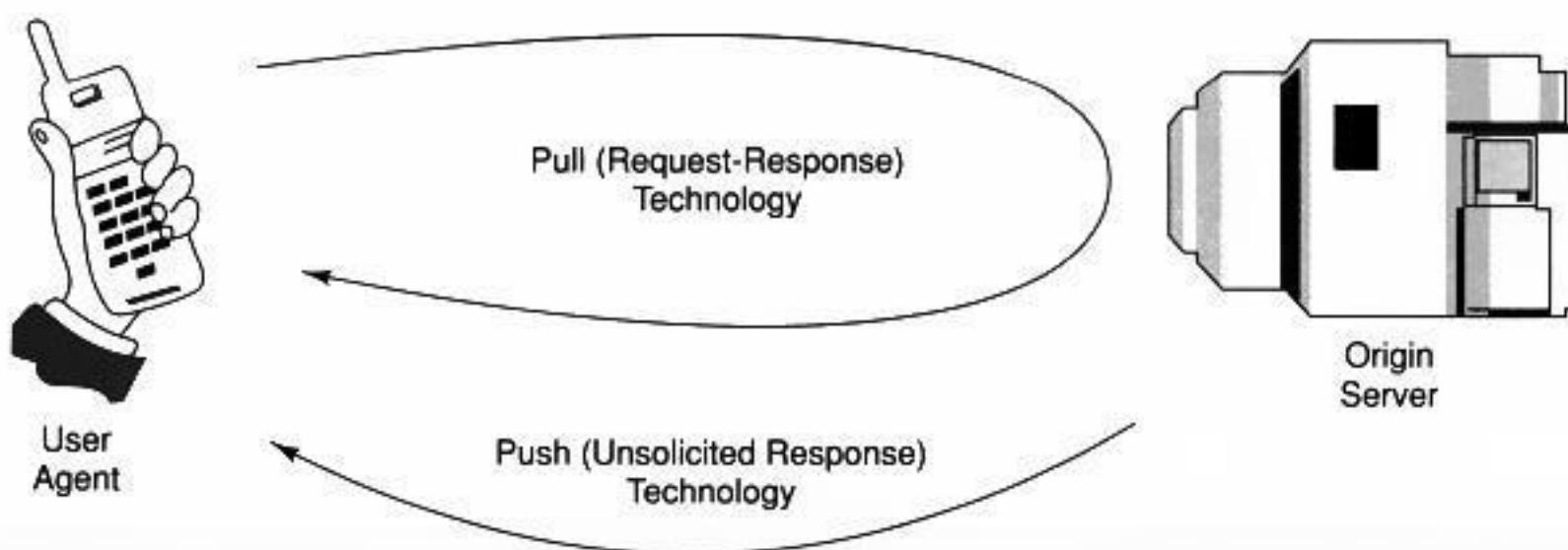


Figure 8.4 Pull versus Push Technology

The Internet-side PPG access protocol is called the *Push Access Protocol*. The WAP-side (OTA) protocol is called the *Push Over-The-Air Protocol*.

8.2.9 Wireless Session Protocol (WSP)

The Wireless Session Protocol (WSP) provides a consistent interface between two session services (client and server). It provides the cooperating client/server applications to:

- (a) Establish a reliable session from client to server and close it in an orderly manner.
- (b) Agree on a common level of protocol functionality using capability negotiation.

- (c) Exchange content between client and server using compact encoding.
- (d) Suspend and resume the session.

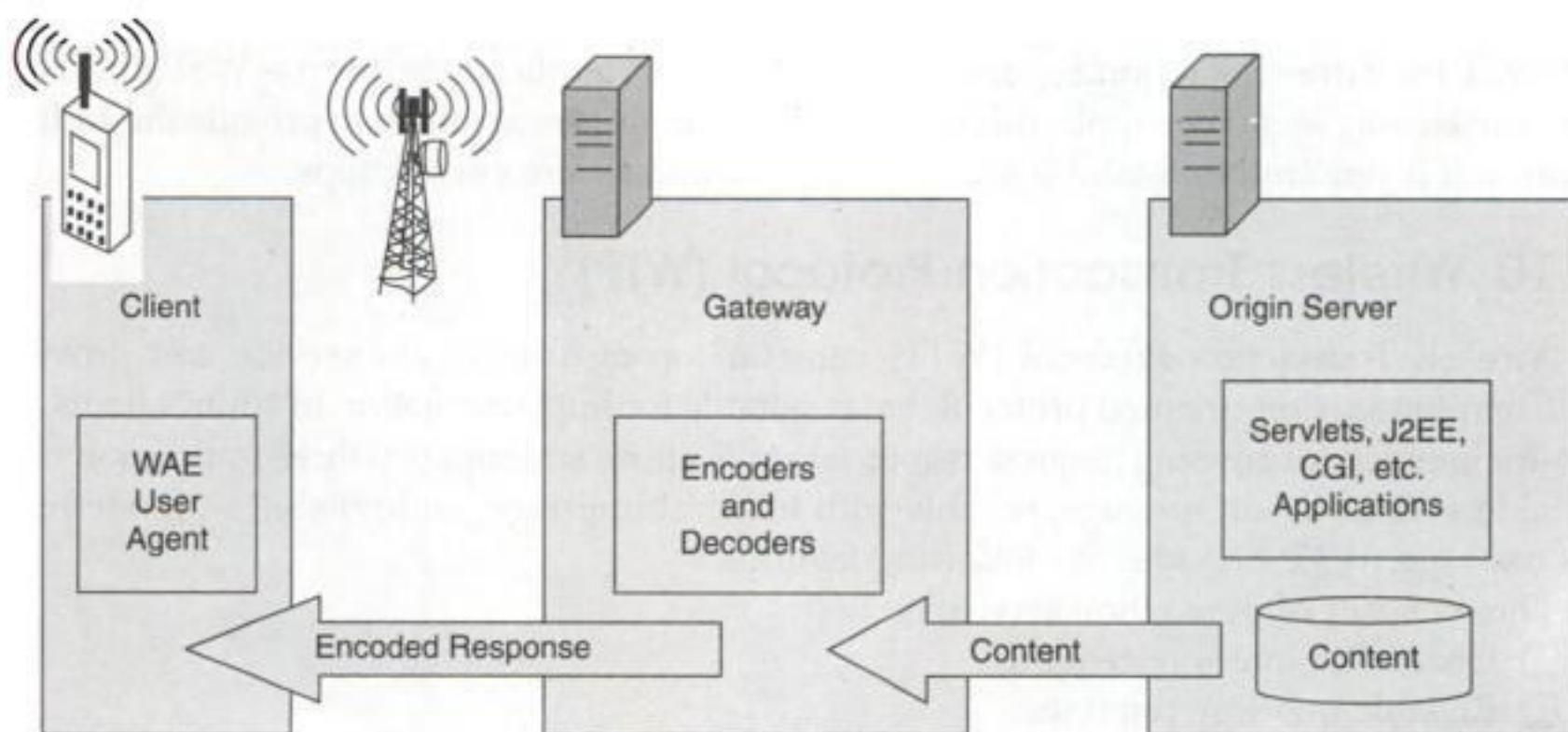


Figure 8.5 WAE Push-based Model

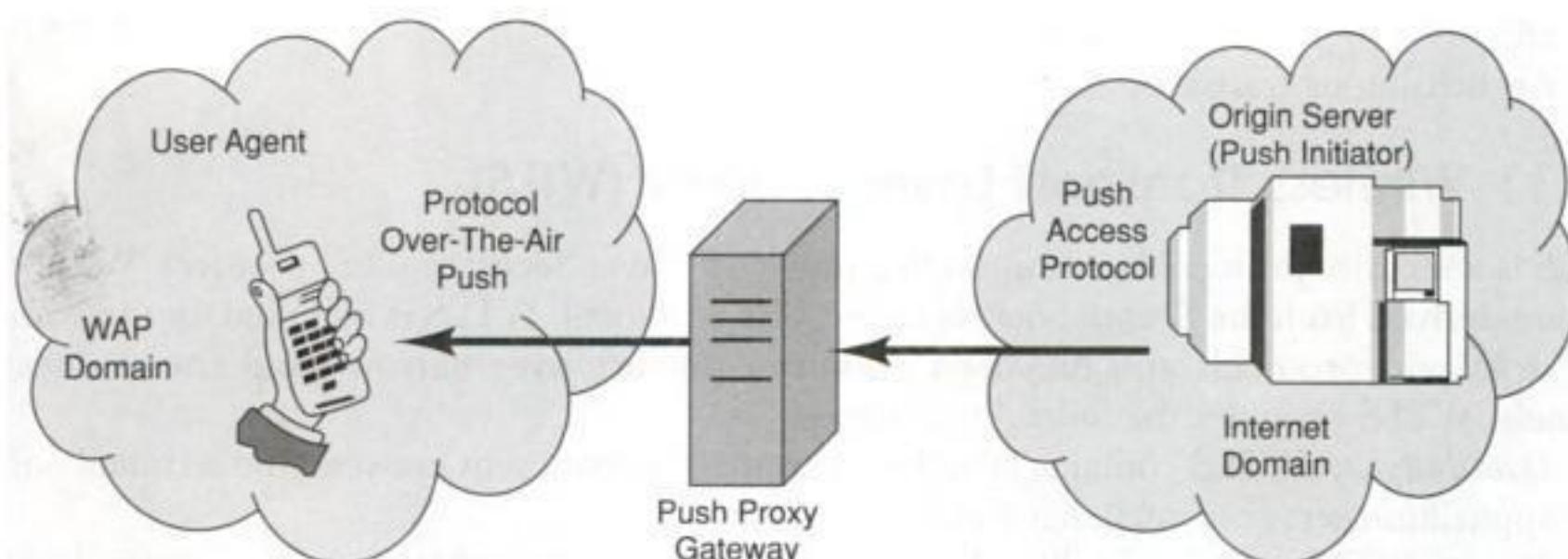


Figure 8.6 Push Framework with PPG (Push Proxy Gateway)

Currently the scope of WSP is suited mostly for browsing applications. It offers both connection-oriented and connectionless service. The connectionless service is most suitable, when applications do not need reliable delivery of data and do not care about confirmation.

The connection-oriented session services are divided into the following categories:

- Session Management facility.
- Method Invocation facility.
- Exception Reporting facility.
- Push facility.

- Confirmed Push facility.
- Session Resume facility.

WSP is designed to function on the transaction and datagram services between WAE and the WTP. WSP itself does not require a security layer; however, applications that use WSP may require it. The transaction, session or application management entities are assumed to provide the additional support that is required to establish security contexts and secure connections.

8.2.10 Wireless Transaction Protocol (WTP)

The Wireless Transaction Protocol (WTP) runs on top of a datagram service and provides a lightweight transaction-oriented protocol that is suitable for implementation in “thin” clients. WTP allows for interactive browsing (request/response) applications and supports three transaction classes: unreliable with no result message, reliable with no result message, and reliable with one reliable result message. WTP provides the following features:

- Three classes of transaction service are:
 - Unreliable one-way requests.
 - Reliable one-way requests.
 - Reliable two-way request-reply transactions.
- Optional user-to-user reliability: WTP user triggers the confirmation of each received message;
- Optional out-of-band data on acknowledgements;
- PDU concatenation and delayed acknowledgement to reduce the number of messages sent; and
- Asynchronous transactions.

8.2.11 Wireless Transport Layer Security (WTLS)

WTLS is a security protocol based upon the Transport Layer Security (TLS) protocol. WTLS and TLS are derived from the Secure Sockets Layer (SSL) protocol. WTLS is intended for use with the WAP transport protocols and has been optimized for use over narrow-band communication channels. WTLS provides the following features:

- *Data Integrity*: WTLS contains facilities to ensure that data sent between the terminal and an application server is unchanged and uncorrupted.
- *Privacy*: WTLS contains facilities to ensure that data transmitted between the terminal and an application server is private and cannot be seen by any intermediate parties that may have intercepted the data stream.
- *Authentication*: WTLS contains facilities to establish the authenticity of the terminal and application server.
- *Denial-of-service Protection*: WTLS contains facilities for detecting and rejecting data that is replayed or not successfully verified. WTLS makes many typical denial-of-service attacks harder to accomplish and protects the upper protocol layers.

8.2.12 Wireless Data Protocol (WDP)

The Transport layer protocol in the WAP architecture is referred to as the Wireless Datagram Protocol. The WDP layer operates above the data capable bearer services supported by the various



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Multimedia Integration Language). This may be a slide show with multiple or even a single slide. The slide show may combine a number of still pictures or animations into one MMS message. The display areas of these slides are divided into different sections. Currently, there are only two sections per slide—one for an image and one for the text. It is also acceptable to have either just an image or a text region. In the second phase, users can record their own video content (10 second video clip) and send it via MMS. The contents of the slides—the actual images, text, and audio—are separate pieces that are sent along with the slides. The maximum size of the entire packaged message that first generation devices could support was 50 kB.

8.3.1 MMS Architecture

The connection between different networks in Figure 8.8 is provided by the Internet protocol and its associated set of messaging protocols. This approach enables messaging in wireless networks to be compatible with messaging systems found on the Internet. Multimedia Message Service Environment (MMSE) encompasses various elements required to deliver a MMS (Fig. 8.9). This includes:

- *MMS Client*: This is the entity that interacts with the user. It is an application on the user's wireless device.
- *MMS Relay*: This is the system element that the MMS client interacts with. It provides access to the components that provide message storage services. It is responsible for messaging activities with other available messaging systems. The SMS relay along with the MMS content server is referred to as MMSC (MMS Controller).
- *WAP Gateway*: It provides standard WAP services needed to implement MMS.
- *MMS Server*: This is the content server, where the MMS content is generated
- *Email Server*: MMS can integrate seamlessly to the email system of Internet.

The messages that transit between the MMS Client and MMS Relay pass through WAP Gateway. Data is transferred between the MMS client and WAP gateway using WAP Session Protocol (WSP). Data is transferred between the WAP gateway and the MMS Relay using HTTP.

8.3.2 MMS Transaction Flows

As mentioned earlier, the MMS service is realized by the invocation of transactions between the MMS Client and the MMS Relay. The general transactions of sending and retrieving messages do not depend on what type of client the message is sent to or received from. The other endpoint for the message may be another MMS Client or a client on a legacy wireless messaging system or it may even be an email server.

The above message exchanges can be considered to form the following logically separate transactions (Fig. 8.10):

- MMS Client (sender) sends a message to MMS Relay (M-Send.req, M-Send.conf).
- MMS Relay notifies MMS Client (recipient) about a new message arrival (M-Notification.ind, M-NotifyResp.ind).
- MMS Client fetches (recipient) a message from MMS Relay (WSP GET.req, M-Retrieve.conf).



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

```
<meta name="title" content="vacation photos" />
<meta name="author" content="Radha Krishna" />
<layout>
  <root-layout width="160" height="120"/>
  <region id="Image" width="100%"
    height="80" left="0" top="0" />
  <region id="Text" width="100%"
    height="40" left="0" top="80" />
</layout>
</head>
<body>
  <par dur="8s">
    
    <text src="FirstText.txt" region="Text" />
    <audio src="FirstSound.amr"/>
  </par>
  <par dur="7s">
    
    <text src="SecondText.txt" region="Text" />
    <audio src="SecondSound.amr" />
  </par>
</body>
</smil>
```

The example above is for a terminal whose screen will displays the slide in a portrait orientation, where the height is greater than the width. On a PC screen, the SMIL slides are all displayed and are exactly 160 pixels wide and 120 pixels tall. The total slide area is divided into two smaller areas. The image region will be 80 pixels tall and always appears above the 40 pixel tall text area. On an MMS client, however, this will be different. The screen may not be large enough to accommodate the layout. Each slide in turn contains at least two elements: one for the image region and one for the text region. Two of the slides also contain an audio element that will be played when the slide is viewed. In normal SMIL, the names of the layout regions (image and text in our MMS message) are just handy names for generic regions that can contain any type of content. In MMS SMIL, however, the image region must contain an image element and the text region, a text element.

As we can see, the SMIL markup is very similar to HTML or WML markup language. The entire message body is enclosed within `<smil></smil>` tags and the message (or document) itself has both head and body sections. The head section contains information that applies to the entire message. The title and author meta fields here correspond to the From and Subject fields of the message. These meta fields are optional. Under MMS implementations of SMIL, a client is free to re-format the layout in a way best suited to the client's display. Actual slides are within the body section of the message. These slides are denoted with the `par`—for parallel tag. Parallel denotes that all the elements within the tag are to be displayed simultaneously. The `dur` attribute for each slide is the duration of the slide in the slide show. Again, the receiving client is free to modify or ignore this, replacing duration with a button for the next slide, for example.

The following are the specific media formats that will be supported in the first generation of MMS systems.

Images: Image formats supported are baseline JPEG with JFIF exchange format, GIF87a, GIF89a, and WBMP. The maximum guaranteed image resolution is 160 pixels wide by 120 pixels high. Larger images are supported, but need to be converted for the target device. The browser safe color palette (256 colors) is recommended for color image. JPEG is better suited for rendering photographs; whereas, GIF is a better choice for line drawings.

Text: The text of the message may use us-ascii, utf-8, or utf-16 character encoding. The supported character sets on any client will always be at least all of ISO 8859-1.

Audio: Audio should be encoded as AMR (Adaptive Multi Rate), a codec used for voice in GSM and 3G networks. Many clients will also support iMelody for ring tones.

8.3.4 MMS Interconnection, Interoperability and Roaming

Like any other service, MMS also has to meet the challenges of interoperability and roaming. Interoperability of MMS means the ability of terminals to exchange mutually acceptable messages between terminals from different vendors, or network components like MMSCs, and with WAP gateways. This includes the end-to-end exchange of formats and protocols. MMS roaming means that a subscriber can send and receive MMS messages when roaming in another network.

The main method for GPRS roaming is PLMN roaming where the home PLMN GGSN is used. The other method is ISP roaming where the visited PLMN GGSN is used. When the user is roaming, MMS messages are sent via normal packet data traffic between the home and roaming operator network. In addition to this, the roaming customer must be able to receive SMS from the home SMSC. To achieve MMS roaming, both GPRS and SMS roamings are required. Participating operators need to have a packet data roaming agreement and SMS roaming agreement in place. A roaming agreement means the technical and commercial agreement between operators on interoperability and charging. Charging includes functions like exchange of charging data, billing the subscriber, and sharing the revenue. Operators must solve the problem of handling the interconnection charge, first within one country and then globally. They both collect statistics from traffic volumes, with clearing based on statistics and agreements. In practice, there are three ways for operators to arrange MMS interconnection: using GRX (GPRS Roaming Exchange), VPN over Internet, or VPN over leased lines. Figure 8.11 depicts MMS sender roaming, whereas Figure 8.12 shows MMS receiver roaming.

OMA and 3GPP have defined three domains for multimedia messages. The first of these is the Core MM Content Domain where full interoperability is guaranteed. The second is the Standard MM Content Domain, where terminals and multimedia messages are still compliant with MMS standards but terminals have certain freedoms. The third domain is the unclassified MM Content Domain, giving full freedom to create multimedia messages.

8.3.5 MMS Device Management and Configuration

MMS services sometime require complex configuration. For example, the settings required for MMS include MMSC IP address, connection type and about 10 other parameters. Therefore,

there is a need to be able to configure the users' devices, by providing device settings over the air. The OMA device management architecture consists of two components: OMA Client Provisioning and a continuous management technology that is based on the SyncML Device Management specification. Client Provisioning is a messaging based provisioning technology that sends settings over the air to the device and configures. All the user has to do is to accept the sent settings and the device will be correctly configured and ready for use.

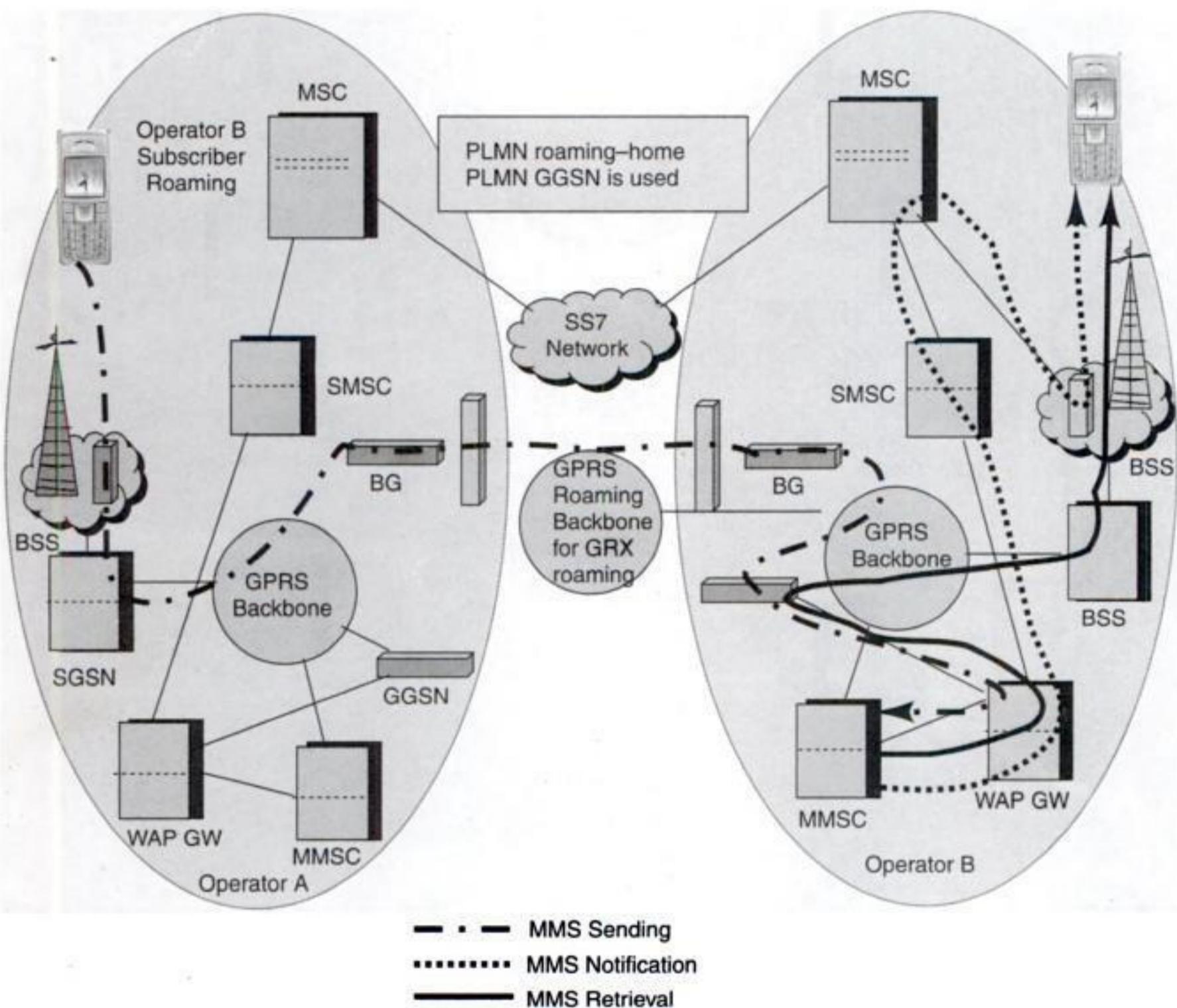


Figure 8.11 MMS Sender Roaming

8.4 GPRS APPLICATIONS

For GPRS or WAP there are no specific services. These are the same services over the wireless media that can run either on GSM or 3G. However, as GPRS offers a higher bit rate, the user



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Different base stations are identified on the downlink based on unique time offsets utilized in the spreading process. Therefore, all base stations must be tightly coupled to a common time reference. In practice, this is accomplished through the use of the Global Positioning System (GPS), a satellite broadcast system that provides information on Greenwich Mean Time and can be used to extract location information about the receiver. This common time reference is known as system time.

There are two types of PN spreading sequences used in IS-95: the long code and the short code. Both the PN sequences are clocked at 1.2288 MHz, which is the chipping rate. Two short code PN sequences are used since IS-95 employs quadrature spreading. These two codes are the in-phase sequence

$$P_I(x) = x^{15} + x^{13} + x^9 + x^8 + x^7 + x^5 + 1$$

and the quadrature sequence

$$P_Q(x) = x^{15} + x^{12} + x^{11} + x^{10} + x^6 + x^5 + x^4 + x^3 + 1$$

These two sequences are generated using 15-bit shift register sequences; although they are nominally $2^{15} - 1 = 32767$ chips, a binary '0' is inserted in each sequence after a string of 14 consecutive 0's appears in either sequence to make the final length of the spreading sequence an even 32768 chips.

The long code is given by the polynomial

$$\begin{aligned} P(x) = & x^{42} + x^{35} + x^{33} + x^{31} + x^{27} + x^{26} + x^{25} + x^{22} + x^{21} + x^{19} + x^{18} + x^{17} + x^{16} \\ & + x^{10} + x^7 + x^6 + x^5 + x^3 + x^2 + x^1 + 1 \end{aligned}$$

It is of length $2^{42} - 1$ chips as it is generated by a 42-bit shift register. It is primarily used for privacy, as each user of the mobile network may be assigned a unique temporal offset for the long code with reference to system time. Since the long code has a period of 41 1/2 days, it is nearly impossible to blindly detect a user's temporal offset. The offset is accomplished with the use of a long code mask, which is a 42-bit value that is combined with the shift.

BPSK and QPSK

The simplest form of a DSSS communications system employs coherent Binary Phase Shift Keying (BPSK) for both the data modulation and spreading modulation. But the most common form of DSSS uses BPSK for data modulation and QPSK (Quadrature Phase Shift Keyed) modulation for spreading modulation. QPSK modulation can be viewed as two independent BPSK modulations with 180 degree phase difference.

The input binary bit stream $\{d_k\}$, $d_k = 0, 1, 2, \dots$ arrives at the modulator input at a rate $1/T$ bits/sec and is separated into two data streams $d_I(t)$ and $d_Q(t)$ containing odd and even bits respectively like,

$$d_I(t) = d_0, d_2, d_4, \dots$$

$$d_Q(t) = d_1, d_3, d_5, \dots$$

QPSK can be viewed as two independent BPSK modulations. Figure 9.4 depicts an example of QPSK for a bit stream 00111000.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

is spread and everybody gets the same signal. Logically a mobile station in CDMA is always connected to different base stations at the same time. Therefore, handoff is managed by changing the attachment. There are three types of handoffs in CDMA. These are Soft handoff, Hard handoff, and Softer handoff.

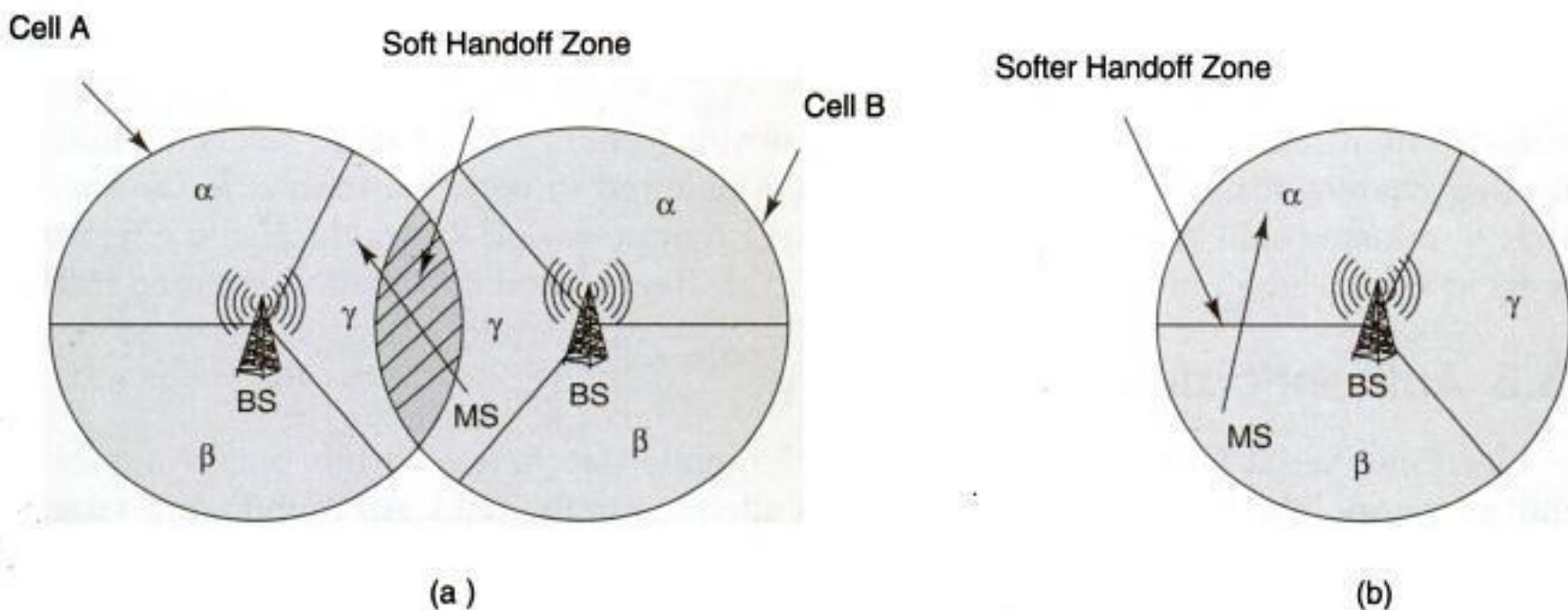


Figure 9.7 (a) Soft Handoff; (b) Softer Handoff

In CDMA a cell is divided into sectors. Like in GSM it is normally divide into three sectors each covering 120° . CDMA antennas are either Switched Beam System (SBS) or an Adaptive Antenna System (AAS). The SBS uses multiple fixed beams in a sector and a switch to select the best beam to receive a signal. In an AAS, the receiving signals by multiple antennas are weighted and combined to maximize the signal to noise ratio (SNR).

- **Soft Handoff:** This is the case of intercell handoffs (Fig. 9.7(a)). Soft handoff is a process in which the control of a mobile station is assigned to an adjacent cell or an adjacent sector (in the same frequency) without dropping the original radio link. The mobile keeps two radio links during the soft handoff process. Once the new communication link is well established, the original link is dropped. This process is also known as “make before break”, which guarantees no loss of voice during handoff. In Figure 9.7(a), as the user moves, a soft handoff takes place from Cell B to Cell A.
- **Hard Handoff:** This is the case of interfrequency handoffs. CDMA to CDMA hard handoff is the process in which a mobile is directed to handoff to a different frequency assigned to an adjacent cell or a sector. The mobile drops the original link before establishing the new link. This is similar to a GSM handover. The voice is muted momentarily during this process. This handoff is completed very fast and cannot be noticed.
- **Softer Handoff:** A mobile communicates with two sectors of the same cell (Fig. 9.7(b)). A rake receiver at the base station combines the best version of the voice frame from the diversity antennas of the two sectors into a single traffic frame. This is a logical handoff where signals from multiple sectors are combined instead of switching from one sector to another.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

REVIEW QUESTIONS

- Q1: What is Direct Sequence Spread Spectrum Technology? How does it work in CDMA technology?

Q2: Describe the IS-95 architecture. Compare its architecture with the GSM architecture.

Q3: Describe CDMA data protocol stack.

Q4: Describe different types of handoffs. What are the differences between Hard handoff, Soft handoff and Softer handoff?

Q5: Describe each of the following in brief:

 - (a) IS-95 Channel Structure
 - (b) IS-95 Call Processing
 - (c) IS-95 Channel Capacity

Q6: Give six functional differences between CDMA and GSM.

Q7: Describe 3G networks. How is a 3G network different from a 2G network?

Q8: Describe Virtual Home Environment (VHE). How is VHE realized in 3G networks?

Q9: Describe each of the following:

 - (a) UMTS
 - (b) USIM
 - (c) ENUM

Q10: What are IMT-2000 set of standards? Explain their evolution from 2G networks.

Q11: What are the characteristic features of IMT-2000?

Q12: How is IMT-2000 set of standards expected to evolve towards 4G? What all would be the necessary conditions for that?



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

10.3 IEEE 802.11 STANDARDS

The IEEE 802 committee was set up in February 1980 (that is the origin of the name) to set the standard for local area networks. From time to time, IEEE came up with different standards in the LAN domain. This includes all the layers from physical, media access, and data link layer. When IEEE deliberated the standards for WLAN, it was clear that wireless LAN will be different only at the physical and media access layer.

There were many WLAN technologies developed by researchers and industry driven by different motivations; some of them were even standardized (Table 10.1). However, WiFi or IEEE 802.11 became the most popular WLAN protocol world over. When we refer to 802.11 or IEEE 802.11, we generally mean the generic IEEE 802.11 WLAN family of standards. The 802.11 standardization originally published in 1997 with the goal to support 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared transmission. All other standards released following that were amendments to this original standard with almost all the letters from the English alphabet starting from 'a' to 'z' like IEEE 802.11a, IEEE 802.11b or IEEE 802.11z. Different standards covered different aspects of WLAN like bandwidths, modulation techniques, physical media, security, roaming etc. Table 10.2 is a list of these standards.

Table 10.1 The IEEE Wireless LAN Standards

Standard	Description	Publication
IEEE 802.11	Standard for Wireless LAN operations at data rates up to 2 Mbps in the 2.4-GHz Industrial, Scientific and Medical (ISM) band.	1997
IEEE 802.15.1	Wireless Personal Area Network standard based on the Bluetooth specification, operating at the 2.4-GHz ISM band.	2002
IEEE 802.1x	Port-based network access control defines infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics.	2001

To avoid confusion, on June 12, 2007 IEEE published the consolidated IEEE Std 802.11-2007 standard entitled "IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". This standard gives users, in one document, the entire IEEE 802.11 set of specifications for wireless local area networks with many amendments that have been published till 2007. This standard includes all amendments of a, b, d, e, g, h, i and j. Theoretically, today standards like IEEE 802.11a or IEEE 802.11g do not exist. The next consolidated standard is expected to be released in 2011 when standards like IEEE 802.11k, IEEE 802.11y and many other may be merged into IEEE Std 802.11-2011.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

The fields in the FHSS PLCP are as follows:

- SYNC.** This field is made up of alternate zeroes and ones. This bit pattern is to synchronize the clock of the receiver.
- Start Frame Delimiter.** This field indicates the beginning of the frame and the content of this field is fixed and is always 0000110010111101.
- PSDU Length Word (PLW).** This field specifies the length of the PSDU in octets.
- PLCP Signaling (PSF).** This field contains information about the data rate of the fields from whitened PSDU. The PLCP preamble is always transmitted at 1Mbps irrespective of the data rate of the wireless LAN. This field contains information about the speed of the link. For example, 0000 means 1 Mbps and 0111 signifies 4.5 Mbps bandwidth.
- Header Error Check.** This field contains the CRC (Cyclic Redundancy Check) according to CCITT CRC-16 algorithm.

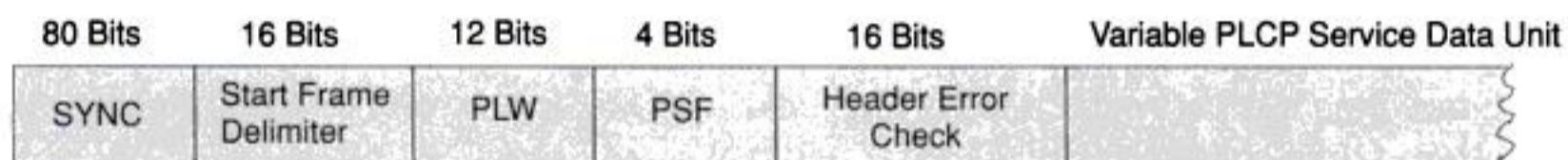


Figure 10.6 Frequency Hopping Spread Spectrum PLCP

FHSS PMD is responsible for converting the binary bit sequence into analog signal and transmit the PPDU frame into the air. FHSS PDM does this using the frequency hopping technique. The 802.11 standard defines a set of channels within the ISM band for frequency hopping. For the US and Europe there are 79 1MHz channels within 2.402 to 2.480 GHz band. The FHSS PMD transmits PPDU by hopping from channel to channel according to a particular pseudo-random hopping sequence. Once the hopping sequence is set in the access point, stations automatically synchronize to the correct hopping sequence.

Direct Sequence Spread Spectrum (DSSS) Physical Layer

DSSS PLCP is responsible for synchronizing and receiving the data bits correctly. Figure 10.7 depicts the DSSS PPDU packet.

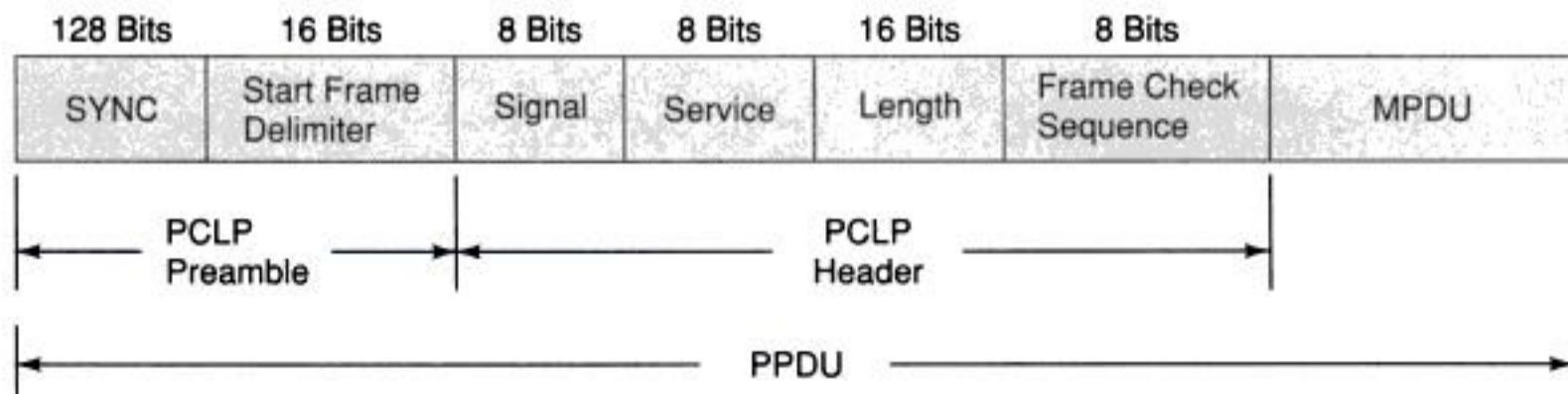


Figure 10.7 Direct Sequence Spread Spectrum PLCP Protocol Data Unit

The fields in the DSSS PLCP are as following:

- SYNC.** This field is made up of alternate zeroes and ones. This bit pattern is to synchronize the clock of the receiver with the received frame.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

The DSSS used in wireless LAN and the DSSS used in the CDMA (IS-94 or CDMA- 2000) for wireless MAN (Metropolitan Area Network) used in CDMA phones operate in similar fashion but with some difference. In wireless LAN the chip used for each and every mobile station is the same. However, in case of wireless MAN the chip used for each different mobile station (for uplink or reverse path) are different.

The MAC Layer (Layer 2) Architecture

The MAC Layer defines two different access methods, the Distributed Coordination Function and the Point Coordination Function:

The Basic Access Method: CSMA/CA

The basic access mechanism, called the Distributed Coordination Function by IEEE standard, is Carrier Sense Multiple Access with Collision Avoidance mechanism (CSMA/CA). CSMA protocols are well known in the industry, the most popular being the Ethernet, which is a CSMA/CD protocol (CD stands for Collision Detection). In a wired environment (Ethernet for example) every station connected to the wire can sense the signal in the wire. In a wired LAN, if there is no activity or a collision of messages, every station connected to the LAN will be able to sense the collection almost instantly. This is not true in the case of wireless media. In the case of wireless LANs, a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol is used, as it is not possible to detect a collision of data packets in mid air.

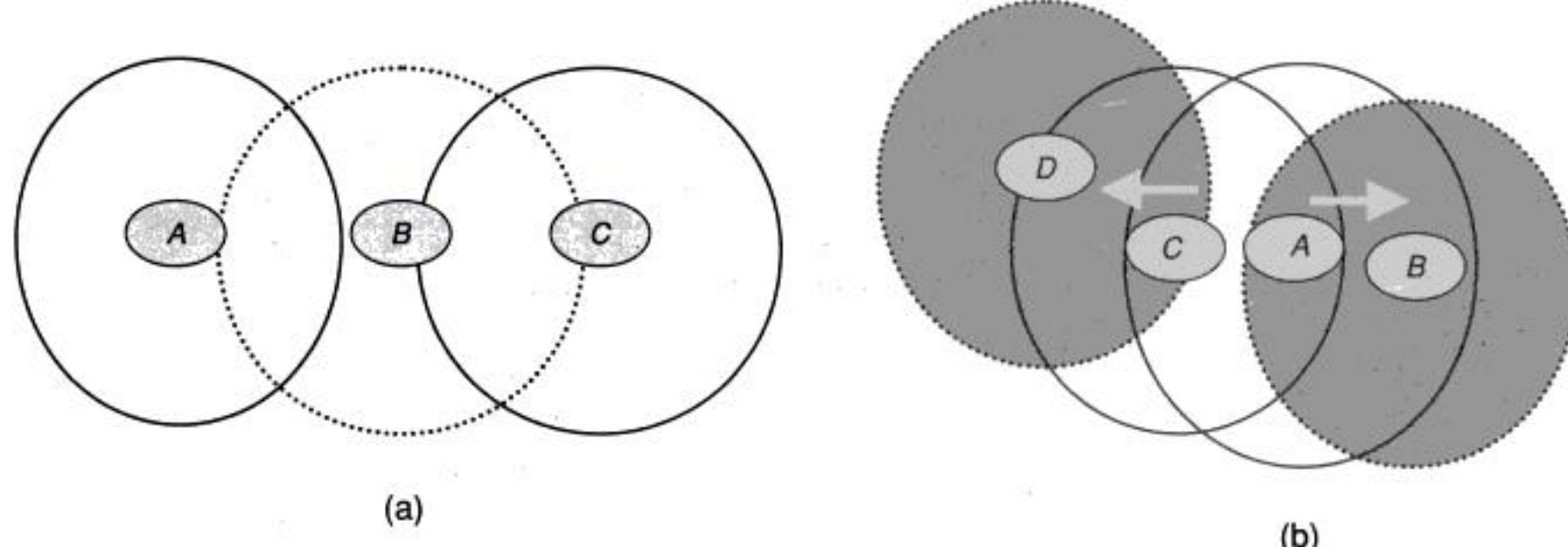


Figure 10.9 (a) Hidden Terminal; (b) Exposed Terminal

Consider the scenario with three mobile nodes as shown in Figure 10.9(a). The transmission of *A* reaches *B*, but not *C*. The transmission of *C* reaches *B*, but not *A*. However, the radio signal of *B* reaches both *A* and *C* making *A* and *C* both in the range of *B*. The net effect is *A* cannot detect *C* and vice versa.

A starts sending to *B*; *C* does not receive this transmission. *C* also wants to send to *B* and senses the medium. To *C* the medium appears to be free. Thus *C* starts sending causing collision at *B*. But now *A* cannot detect the collision and continues with its transmission. *A* is “hidden” for *C* and vice versa.

Consider another case as shown in Figure 10.9(b). The radio transmission signal of *A* reaches *C* and *B*. The radio signal of *C* reaches both *A* and *D*. *A* wants to communicate to *B*, *A* starts sending signals to *B*. *C* wants to communicate with *D*, *C* senses the carrier and finds that *A* is talking to *B*. *C* has to wait till the time *A* finishes with *B*. However, *D* is outside the range of *A*, therefore waiting is not necessary. In fact *A*, *B* and *C*, *D* can communicate with each other in parallel without any collision, but according to the protocol that is not possible. *A* and *C* are “exposed” terminals.

While Collision Detection mechanisms are a good idea on a wired LAN, they cannot be used on a Wireless LAN environment for two main reasons:

- Implementing a Collision Detection mechanism requires the implementation of a Full Duplex radio capable of transmitting and receiving at the same time. This increases the cost significantly.
- In a wireless environment we cannot assume that all stations will be able to receive radio signals from each other (which is the basic assumption of the Collision Detection scheme). The fact that a station wants to transmit and senses the medium as free (not able to sense signal from another station) does not necessarily mean that the medium is free (like the case of the hidden terminal) around the receiver area.

The mechanism behind CSMA/CA is as follows:

- When a wireless station (a wireless LAN device) wants to communicate, it first listens to its media (radio spectrum) to check if it can sense radio waves from any other wireless station.
- If the medium is free for a specified time then the station is allowed to transmit. This time interval is called Distributed Inter Frame Space (DIFS).
- If the current device senses a carrier signal of another wireless device on the same frequency, as it wants to transmit on, it backs off (does not transmit) and initiates a random timeout.
- After the timeout has expired, the wireless station again listens to the radio spectrum and if it still senses another wireless station transmitting, it continues to initiate random timeouts until it does not detect or sense another wireless station transmitting on the same frequency.
- When it does not sense another wireless station transmitting, the current wireless station starts transmitting its own carrier signal to communicate with the other wireless station, and once synchronized, transmits the data.
- The receiving station checks the CRC of the received packet and sends an acknowledgment packet (ACK). Receipt of the acknowledgment indicates to the transmitter that no collision occurred. If the sender does not receive the acknowledgment then it retransmits the fragment until it receives acknowledgment or is abandoned after a given number of retransmissions.

It can be seen from the above that the more times a wireless station has to back off or go into a random timeout, the less opportunity it has to transmit its data. This reduced opportunity for data transmission leads to less effective access to wireless bandwidth. This reduces the speed of the operation. In a worse case scenario the system would, after a number of retries, completely timeout and the wireless connection would be lost.

Virtual Carrier Sense

In order to reduce the probability of two stations colliding because they cannot sense each other's presence, the standard defines a Virtual Carrier Sense mechanism: A station wanting to transmit a packet first transmits a short control packet called RTS (Request To Send), which includes the source, destination, and the duration of the following transaction (the data packet and the respective



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

In a majority of cases, the wireless LAN uses standard Ethernet LAN as the backbone. Therefore, it is necessary that wireless LAN is able to handle Ethernet packets of 1518 bytes long. Also, any change in the protocol for wireless LAN may cause a major change in the protocol of the higher layers. Therefore, the IEEE committee decided to solve the problem by adding a simple fragmentation/reassembly mechanism at the MAC Layer of the wireless LAN. The mechanism is a simple Send-and-Wait algorithm, where the transmitting station is not allowed to transmit a new fragment until one of the following conditions happens:

1. Receives an ACK for the said fragment, or
2. Decides that the fragment was retransmitted too many times and drops the whole frame.

It should be noted that the standard does allow the station to transmit to a different address between retransmissions of a given fragment. This is particularly useful when an AP has several outstanding packets to different destinations and one of them does not respond. Figure 10.11 shows a frame (MSDU) being divided to several fragments (MPDUs).

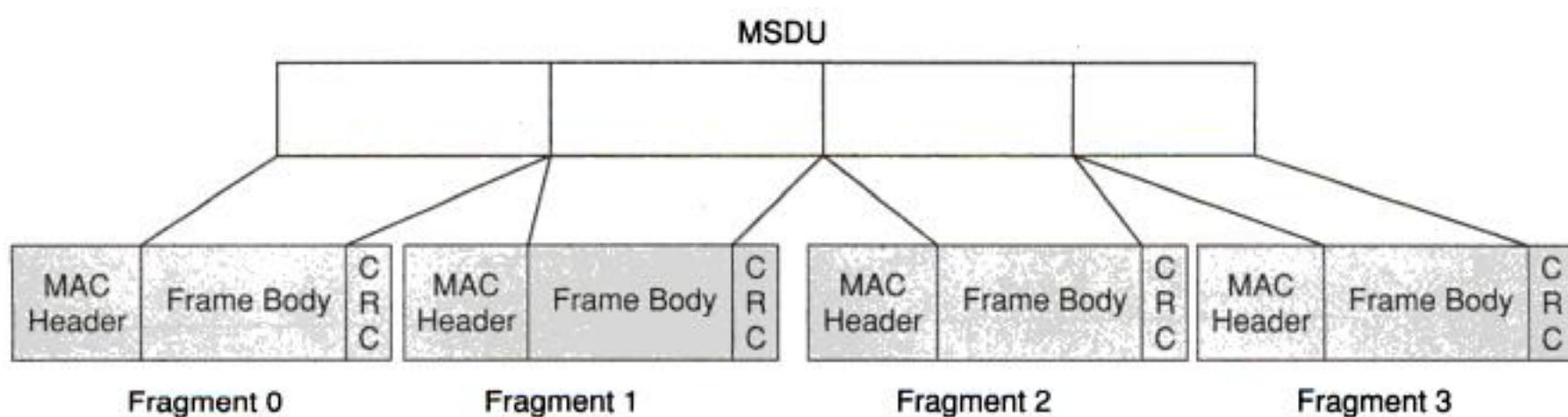


Figure 10.11 Frame Fragmentation

Inter Frame Spaces

The standard defines four types of spacing intervals. These are called Inter Frame Spaces (IFS). IFSs are used to defer a station's access to the medium and provide various levels of priorities:

- **SIFS (Short Inter Frame Space)**, is the shortest Inter Frame Space with the highest priority. RTS, CTS use SIFS intervals. SIFS value is a fixed value per PHY and is calculated in such a way that the transmitting station will be able to switch back to receive mode and be capable of decoding the incoming packet.
- **PIFS (Point Coordination IFS)**, is used by the Access Point (or Point Coordinator), to gain access to the medium before any other station. This value of PIFS is SIFS plus a Slot Time, i.e., 78 microseconds.
- **DIFS (Distributed IFS)**, is the Inter Frame Space used for a station willing to start a new transmission, which is calculated as PIFS plus one slot time, i.e., 128 microseconds.
- **EIFS (Extended IFS)**, is a longer IFS used by a station that has received a packet that it could not understand. This is needed to prevent the station (which could not understand the duration information for the Virtual Carrier Sense) from colliding with a future packet belonging to the current dialog.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

direct a message addressed to Mumbai to a west-leading link than to an east-leading link. STP routing decisions are based on geography, distance, congestion, and least cost criteria. Once a SS7 message is delivered from a source to destination, a circuit on the same path is reserved for traffic. For fault tolerance, STPs are always installed in pairs with cross connections.

The SSP (Service Switching Point)

Service Switching Point is a switch in the SS7 network that can handle call set-up. The SSP has the ability to stop call processing, make queries to even unknown databases, and perform actions appropriate to the response. SSP is equipped with all the intelligence required to handle numerous feature capabilities. Example of a SSP will be a MSC in a cellular network. There is another switching point called a CCSSO (Common Channel Signaling Switching Office). These are end or tandem offices which have the capability to use the SS7 in what is referred to as a trunk signaling mode for call set-up. CCSSO is a limited version of the SSP.

The SCP (Service Control Point)

One of the first purely digital uses for the SS7 network was to provide a service to translate from one form of data to another. For example, switches need to maintain tables to translate dialed digits into routing information consistent with the international numbering system (for example iitb number +91808410628). It is that plan that breaks India (country code 91) down into city code (80), exchange code (841), and finally to the line (0628) serving individual telephone. Let us take another example where a person has moved his home from one part of the town to another. When we dial the telephone number, it plays a recorded message like "The number you have dialed is 28670203, the number has changed to 25320203. You may dial the new number or wait for a while to be connected automatically."

When a virtual number like 1-800 in India is dialed, there is no way for the switch to determine how to route this call. This is because such prefixes have no reference to the international numbering plan. In fact, a 1-800 number dialed in Mangalore may be connected to a number in Bangalore, while the same number dialed in Pune may result in a connection to Mumbai. When that translation is returned to the switch, the number can be connected exactly as it would have been if it had been dialed in the first place. This database is located at an SS7 address called Signaling Point Code. SCPs are used for a variety of applications such as Calling Card verification, toll-free calls, tele-voting, premium tariff (1-900) calls, etc. Such intelligent nodes make the network intelligent. This also frees the switch from trying to maintain ever larger routing tables, and enables the use of a broad range of services which depend on translations or digital data services of a variety of types.

SCP provides the access mechanism required for a service. These services may reside in the same location as the SCP or the SCP may serve as a "front end" for services located elsewhere. In either case the SCP controls many services. To identify a service in a SS7 network, two parameters are required. These are SCP address and the service within the SCP.

CRP (Customer Routing Point)

The CRP provides on-premises control of the routing information requested by switches for translation of 800 type dialing. The operator of the CRP is a customer who requires rapid update and control of the translation of their own numbers.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

fields (SIF). The functionality of the MSU is defined through service indicator octet (SIO) and the service information fields (SIF). The SIO is an 8-bit field that contains three types of information: 4 bits to indicate service indicator (0—signaling network management; 1—signaling network testing and maintenance; 2—SCCP; 3—ISUP), 2 bits to indicate national (proprietary within a country) or international (ITU standard) message; remaining 2 bits to indicate priority with 3 being the highest priority. The service information field (SIF) defines the information necessary for routing and decoding of the message. SIF transfers control information and the routing label used in MTP Level 3. The routing label consists of the destination point code (DPC), originating point code (OPC) and signaling link selection (SLS) fields.

The common fields in all the signal units are as follows:

Flag: This contains a fixed pattern 0111110 and is used for clock synchronization

BSN: Backward Sequence number.

BIB: Backward indicator bit.

FSN: Forward Sequence number.

FIB: Forward indicator bit.

Length indicator: Out of 8 bits only 6 bits are used to indicate the length.

11.5 IN CONCEPTUAL MODEL (INCM)

INCM was developed to provide a framework for the design and description of each capability set and the target IN architecture. In an IN scenario there are four main actors. The first, the service user, is the end-user of the service. For example, this is the person who calls a free-phone or utilizes his calling card to call a friend while he is roaming. The second, the service subscriber, is the actor who subscribes to an IN feature. He can use it for himself or provide it to his customers. This could be an individual, a corporation, or a virtual service provider. The third, the service provider creates, deploys and supports IN services. This actor has contracts with service subscribers. These contracts specify the billing and the subscribed features. The fourth and last one is the network operator. This actor provides the infrastructure needed to support IN services. This actor has contracts with service providers. INCM captures the whole engineering process of the IN.

The INCM is structured into four planes (Fig. 11.6) as follows:

- Service plane.
- Global functional plane.
- Distributed functional plane.
- Physical plane.

The upper two planes focus on service creation and implementation, whereas the lower two planes address the network and physical needs.

Service Plane (SP)

This plane is of primary interest to service users and providers. It describes services and service features from a user perspective, and is not concerned with how the services are implemented within the network.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

A PDA as the name suggests is a personal digital assistant. Its major functionality is related to storing, accessing and manipulating data. None other than the team of Star Trek conceived the idea of PDA in the early 1960s. But till the later half of the 1980s this remained mostly a concept. Apple demonstrated the first device. This device was the Newton. Figure 12.3 shows the evolution of the PDA.

From a stand-alone organizer the PDA has come a long way. Most of this significant evolution is due to the progress in hardware capabilities and development of underlying bearer networks. We now take a look at the current offerings. Most handheld devices can be classified as smart phones, PocketPCs or smart communicators (a combination of the two). Figure 12.4 gives the features based on which this classification is made. However, note that the lines dividing these kinds of devices are greatly blurred and it may be difficult to identify each of them in the future.

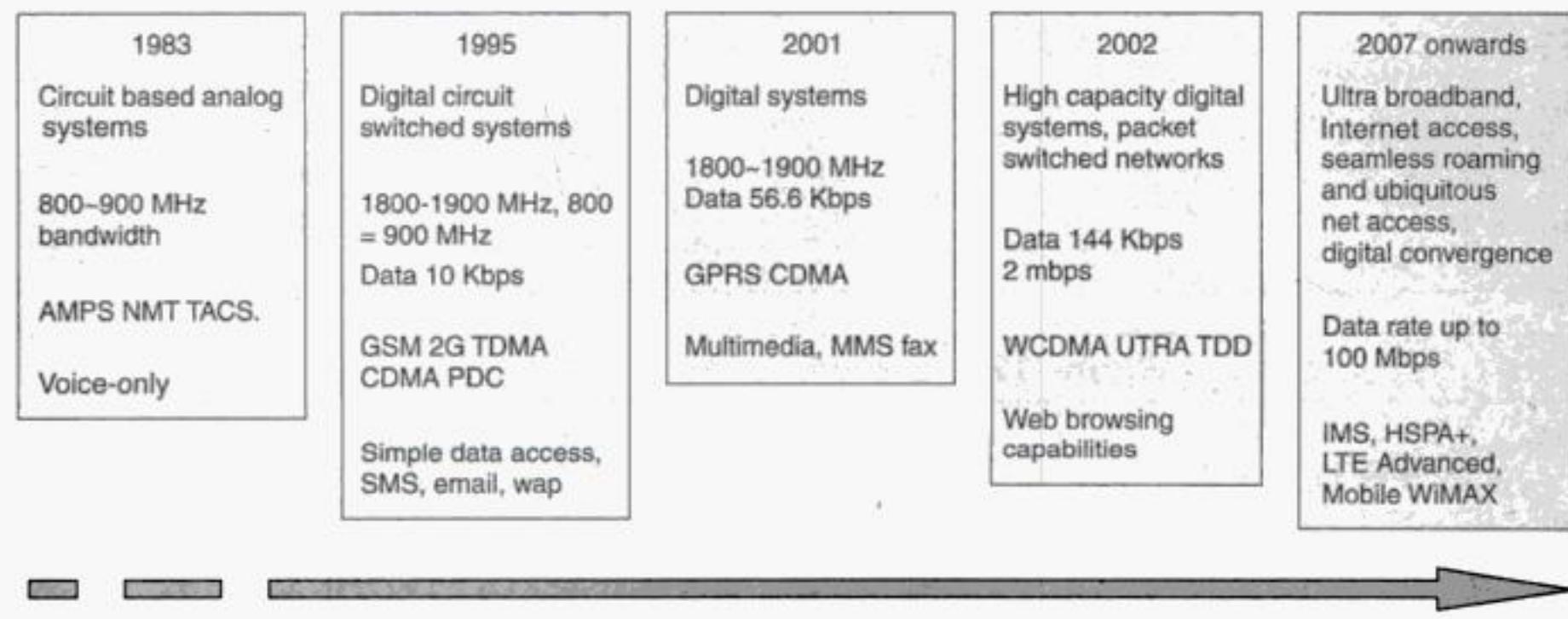


Figure 12.2 Evolution of Cellular Technology

Time	1970s–1987	1988–1992	1993	1994–1996	1997–1999	2000–2005	2005 onwards
Devices	Pison Organizer	Grid Pad, Atari, Sharp	Message Pad, Zoomer, PenPad, Envoy	Palm, Marco, MagicLinc	Sharp, Palm VII	Nokia 9210, iPaq	Nokia E72, Nokia N97, Nokia N 900, Blackberry, Treo Pro, i-mate ULTIMATE 8502
Key features	Stand alone data organizer	Handwriting recognition	Telephony application	Synchronization	Wireless link	Personal organizer cum wireless data communicator	Could run almost all desktop applications while being connected to Internet 24 x 7; Great multimedia capabilities

Figure 12.3 Evolution of PDA



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

founding father Jeff Hawkins carried a block of wood to every meeting to take a practical approach that the user should learn the hieroglyphics of graffiti rather than putting together software that understands all nuances of human handwriting. These were based on learnings from costly mistakes made earlier and feedback from customers of an earlier product Zoomer. The Palm was designed with three commandments:

- Handwriting recognition to be limited to simplified hieroglyphics.
- Size should be small enough to fit into the pocket.
- A cradle to synchronize data with a PC.

The result was a blueprint of what the PDA should be. But by 1994, successive debacles in the PDA market ensured that financers for the project were scarce. The lucky break came in the form of U.S. Robotics which lent its might to Palm. The prototype, till then known as touchdown was christened PalmPilot 1000 and officially released in February 1996. Within the year they sold an unprecedented 350 thousand units. The volumes were growing and the tempo was built. At the same time certain management changes were happening, U.S. Robotics was acquired by 3Com in 1997. The next milestone was March 1998 when the fruits of investment and innovation saw PalmPilot III being released by 3Com. The device had double the RAM, supported infrared connections, had a better character recognition algorithm, more fonts, a handy cradle, an improved Palm OS 3.0 and stylish design. But much of it was only filling up the gaps in the earlier products. By then competition was also born in the form of WinCE still in its infancy.

At the dawn of the fateful year of 1999, everything was great; sales was at its peak, employees were motivated and competition non-existent. Trouble, however, was afoot; foresight was slow in coming. Two new models—the PalmV and PalmVII that were minor variations of the PalmIII were released but failed to make a mark. The founding parents of Palm Computing, Jeff Hawkins and Donna Dubinsky, parted ways with 3Com to set up a competitor, namely, Handspring. By September they came out with Visor. The year 2000 was quite uneventful except for the release of WinCE 3.0. The curtains, however, had come down the golden age of Palm. The year 2001 saw both Palm and Handspring slowly rolling downhill. A global market recession leading to very low demand and fierce competition both within and without, saw the blue-eyed boy of the industry getting into trouble. Some good things too happened: new high-end models m500, m505 and m515, were released, these support for Secure Digital flash cards, a new version of operating system (Palm OS 4.0), new batteries with longer life and even a color display. The company was split giving birth to two divisions, one working on and licensing the Palm OS called PalmSource and the other manufacturing Palm devices called palmOne. The acquisition of Be, marked the move from dragonball processor to a more advanced ARM core based one. On the whole, though things were not rosy; the PDA market at the close of 2001 was clearly in favor for Palm Computing and its allies.

The year 2002 saw the effort to counter this downslide with the release of wireless capable devices like i705 and Treo series from Handspring. A series of belt-tightening measures both technically and financially in the previous year yielded some bright moments. They also had to counter a patent infringement suite from Xerox on the graffiti. This led to the licensing and adoption of jot. But now there was a need for a keyboard for applications like e-mail leading to more licensing from Blackberry Rim. On the downslide was the release of PocketPC 2002 which already enjoyed substantial support from the elite corporate and of course the global reduction of the PDA market.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Symbian OS uses page memory architecture. It implements a two-level page table using 4 KB pages. This allows for efficient memory usage.

Owing to the multi-tasking capability of the OS, security becomes an important consideration. Symbian OS addresses security concerns in two ways. First, by using privileged and non-privileged mode execution it takes care of restricting access to kernel and hardware access. Second, it requires all applications to run in a virtual machine (VM) thereby protecting the applications from each other. Each application executes as a single process. (A single process is likely to have multiple threads). At launch or initialization, the application is allocated memory for its data; the outer page table stores a reference to this. When a context switch causes this process to be activated, all the pages are moved to a pre-defined location in the virtual memory map, hence execution continues in the appropriate thread. Applications cannot make direct calls to the call to hardware drivers; they have to use user library APIs which in turn use system services through the kernel.

As mentioned earlier the primary concern of the MMU is to provide a protected mode system. Other functions of the MMU include

- Restriction on access to process data.
- Protection of application and OS code.
- Isolation of the peripheral hardware.

More information on the MMU and CPU architecture can be found at the Symbian site.

All handsets have limited runtime memory. Out of memory exceptions are quite likely. One way that Symbian uses to counter this is by having a clean-up stack, all partially constructed objects are placed here until their construction has been completed. If the phone does not have sufficient memory to complete object creation then it simply deletes the contents of this stack. By not allowing partially constructed objects it avoids memory leaks as well as protects applications from potential data loss.

14.2.3 System Software

All applications require system services of one type or the other. The Symbian OS System services framework operates in a client server mode where in most of the system services are provided as servers for example a file server, font and bitmap server, a media server etc. An application is a client that connects to these servers and requests their services. The client connects to the server using the kernel interfaces and uses a message passing mechanism for interaction. The server however runs in an unprivileged mode and will use other backend device drivers or kernel extensions to perform its tasks. From an application perspective we need to concentrate on the user library. The user library provides APIs to application framework and controlled access to the kernel. We will see the different frameworks and the applicable APIs as we proceed.

14.3 APPLICATIONS FOR SYMBIAN

The open architecture of Symbian enables Independent Software Vendors (ISVs) to focus on developing new applications for mobile phones. Third-party vendors provide software in the form of an installation (SIS) file. This file contains the libraries and resources of the application, secured by a certification system. This mechanism ensures a secure application where the vendor is identified



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

- recordAdded(): When a new record is added to the record store.
- recordDeleted(): When a record in the record store is deleted.
- recordChanged(): When a record in the store has been updated.

Any application that wants to listen to the RecordListener has to implement the RecordListener interface and override the three functions above. The next step is to associate listener with the object. The sample implementation just shows the methods and a simple print statement for the function activated. We have already seen the output from these methods above.

```

public void recordAdded(RecordStore recordStore, int recordId)
{
    try
    {
        System.out.println("MSG From RecordListener: Record
                           added " + "Store Name \\" " + recordStore.getName( ) + "\"
                           ID " + recordId + " Value " + getRecord(recordId) );
    } catch (RecordStoreNotOpenException e)
    {
        e.printStackTrace( );
    }
}

public void recordChanged(RecordStore recordStore, int
recordId)
{
    try
    {
        System.out.println("MSG From RecordListener: Record
                           changed " + "Store Name \\" "+ recordStore.getName( ) +
                           "\\" ID " + recordId + " Value " + getRecord
                           (recordId));
    } catch (RecordStoreNotOpenException e)
    {
        e.printStackTrace( );
    }
}

public void recordDeleted(RecordStore recordStore, int
recordId)
{
    try
    {
        System.out.println("MSG From RecordListener: Record
                           deleted " + "Store Name \\" " + recordStore.getName( )
                           + "\\" ID " + recordId + " Value " + getRecord
                           (recordId));
    } catch (RecordStoreNotOpenException e)
    {
}
}

```



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

<i>JSR #</i>	<i>Name of JSR</i>	<i>Description</i>
190	Event Tracking API for J2ME	This defines an optional code package that standardizes application event tracking on a mobile device and the submission of these event records to an event-tracking server via a standard protocol.
195	Information Module Profile	This JSR will define J2ME profile targeting embedded networked devices that wish to support a Java runtime environment, but do not have graphical display capabilities.
201	Extending the Java Programming Language with Enumerations, Autoboxing, Enhanced for loops and Static Import	This JSR proposes four new Java programming language features: enumerations, autoboxing, enhanced for loops and static import.
205	Wireless Messaging API 2.0	This JSR will extend and enhance the “Wireless Messaging API” (JSR-000120).
209	Advanced Graphics and User Interface Optional Package for the J2ME Platform	The Advanced Graphics and User Interface (AGUI) Optional Package will migrate the core APIs for advanced graphics and user interface facilities from the J2SE platform to the J2ME platform.
211	Content Handler API	Enabling J2ME applications to handle multi-media and web content can give developers and users a seamless and integrated user environment on mobile phones and wireless devices.
213	Micro WSCI Framework for J2ME	Effort to define another layer of the J2ME Web Service stack, implementing the “observable” behavior of a choreographed Web Service on the device, relative to the message exchange requiring support.
214	Micro BPSS for J2ME Devices	This JSR is to provide a standard set of APIs for J2ME Devices for representing and manipulating Collaboration Profile and Agreement information described by ebXML CPP/A (Collaboration Protocol Profile/Agreement) documents.
216	Personal Profile 1.1	This JSR will update the existing Personal Profile (JSR-62 specification to reflect the J2SE 1.4 APIs).
217	Personal Basis Profile 1.1	This JSR will update the existing Personal Basis Profile (JSR-129) specification to reflect the J2SE 1.4 APIs.

(Contd)

<i>JSR #</i>	<i>Name of JSR</i>	<i>Description</i>
218	Connected Device Configuration (CDC) 1.1	This JSR defines a revision to the J2ME CDC specification. This JSR provides updates (based on J2SE, v1.4) to the existing core, non-graphical Java APIs for small electronic devices.
219	Foundation Profile 1.1	This JSR defines a revision to the J2ME Foundation Profile. This JSR provides updates (based on J2SE, v1.4) to the existing core, non-graphical Java APIs for small electronic devices.
226	Scalable 2D Vector Graphics API for J2METM	This specification will define an optional package API for rendering scalable 2D vector graphics, including image files in W3C Scalable Vector Graphics (SVG) format.
228	Information Module Profile-Next Generation (IMP-NG)	This specification will define a profile that will extend and enhance the "J2ME Information Module Profile" (JSR-195).
229	Payment API	Enabling application developers to initiate mobile payment transactions in J2ME applications.
230	Data Sync API	Enabling J2ME applications to access native data synchronization implementation.
232	Mobile Operational Management	Create a predictable management environment for mobile devices capable of installing, executing, profiling, updating, and removing Java and associated native components in the J2ME Connected Device Configuration.
234	Advanced Multimedia Supplements	This specification will define an optional package for advanced multimedia functionality which is targeted to run as an supplement in connection with MMAPI (JSR-135) in J2ME/CLDC environment.
238	Mobile Internationalization API	This JSR defines an API that provides culturally correct data formatting, sorting of text strings and application resource processing for J2ME MIDlets running in MIDP over CLDC.
239	JavaTM Binding for the OpenGL® ES API	Java bindings to the OpenGL ES (Embedded Subset) native 3D graphics.
242	Digital Set Top Box Profile-“On Ramp to OCAP”	The requested specification will define a J2ME profile based on the Connected Limited Device Configuration (CLDC) that is appropriate for use by small-footprint cable television set-top boxes.

(Contd)



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

the hardware of the device. It facilitates communication between the operating system (OS) and the target device and includes code to handle interrupts, timers, generic IOCTLs (I/O control codes), etc. Physically, the OAL is linked with the kernel libraries to create the kernel executable file.

In any device we have a layer of software called device drivers. This is no different in the case of Windows CE. In Windows CE, different hardwares interact with the kernel through respective device drivers.

The boot loader is a piece of software that is required to boot the device. The boot loader generally resides in non-volatile storage on the device. It is executed at system power-on/reset (POR). To get the boot loader on the target device for the first time, some special program is used. However, updates of boot loaders are handled by boot loader itself flash the new OS images. The platform initialization code for the device is shared between the boot loader and the OAL. The boot loader provides a menu that allows the user to set different configuration options, such as DHCP or static IP information. These configuration parameters are stored in a configuration file.

16.3.2 Operating System Layer

The operating system layer contains all the software supplied by Microsoft as a part of the operating system. The main component in this layer is the kernel. Along with the kernel, this layer includes functions like Applications and Services Development, Core DLL, Object Store, Multimedia Technologies, Graphics Windowing and Event System (GWES), Device Manager, Communication Service and Networking. Several of these modules are divided into components. Components help Windows CE to become very compact (less than 200 KB of ROM), using only the minimum ROM, and RAM. These are explained in the following sections.

Kernel

The kernel is the core of the OS, and is represented by the Coredll.dll module. It provides the base operating system functionality that is common to all devices. Like any other operating system, Windows CE kernel is responsible for memory management, process management, and certain required file management functions. It manages virtual memory, scheduling, multitasking, multithreading and exception handling. There are some optional kernel components that are needed to include features like telephony, multimedia and graphics device interface (GDI).

Windows CE maps the bottom section of memory into 33, 32 Mb slices called "slots". The lowest slot is used for the currently running process (the process at slot 0), and other low slots are used for system processes as:

- Slot 0: current running process
- Slot 1: kernel (NK.EXE)
- Slot 2: File system – object store, registry, CeDB etc. (Filesys.exe)
- Slot 3: Device manager (Device.exe)
- Slot 4: Windows CE shell (Shell32.exe).

Five slots are used, leaving 28 remaining slots for user processes.

Being a 32-bit machine, the Windows CE address space is 4GB. The top 2GB address space is used by the operating system, which includes hardware, object store and ROM. The bottom 2GB address space is used for processes and application shared space.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

based APIs, allowing developers to readily implement communications capability in their applications. In many cases, existing code from other flavors of Windows CE can be used with little or no modification.

Serial I/O

Serial I/O is the most fundamental feature of the Windows CE communications model and is available virtually for all devices. The serial communication would be accessed via a cable or through the IR transceiver. A cable connection is handled with the standard API for serial and file system functions. They can be used to open, close, and manipulate COM ports and read from and write to them. The IR transceiver is also assigned a COM port. Therefore, direct serial I/O is available on an IrDA port using the usual serial communications functions.

Networking and Communication Support

Networking support includes primarily the socket programming interface. This includes different APIs and application interfaces to user programs along with WinSock for normal sockets and IrSock for infrared sockets.

- **WinSock and IrSock:** WinSock is the socket implementation for the standard TCP/IP. IrSock is an extension of WinSock implementation over the IrDA interface. The Windows CE TCP/IP stack is designed quite efficiently so that it can be configured to effectively support WiFi wireless networking. Windows CE also supports Secure Sockets Layer 2.0, 3.0 and PCT1.0 security protocols. IrSock enables socket-based communication via an infrared transceiver. It is designed to support the industry-standard IrDA protocols. Applications implement IrSock in much the same way as conventional WinSock, although some of the functions are used somewhat differently.
- **Browser support (WinINET API):** Windows CE supports subsets of the WinINET and Wnet APIs, and an SMB (Service Message Block) redirector. The WinINET API provides support for Internet browsing protocols, including FTP and HTTP 1.0. Only one proxy is supported, and there is no caching. It also provides access to two Internet security protocols, Secure Sockets Layer (SSL), and Private Communication Technology (PCT).
- **Remote file access (Wnet API):** The Wnet API provides access to an SMB redirector for remote file access. Currently only Microsoft Windows 95 and Windows NT operating system connections are supported.

Remote Access and Networking

This includes remote access where the Windows CE device is a client.

- **Windows CE supports a remote access services (RAS) client.** RAS is multi-protocol router used to connect remote devices. The Windows CE RAS client supports one point-to-point connection at a time.
- **NDIS 4.0 for local area networking:** For local area networks (LANs), Windows CE includes an implementation of NDIS 4.0. At present, only Ethernet miniport drivers are supported. Wide area networks (WANs) are not supported.
- **Windows CE-based devices will connect to their network via a serial communications link,** such as a modem. To support this type of networking, Windows CE implements the widely used Serial Line Interface (SLIP), and point to point (PPP) protocols. Authentication is provided



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

CHAPTER 17

Voice Over Internet Protocol and Convergence

17.1 VOICE OVER IP

Traditionally, for decades circuit-switched technologies were in use for voice communications. In a circuit-switched technology, a channel (a timeslot in Time Division Multiplexing, a frequency in Frequency Division Multiplexing, or a space in Space Division Multiplexing, etc.), is reserved to establish an end-to-end circuit. The channel is reserved for the connection, and users pay for the entire length of the circuit (in space and time) irrespective of the fact whether they are talking or thinking. The circuit could carry voice traffic, which could be either a digitized or analog voice. While circuit-switching provides good voice quality, it may not be efficient in channel utilization. In contrast, packet-switched networks carry data in packets from multiple sources and destinations over one channel. Such networks are better in channel utilization but suffer from delays and jitters. For real-time traffic like voice, delays and jitters are not nice qualities. IP (Internet Protocol) is one such packet-switched network protocol which is efficient for data communication but not suited for real-time voice.

In 1995 some lobbyists in Israel made an attempt to send voice over IP network between two PCs. Later in the same year, Vocaltec, Inc. released Internet Phone Software. By 1998 few companies started setting up gateways to allow PC-to-Phone and later Phone-to-Phone (over private corporate IP networks) connections. Technology to enable such voice communication over the IP network became known as Voice over Internet Protocol or VoIP in short. By 2000, VoIP traffic exceeded 3% of voice traffic. Most of these VoIP technologies were proprietary and did not interoperate. To ensure interoperability between protocols and equipment from different vendors, standards started emerging. These standards were from two major camps, viz., the telecommunication camp and the data camp. Today there are two sets of standards for VoIP switching, media, and gateways. These are H.323 from ITU (International Telecommunications Union) and SIP (Session Initiation Protocol) from IETF (Internet Engineering task Force). Figure 17.1 depicts the H.323, SIP and MGCP (Media Gateway Control Protocol) and connection among them.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

- User location: Determination of the location and end systems to be used for communication.
- User capabilities: Determination of the media and media parameters to be used for the communication.
- User availability: Determination of the called parties' willingness to engage in communication.
- Call setup: "Ringing," establishing call parameters at both calling and called party.
- Call handling: Managing the transfer of data (voice).
- Call teardown: Terminating the call and releasing all resources.

Figure 17.4 depicts the VoIP architecture with respect to SIP. In such a VoIP setup, the end-user device can be either an IP phone or a computer in an IP network. The conversation can be IP-to-IP, PSTN-to-IP, IP-to-PSTN. In a SIP environment along with the endpoint devices, five entities are required. These are:

- Proxy server
- Registrar server
- Redirect server
- Location server
- Gateways

We describe the functions of these entities and the mode of communications in the following sections.

17.3.1 Proxy Server

According to the SIP standard (RFC3261), "SIP proxies are elements that route SIP requests to user agent servers (UAS) and SIP responses to user agent clients (UAC). A request may traverse several proxies on its way to a UAS. Each will make routing decisions, modifying the request before forwarding it to the next element. Responses will route through the same set of proxies traversed by the request in the reverse order." In the SIP context, UAC is the endpoint initiating a call and UAS is the endpoint receiving the call.

SIP proxies function similar to routers and make routing decisions, modifying the request before forwarding it to the next element. SIP standard make provision for proxies to perform actions such as validate requests, authenticate users, resolve addresses, fork requests, cancel pending calls. The versatility of SIP proxies allows the operator to use proxies for different purposes and in different locations in the network. Proxies could be deployed as edge proxy, core proxy or even enterprise proxy. This versatility also allows for the creation of a variety of proxy policies and services, such as routing calls on various intelligent rules. The 3GPP IMS architecture (Section 17.9) for example, uses proxies known as Call State Control Functions of different kinds for various purposes.

17.3.2 Registrar Server

The Registrar server in a VoIP network can be defined as the server maintaining the whereabouts of a domain. It accepts REGISTER requests from nodes in the VoIP network. It places the information it receives as a part of those requests into the location service for the domain it handles. REGISTER requests are generated by clients in order to create or remove a mapping



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Support for Internetworking: Although, the connection to Internet shall be packet switching based connection, IMS aims to connect to circuit switched networks too. This is because there still exist important circuit switched networks like PSTN networks.

Support for service control: IMS aims to empower operators with effective service control mechanisms. Such mechanisms shall be applicable not only generally (that is, to all users) but also specifically (that is, to a specific user). Such application of service control shall be directly dependent on usage terms of subscribers.

19.4 ARCHITECTURE OF IMS NETWORKS

IMS considers the networking infrastructure by dividing it logically into separate group of functions with standard interfaces between them. Such interfaces are known as “reference points” in the context of IMS networks. Thus, as was mentioned earlier, IMS aims to standardize service developing capabilities than services. There are many interfaces in IMS networks and each defines both the protocol over the interface and the functions between which it operates. However, standards do not dictate what functions should be correlated or how should the functions be grouped into networks nodes. This feature provides enough independence to operators/applications with respect to scalability, requirements and flexibility.

3GPP specifications split the IMS architecture logically into three planes: Application or Service Plane, Control or Signaling Plane, and Transport or User Plane.

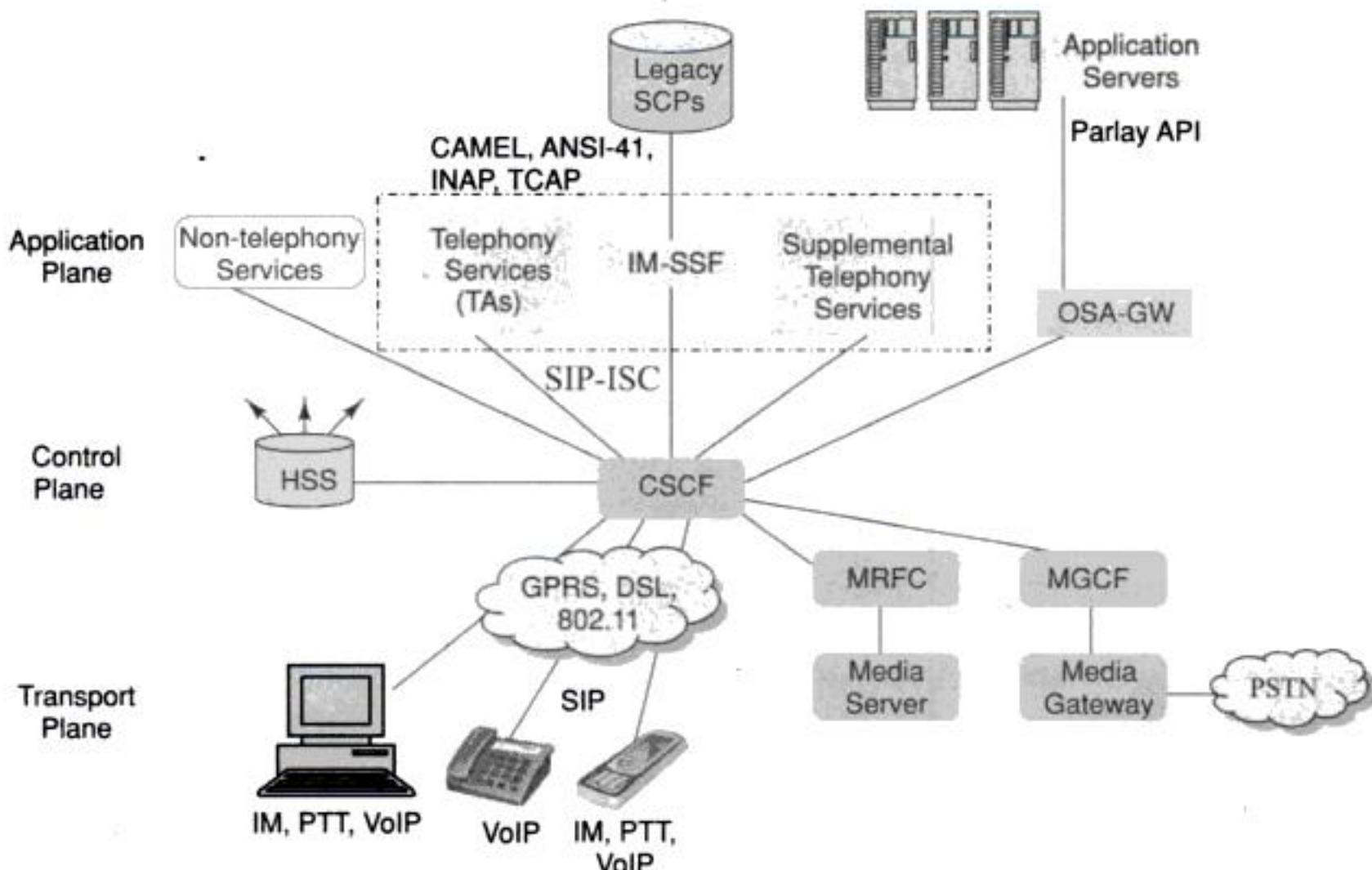


Figure 19.2 IMS Architecture in Relation to Service Planes



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

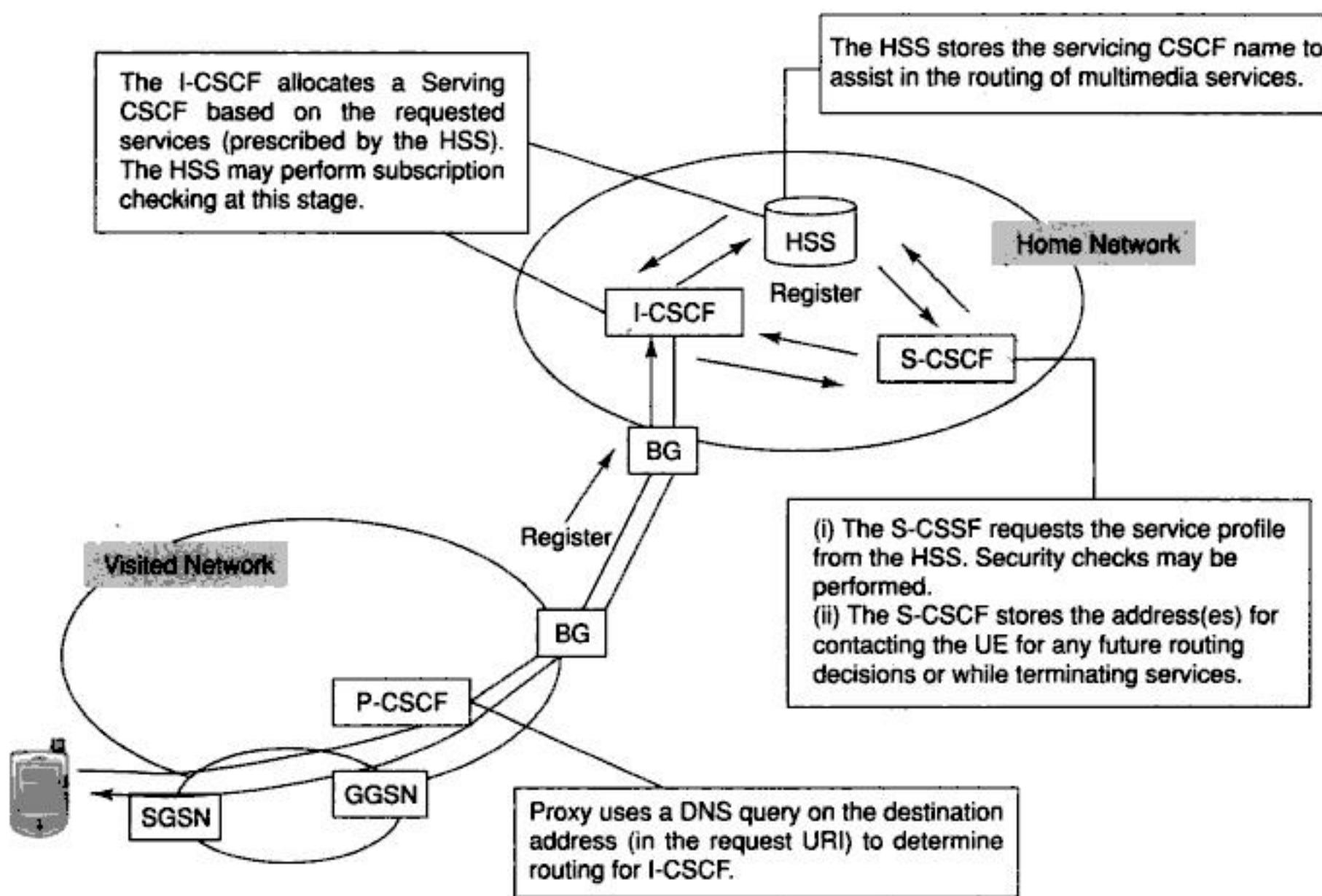


Figure 19.3 Call Flow from Visited Network

IMS charging functions will be any combination of the following criteria:

Volume based charging: In this mode the volume of data transacted will be charged. For example, the charging is done based on MB (Mega Bytes) of data transferred. This is also referred as usage-based charging. This is done through the network flow data. IP Data Record is used to measure and charge a subscriber.

Time based charging: This handles the duration for which the user was logged in into the network. The charging could also be based on time of the day. For example, accessing the network after 11:00 PM at night could be free. Also, there could be different rates during the weekend.

QoS based charging: This type of charging is dependent on quality of service. For example, a user wants to subscribe to some video (Video on Demand) for which the user needs a higher bandwidth for some fixed duration. For this duration the network will guarantee some higher bandwidth and the user needs to pay a different tariff for this activity.

Event based charging: This type of charging is dependent on events. Events could be mail, instant messaging or some other push events like stock quotes when the price of some script moved up or down compared to some user defined threshold.

Service based charging: The operator could charge different rates for different services. For example, a VoIP service may be priced differently compared to Web browsing. Also, browsing some sites could be free. Even browsing web sites with operator injected advertisement could be free.

Content based charging: This type of charging is dependent on the content that is being accessed. For example, a live soccer game could be charged differently compared to other IPTV programs.

19.8.1 IMS Charging Functions

The architecture of IMS allows for various models which can be put in practice. Such models can not only be provisioned to include only the calling party for charging but also the called party. A called party can be charged in case it adds a new media stream to the existing stream or modifies the existing one to a costlier one. It is also possible that the operator is interested in correlating charging information generated in transport and IMS charging levels.

IMS is well supportive of both online and offline charging mechanisms. Online charging directly interacts with session and affects the service rendered in real time. A good example is prepaid service. On the other hand, offline charging does not affect the services consumed in real-time and the operator posts a bill to the user for a period. For supporting the online charging mechanism, IMS network nodes consult the Online Charging System (OCS). OCS maintains a real-time interaction with the user's account and continuously monitors the charges depending on the service usage (Refer to Figure 19.4).

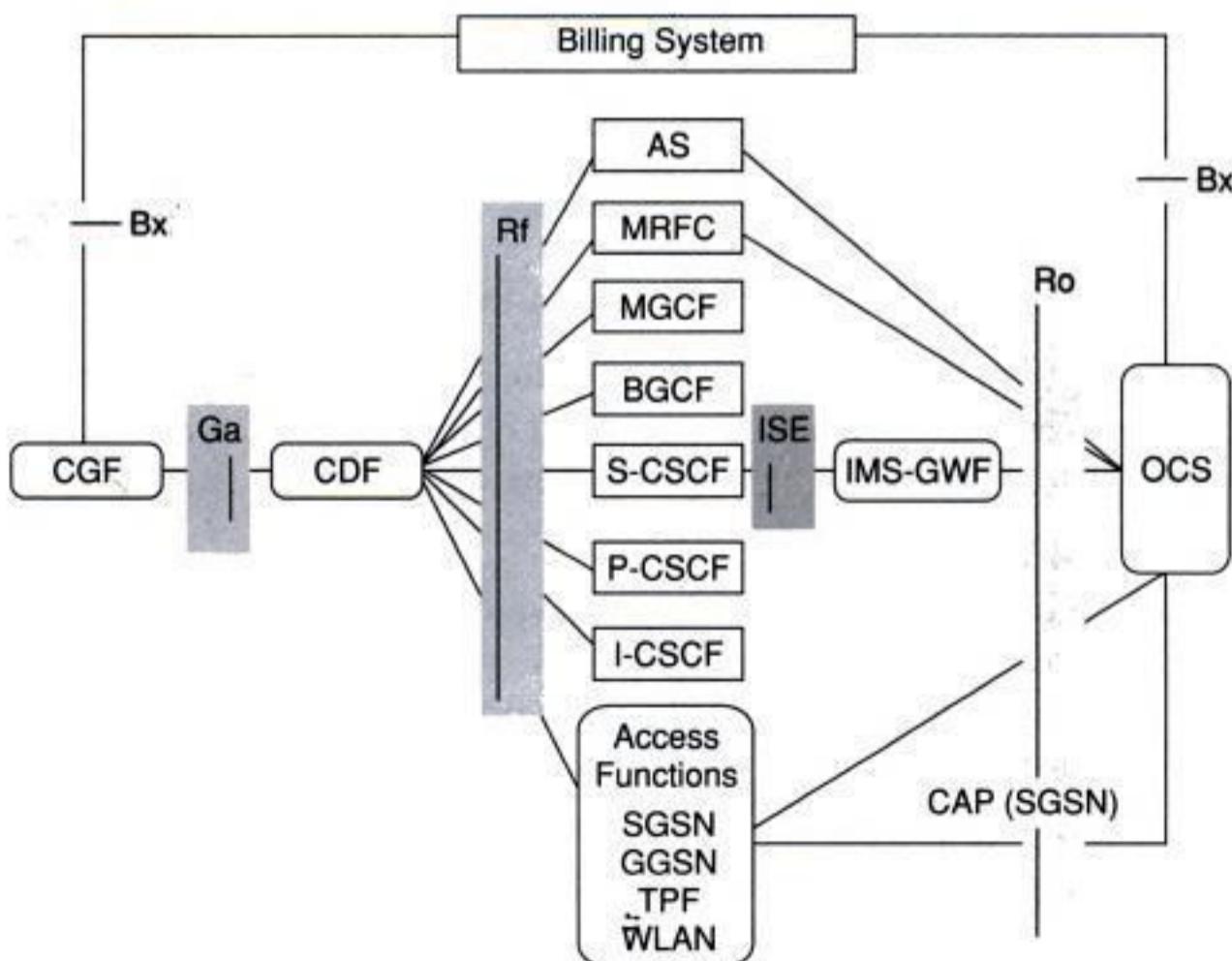


Figure 19.4 Architecture of IMS Charging (Left portion—offline charging and right portion—online charging)



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



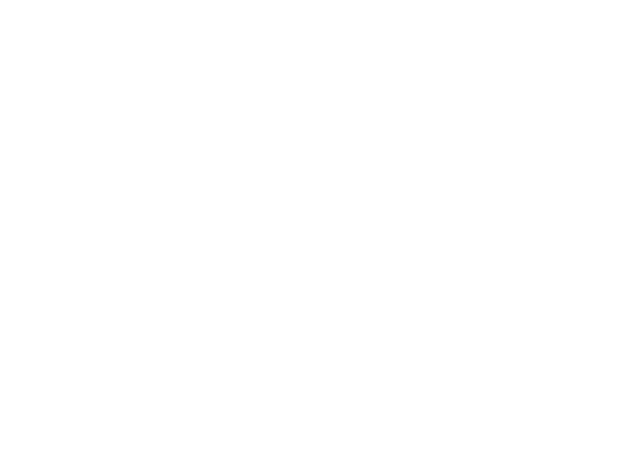
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

be able to decrypt the message using his or her own secret private key. If there is a surrogate who is able to intercept the encrypted message, he will not be able to decrypt the message, as the key required to do so is the private key. The receiver's private key is kept secret with the receiver. The methodology used for authentication or digital signature is just the reverse. In case of signing the transaction, the private key of the sender is used by the sender. The receiver uses the public key of the sender to read the signature. This authenticates that the transaction was indeed done by the sender.

20.3.4 Key Exchange Algorithm

Whitfield Diffie and Martin Hellman first introduced the notion of public key cryptography in 1976. In the Diffie Hellman technique, secret keys are never exchanged. However, the technique allows two parties to arrive at a secret key through the usage of public keys. Communicating parties select a pair of private and public keys. Public keys are exchanged. The shared secret key is generated from the private key and the public key of the other party.

Let us assume that there are two parties A and B. A and B choose some prime number p and another number g less than p . These numbers are selected and made available to both A and B in advance. The steps followed in Diffie Hellman algorithms for key generation are as follows:

1. Let these p and g be: $p = 13$ and $g = 3$;
2. A chooses a random number SA . This number is kept secret as a private key with A. Let this number be 5.
3. B chooses a random number SB . This number is kept secret as a private key with B. Let this number be 7.
4. A takes g and raises it with his secret key SA modulo p . This will be $TA = (g ^ SA) \bmod p \Rightarrow (3 ^ 5) \bmod 13 = (243) \bmod 13 = 9$. This number 9 is A's public key. A already has chosen 5 as his private key.
5. B takes g and raises it with his secret key SB modulo p . This will be $TB = (g ^ SB) \bmod p \Rightarrow (3 ^ 7) \bmod 13 = (2187) \bmod 13 = 3$. This number 3 is B's public key. B has already chosen 7 as his private key.
6. Public keys of A and B are exchanged. This means A sends the public key 9 to B and B sends his public key 3 to A over a public channel like Internet.
7. A takes B's public key and raises it with his own private key mod p . Therefore, we now have $KA = (TB ^ SA) \bmod p \Rightarrow (3 ^ 5) \bmod 13 = (243) \bmod 13 = 9$.
8. B now takes A's public key and raises it with his own private key mod p in a similar fashion as A. The result will be $KB = (TA ^ SB) \bmod p \Rightarrow (9 ^ 7) \bmod 13 = (4782969) \bmod 13 = 9$.
9. The value of $(TA ^ SB) \bmod p = (TB ^ SA) \bmod p = 9$. Though KA and KB have been calculated by A and B independently; it will always be equal. Therefore, these keys KA and KB can now be used by A and B as the shared key for payload encryption.

Neither A nor B shared their secret key for use in symmetric encryption, but arrived at that using some properties of modulo arithmetic with prime numbers. The example above may look trivial. However, when these numbers are large, nobody can calculate the key just by knowing p , g and Sx in a reasonable period of time. An eavesdropper could not compute discrete logarithm, i.e., figure out KA based on seeing SB .

Similar techniques are used to make ciphering look random in few other algorithms with some variations. These are,

- Propagating cipher-block chaining (PCBC)
- Cipher feedback (CFB)
- Output feedback (OFB)
- Counter (CTR)

20.4 SECURITY PROTOCOLS

To provide confidentiality, integrity etc., we need to use different algorithms. However, we need to devise protocols that will use these algorithms in such a fashion that vulnerabilities are eliminated and security is ensured. The protocol needs to be so robust that a masquerader is unable to get the message being sent. The protocols need to ensure that if the masquerader is able to modify the message, we can detect it. There are many protocols for secured communication. One such protocol is depicted in Figure 20.5. However, the most popular protocol is SSL (Secured Socket layer—Section 20.4.1). SSL was originally developed by Netscape. The Internet standards for TLS (Transport Layer-Security—Section 20.4.2) and WTLS (Wireless Transport Layer Security—Section 20.4.3) have been derived from the SSL protocol.

20.4.1 Secured Socket Layer (SSL)

The Secured Socket Layer or SSL protocol is used to provide security of data over public networks like Internet. It runs above the TCP/IP protocol layer and below higher level protocols such as HTTP or IMAP (Fig. 20.5). SSL allows both machines (server and the client) to establish a secured encrypted channel so that all the data transacted between them are confidential and tamper-resistant.

Public-key encryption provides better authentication techniques. On the other hand, symmetric key encryption is much faster than the public key encryption. The SSL protocol uses a combination of both public key and symmetric key encryption. An SSL session begins with SSL handshake. SSL handshake allows the server to authenticate itself to the client using public-key techniques. Optionally, the handshake also allows the client to authenticate itself to the server. It then allows the client and the server to cooperate in the creation of symmetric key. It then uses this shared key for payload encryption, decryption, and tamper detection during the session that follows.

20.4.2 TLS

Transport Layer Security or TLS in short is a security protocol to offer secured communication at the transport layer. TLS protocol is the Internet standard and based on the SSL 3.0 protocol specification. According to RFC 2246 (TLS Protocol Version 1.0), the primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications. At the lower levels, TLS uses TCP transport protocol. The TLS protocol is composed of two layers: the TLS Handshake Protocol and the TLS Record Protocol.

key. It requires multiple keys. One key belongs to the customer; the other key is with the bank employee. Both the keys need to be used to open the locker. Take the example of ATM, where an ATM card and the PIN are required to withdraw cash. This technique is called multifactor security. These factors are generally a combination of “what you have”, “what you know”, and “what you are”. Multifactor security can be a combination of any of the following factors.

What You Have

- Magnetic stripe card
- Private key protected by password
- Smart card
- Hardware token
- RF badge
- Physical key

What You Know

- Password
- Pass Phrase
- PIN (Personal Identification Number)
- Answer to some personal questions
- Sequence of numbers
- Predetermined events

Who You Are

- Fingerprint
- Voice Recognition
- Retinal Scan
- Hand Geometry
- Visual Recognition
- Face (picture in passport)
- Other biometric identities

Most of the multifactor security systems in use today are two-factor ones. However, for defense systems and high security establishments three-factor securities are used. In a two-factor security any two of the above factors are used. In a three-factor security, one each from the above factors are used.

20.4.5 Digital Watermark

Watermarks are being used for a long time as a security measure. If we take a 100-rupee currency note of Reserve Bank of India and hold it in front of a light source, we can see Gandhi's face on the white circle. This is called the watermark in the currency note. If we photocopy a currency note using a color photocopier, we will not be able to copy the watermark. The term “digital watermark” refers to a pattern of information inserted in a file. The file can be a digital audio file, digital video file, or a data file that identifies the file's copyright information (author, rights, etc.). The purpose of digital watermark is to provide copyright protection for intellectual property that is in digital format. Unlike printed watermarks which are intended to be visible, digital watermarks are designed to be



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

21.5 FAMA/DAMA

In order to resolve medium access control issues, the Fixed Assignment Multiple Access (FAMA) protocol was proposed. The applications of FAMA protocol are characterized by the assignment of capacity in a fixed manner amongst multiple stations. Irrespective of the fluctuating demands (of stations), the stations are assigned a fixed channel capacity. However, this results in significant underuse of the overall available capacity.

FAMA protocols can be in of different flavors such as Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA) or Space Division Multiple Access (SDMA). However, all such FAMA flavored protocols assign a static portion which can be in terms of time, frequency, code or space, of the overall link capacity to different stations. That is, the assignment of resources are fixed and do not change according to station traffic patterns. The major benefit of FAMA based protocols is they can provide bounds for delay performance which become of paramount importance in real-time applications. However, following are some potential drawbacks:

- It is difficult to configure FAMA protocols when a new station comes in or moves out of a network system.
- The schemes of tuning FAMA flavored protocols (like TDMA, FDMA and Multi-Frequency TDMA) are labor intensive and unscalable.
- It is difficult to implement FAMA based protocols in a distributed mode.

Improvement over FAMA protocols, Demand Assignment Multiple Access (DAMA) protocols have capacity assignment in a manner that optimally respond to demands from/amongst multiple stations. DAMA protocols assign channels to stations based on the traffic information in the network. The assignment of channels is achieved through reservation or polling techniques so that each station can express their interest in using the channel for transmission based on its own traffic information. Such a process differs for different flavors of DAMA protocols. The reservation process can take place either in the primary communication channel or in a separate signaling channel depending upon the actual protocol. DAMA protocols can be collision free, in which each station will be assigned a fixed reservation slot, or it can be collision based, in which each station needs to compete with other stations when transmitting requests. Polling techniques can be used to decide which station should get the right of transmission over a certain channel during a certain time period as polling is naturally suited to networks with a centralized base station.

21.6 MULTI PROTOCOL LABEL SWITCHING (MPLS)

As a packet in a connectionless network layer protocol like IP travels from one router to the next, each router makes an independent forwarding decision for that packet. A smarter routing is essential for traffic engineering and efficient routing of packets in a converged network where there are payloads from both circuit switched networks and packet switched networks. Multiprotocol Label Switching (MPLS) as described in RFC 3031 (Multiprotocol Label Switching Architecture), does exactly this. MPLS operates at an OSI Model layer that is generally considered to lie between traditional definitions of Layer 2 (data link layer) and Layer 3 (network layer) to perform smarter routing, and thus is often referred to as a "Layer 2.5" protocol.

forward the traffic only to those interfaces from which it has received join messages. Destination IP addresses for multicast traffic fall within the range of 224.0.0.1 through 239.255.255.255 (although some addresses within this range are reserved). Destination Ethernet addresses for multicast traffic begin with 01:00:5E and end with the lower order 23 bits of the destination IP address. Many of the world's major telecommunications providers are exploring IPTV as a new revenue opportunity from their existing markets and as a defensive measure against encroachment from more conventional cable television services. In India BSNL is already offering IPTV through its Internet network. AT&T in the US launched its U-Verse IPTV service in 2006. AT&T offers over 300 channels.

IPTV uses a two-way digital broadcast signal sent through a switched telephone or cable network by way of a broadband connection and a set-top-box (STB) programmed with software that can handle viewer requests to access to many available media sources. The STB is programmed to allow only these channels that the subscriber has paid for. This is managed through close coordination between the CAS (Conditional Access System) at the head-end and a programmed smart-card within the STB.

IPTV covers both live TV as well as stored video through VoD (Video on Demand). The playback of IPTV requires either a PC or a STB connected to a conventional TV. Video content is typically compressed using either a MPEG-2 or a MPEG-4 codec and then sent in an IP Multicast in case of live TV or via IP Unicast in case of Video on Demand.

21.8.4 Internet TV

IPTV deals with TV broadcast over satellite, terrestrial, or mobile network. In IPTV the receiver device is still a HDTV (High Definition TV) or a SDTV (Standard Definition TV). By contrast "Internet TV" generally refers to transport streams sent over IP networks (normally the Internet) with receiver station being a PC or computer. An Internet TV provider has no control over the final delivery and so broadcasts on a "best effort" basis. Elementary streams over IP networks and proprietary variants as used by websites such as YouTube are now rarely considered to be IPTV services. Another main difference between IPTV and Internet TV is that IPTV are paid services that carry both free channels and paid channels; whereas, Internet TV is generally free.

21.9 MULTIPLE PLAY

Multiple play is a way to describe provision of diverse telecommunication services by vendors that usually offered one or two of such services. Some of the very common such telecommunication services are broadband Internet access, television, telephone (both wired and wireless), etc. Multiple play is a generic term for conglomeration of more than one service into a single bundled product or service. Terms like Triple Play or Quadruple Play describe specific service bundles.

21.9.1 Triple Play

Triple Play means provisioning of two broadband services—high-speed Internet access and television, and one narrowband service—telephone over a single broadband connection. Triple Play is, usually, delivered using a DSL link. In Triple Play, television contents are delivered through

DVB technology using set-top-box. Internet access is usually provisioned through an Ethernet port while voice services can be provided using either existing telephone network or voice over IP (VoIP). There is no standard configurations to offer Triple Play services. There can be different methods as well depending upon the budget at disposal, types of subscribers and geography of subscribers' premises.

The business challenges in offering Triple Play services are associated with ascertaining the right business model, backend processes, customer care support and capital expenditure. There are some technology challenges as well because voice, video and high speed data all have different characteristics and place different burdens on the network that provides access to these services.

21.9.2 Quadruple Play

Triple Play has led to a new term called Quadruple Play where wireless communications is introduced as another medium to deliver Triple Play services. Quadruple Play can be thought as Triple Play plus mobility. In the traditional business model of offering Quadruple Play services, the following are the major drawbacks:

- The networks are separate as the individual services have been offered using their own networks. Usually, wired access has been about voice and broadband access is a data service moving towards entertainment. Wireless networks deliver data and entertainment and, again, IPTV is about video. An operator may be maintaining two or even three different network infrastructures to deliver all these services.
- The user experiences are separate as subscribers use different devices, interfaces and methods to access various services which do not interact with each other.
- The billing systems are separate as subscribers may see all their service charges integrated on one bill but behind the scenes are disparate billing systems that must be maintained separately for each service.

Because of duplication of infrastructure, operating expenses for operators are high. It is difficult and costly to introduce new services. Even if consistent user experience for a service across multiple media can be created, the applications would have to be developed separately on each platform. For subscribers, too, there is not much benefit in moving all their services to one provider, besides the promise of a better price.

However, with advances in Internet Protocol and IP Multimedia Subsystem technologies, there are better options such as:

- IP provides a cost efficient way to converge voice, data and video transport on to a unified network infrastructure.
- IMS provides the next generation network architecture that converges voice, data and IPTV service attributes over multiple access types into a consistent user experience.
- By linking IPTV with IMS, television set-top-boxes can be added to the list of IMS endpoints along with mobile phones, personal computers and other consumer entertainment devices.

Due to advantages garnered by IP and IMS, users can enjoy a consistent user experience across various devices and access networks. Service providers can offer services that help users manage their personal libraries of commercial and private content. Then, such services can be extended to multiple devices and access networks. However, customers are more eager for just price breaks



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Index

- 1G, 4
2.5G, 4, 175
2G, 5, 189
3DES, Triple DES, 572
3G, 4
3G Specific Applications, 243
3GPP (Third Generation Partnership Project), 22
3GPP LTE, 606
3GPP Security, 592
4G, 605
6to4cfg, 109
802.11 Architecture, 258
802.11, 4, 5, 21
802.11i, 255
802.15, 254
802.16 MAC, 94
802.1x Authentication, 330
- A Party, 60
AAA (Authentication, Authorization and Accounting), 561, 605
Access channel, 231
Access point, 257–258
Access, 30
ACL (Asynchronous Connectionless Link), 85
ACM (Address Complete Message), 288, 289
- Active RFID tags, 90
ActiveSync, 477
Ad hoc, ad-hoc network, 5, 256, 275
AD, 605
Adaptability manager, 47
Adaptation manager, 42, 45, 46
Adopted protocols, 88
AES (Advanced Encryption Standard), 46, 279, 572
Agent application, 33
Aida32, 271
AirMagnet, 272
AKA (Authentication and Key Agreement), 561
Alternate line service, 297
AM, 610
AMC, 604
AMPS (Advanced Mobile Phone Service), 3, 10
A-Netz, 2
ANM (Answer Message), 289
ANSI (American National Standards Institute), 22
Applet firewall, 113
Application framework, 368
level security, 616
mode, 185
tier, 32, 33, 34
- toolkit, 122
on 3G, 243
AR (Access Requestor), 546
ARFCN (Absolute Radio Frequency Channel Numbers), 138
ARPA, 1
ARPU (Average Revenue Per User), 539
ASP, 50, 55
Association Process, 267
AT-Commands, 87
ATM, 9, 608
ATN (Automated Trust Negotiation Systems), 557
Attacks, 566
AUC (Authentication Center), 120, 124, 140
Authentication process, 267
Authorization, 544
Autonomous computing, 52
Awareness modules, 42
- B Party, 68
B3G, 601
Base station subsystem, 120, 122
Base station, 284
BCP (Basic Call Process), 300
Beacon frames, 367
Bearer mobility, 7

- Bearer, 10
 Behavior adaptation, 17
 Behavior management middleware, 10, 11
BGCF (Breakout Gateway Control Function), 548
 Bluetooth application model, 88
 Bluetooth, 4, 10, 22, 84
B-Netz, 2
BPSK (Binary Phase Shift Keying), 225
 Broadband Mobile Cellular System, 95
 Broadband, 9
BSC (Base Station Controller), 118–122, 227, 280
BSSAP (Base Station System Application Part), 129
BSSGP, 179, 180
BTS (Base Transceiver Station), 118, 122, 133, 227, 280
 Buffer overflow attacks, 567
 Burst formatting, 125
 Busy tone, 60
BWA (Broadband Wireless Access), 280
 Bx reference point, 553

CA (Certification Authority), 583, 588, 596
 Cable modems, 603
 Cable replacement protocol, 87
 Call barring, 296
 flow, 71, 72, 83
 forwarding, 295
 routing, 492
 waiting, 297
 Caller line ID, 297
CAMEL (Customized Application for Mobile Enhancement Logic), 246, 255
 CAMEL application part, 298, 351
CAP (CAMEL Application Part), 553
 CAP file, 131

 CAP, 298–305
CAP, CAMEL Application Part, 298
 Care-of address, 97–100
CAS, 612
CC/PP (Composite Capabilities/Preference Profiles), 43
 CDC, 364, 393, 394
CDF (Charging Data Function), 553
CDG (CDMA Development Group), 22
CDMA, 4, 10, 607
 CDMA Registration, 233
 CDMA versus GSM, 235
 CDMA-2000, 263
 cdmaOne, 224–226, 278–285
CDPD, 9
 CDR (Charging Data Records), 553
 Cell cluster, 118
 Cell ID, 154
 Cell identifier, 130
 Cells design in wireless LAN, 258
 Cellular IP, 102–105, 115
 network, 2
 phone, 2
 technology, 117
 Certificate, 586
CFB (Call Forwarding Busy), 119
Cflowd, 272
CFNA (Call Forwarding Not Answered), 119
CFNR (Call Forwarding Not Reachable), 119
CFU (Call Forwarding Unconditional), 119
CGF (Charging Gateway Function), 553
CGI, 34
 Channel coding, 125, 177
 selection, 271
CHAP (Challenge Handshake Authentication Protocol), 278

 Charging, 550
 checkv4, 107
 Chirp, 220
cHTML (Compaht Hyper Text Markup Language), 195
CICS, 35
CID, 154
CIMD, 149
 Ciphering, 125, 135, 145
CLDC, 457, 395–400
CLI (Caller Line Identification), 119
Client Context Manager, 42, 45, 56
 Closed user group, 297
CO, 601
 Coarse Grained IP Mobility, 111
 Code Division Multiple Access (CDMA), 63
 Code transcoding, 48
CELP (Code-Excited Linear Prediction), 227
 Combined Delivery, 215
 Communication middleware, 10, 11, 35
 Communication Services and Networking, 468
 Components of Information Security, 568
CC/PP (Composite Capability/Preference Profile), 43, 198
 Computer Telephony Interface, 66, 67
CEPT (Conference of European Posts and Telegraphs), 3
 Confidentiality, 46, 568
 Configuring the Wireless LAN, 271
 Connection Management, 131
 Content aggregation, 50
 based Charging, 552
 filtering, 38, 49
 rating, 56, 57
 Context aware systems, 43
 Context-sensitive content switch, 418
 Convergence, 601, 605

- Converted Aplet, 113
COPS (Common Open Policy Service), 486, 487, 502
COPS-PR (COPS for Policy Provisioning), 546
CORBA, 37
Core, 30
Cos, 608
CPI (Capability and Preference Information), 198
CPL (Call Processing Language), 497
CRC (Cyclic Redundancy Code), 86
Crossbar exchange, 59
CRP (Customer Routing Point), 293
CSCF (Call Session Control Function), 547
CSD (Circuit Switched Data), 4
CSMA/CA, 263, 264, 265
CSP (Communications Service Provider), 539
CT, 601
CTI (Computer Telephony Integration), 67
CAMEL (Customized Applications for Mobile Network Enhanced Logic), 298
Cx Reference Point, 554
Cyborg, 6
DAB, 606
DAMA, 607
Data tier, 32, 33, 39
DUP (Data User Part), 297
Database Middleware, 35, 40
DCE (Data Circuit terminating Equipment), 87
Denial of Service, 567
DES (Data Encryption Standard), 572
Developing Mobile Computing Applications, 26
Device Mobility, 7
Dh Reference Point, 555
DHCP, 181, 184, 237
Dial Tone, 60
Dialogic, 67–70
Dial-up, 4, 9
Diffie Hellman, 580
DIFS, Distributed IFS, 266
DSP (Digital Signal Processing), 69, 75
Digital Signature, 39, 47, 50
Digital TV, 8
Digital watermark, 582
Digitizer and source coding, 124
Direct sequence, 219, 220, 242
Distributed functional plane, 300
Distributed object and components, 35
Distribution system, 258
DNS, 182
DoCoMo, 10, 195, 238
Document server, 75, 76
DSL (Digital Subscriber Link), 539
DSL (Digital Subscriber Line), 9, 92, 600
DSSS (Direct Sequence Spread Spectrum), 220, 242, 250, 260, 261
Dstumbler, 272
DTE (Data Terminal Equipment), 87
DTMF (Dual Tone Multi Frequency), 8, 68
DVB, 606
Dx reference point, 554
Dynamic label segment, 610
E1, 67
EAP (Extensible Authentication Protocol), 278
Edge, 30
EIA (Electronic Industries Alliance), 21
EIFS (Extended IFS), 266
EIR (Equipment Identity Register), 120, 121, 124, 129, 136
Elliptic curve, 574
eMbedded visual tools, 477
End Office, 60
Engineers, 5, 6, 21
Enhancement logic, 246, 255
ENUM, 248, 249
ESME (External Short Message Entity), 149, 166–167
ESS (Electronic Switching System), 2, 59, (602)
Ethernet, 8, 24, 612
ETSI (European Telecommunication Standards Institute), 3, 20
Event based charging, 551
EventLoop, 337
Events, 79
Exposed terminal, 263
Extended service set, 258
Fabrication, 566
FAMA, 607
FCAPS, 603
FCC (Federal Communication Commission), 2
FDD (Frequency-division duplexing), 94
FDMA (Frequency Division Multiple Access), 4, 61, 63, 83, 607
FEC (Forward Error Correction), 86
FHSS (Frequency Hopping Spread Spectrum), 259–261
Fiber-optic systems, 59
File transfer, 88
Fill-in signal unit, 298
Fine grained IP mobility, 111
Firewall, 47
First palm, 340
Fixed wireless, 242
FM, 610
Foreign agent, 97–102, 111
Form, 341
Forms, 79
Fortezza, 572
Forward traffic channel, 231
Forward-lock, 215
Foundation profile, 395
FRA (Fixed Radio Access), 280

- Fragmentation, 260, [266](#)
 Frame relay, [9](#), [176](#), 179
 Frequency band, 85
 hopping spread spectrum, 85, 256, 260
 hopping, 220, 236
 reuse considerations, 235
 reuse distance, [117](#)
 division duplex, 242
 FSU (Fixed Subscriber Unit), 280
 ftp, 109
 Functional entity action, 302
 entity, 302, 303
 FWA (Fixed Wireless Access), 280
 G.711, 481
[G.723.1](#), 481
 G.728, 481
 Ga reference point, 553
 Gatekeeper, 482
 Gateway MSC, 118, 121, 123, [124](#), 127, [136](#)
 Gateway, [8](#), 481
 GGSN (Gateway GPRS Support Node), [176](#)
 GIWU (Gateway Interworking Unit), 121
 Global functional plane, [300](#)
 Global system for mobile communications, [116](#)
 Gm reference point, 553
 GMSC (Gateway MSC), 118, 121, 123, [124](#), 127
 GMSK (Gaussian Minimum Shift Keying), 125
 Go reference point, 556
 GPRS (General Packet Radio Service), 174, 601
 GPRS
 applications, 178
 architecture, 190
 attachments, 181
 bearers, 186
 billing, 189
 channel coding, 177
 data, 185
 detachments, 181
 handset, 186, 187
 mobility management, 183
 physical interface, routing, 183
 security, 181
 tariffing, 189
 GPS (Global Positioning System), [53](#), [54](#), 154
 grammar, 78
 GSM (Groupe Spécial Mobile), [3](#), [116](#), 601
 GSM
 1800 MHz, [116](#)
 1900 MHz, [116](#)
 900 MHz, [116](#)
 algorithm A3, [135](#)
 algorithm A5, [140](#)
 algorithm A8, 141
 architecture, 118
 call routing, [124](#)
 entities, 119
 frequency allocation, 138
 identifiers, 129
 interworking unit, 123
 modem, [151](#), 154, 155, 161, 164, 166
 security, [140–142](#)
 Guard interval, 606
 GWES (Graphic Windowing and Event System), 469
[H.225.0](#), 481
[H.245](#), 481
[H.261](#), 481
[H.263](#), 481
[H.323](#), 481
 Handoff, [51](#), [52](#), 133
 Handoff and roaming, 233
 Handover, 123, 129, 130, 133
 Hard handoff, [234](#)
 Hardware interfaces, 362
 Hashing algorithms, [47](#)
 HC SDMA, 614
 HCI (Human Computer Interface), [8](#)
 HDML (Handheld Device Markup Language), 195
 HDTP (Handheld Device Transport Protocol), 195
 HDTV, [612](#)
 HE AAC, 610
 Headset, [88](#)
 HelloSymbian, 365
 Hidden terminal, [263](#)
 HLR (Home Location Function), 547
 HLR (Home Location Register), 118–147, 280
 Home address, 97–102
 Home agent, 97–102
 HomeRF, 256
 Host mobility, [7](#)
 Hot spot, 258
 HSDPA, 604
 HSOPA, 616
 HSPA, 604, 616
 HSS (Home Subscriber Server), 547
 HSUPA, 604
 HTTP, [29](#)
 Hybrid system, 220
 HyperLAN, 256
 IAM (Initial Address Message), 289, 295, 297
 ICAP (Internet Content Adaptation Protocol), [37](#)
 ICC, [112](#)
 icmp6, 109
 I-CSCF (Interrogating Call Session Control Function), 547
 ICT, [2](#), 602
 ID hopping, 130
 IEEE (Institute of Electrical and Electronics Engineers), [5](#), [6](#), [21](#)
 IEEE
 [802.11](#) Standards, [254](#)
 [802.16](#), [92–94](#)
 802.16e, 605
 IEEE802.11, [4](#)
 IGMP, 611
 IM SSF (IP Multimedia Services Switching Function), 548

IMAP, [11](#), [40](#)
 iMode, [8](#)
 IMS (IP Multimedia Subsystems), [539](#)
 IMS GWF (IMS Gateway Function), [553](#)
 IMS, [613](#)
 IMSI, [118](#), [122](#), [129](#), [130](#)
 IMT-2000, [175](#), [196](#), [219](#), [239](#)
 IN Conceptual Model, INCM, [311](#)
 ISM (Industrial, Scientific, and Medical), [5](#)
 InfoPyramids, [48](#)
 Information and communications technologies, [2](#)
 Information flow, [298](#), [302](#)
 Information security, [568](#)
 IrMC (Infrared Mobile Communication), [88](#)
 Infrastructure Level Security, [588](#)
 Infrastructure mode, [256](#)
 Inquiry hopping sequence, [87](#)
 Integrity, [46](#), [489](#), [520](#)
 Intellectual Property Rights Management, [50](#)
 INAP (Intelligent Network Application Protocol), [310](#)
 IN (Intelligent Networks), [67](#), [246](#), [287](#)
 Intelligent peripheral, [294](#), [302](#)
 ITTP (Intelligent Terminal Transfer Protocol), [195](#)
 Inter Domain Security, [560](#)
 Inter Frame Spaces, [266](#)
 IAPP (Inter-Access Point Protocol), [268](#), [255](#)
 Interception, [566](#)
 Interconnecting IPv6 networks, [111](#)
 Interfaces, [344](#), [363](#), [368](#)
 Interleaving, [125](#)
 IMEI (International Mobile Station Equipment Identity), [129](#)

IMSI (International Mobile Subscriber Identity), [118](#), [122](#), [129](#)
 Internet bridge through Bluetooth, [88](#)
 IETF (Internet Engineering Task Force), [19](#)
 Interworking MSC, [124](#)
 Interworking with IP network, [184](#)
 Intra domain security, [562](#)
 IMS (IP Multimedia Subsystem), [498](#)
 IP, [600](#)
 ip6, [108](#)
 IPDR (IP Data Record), [549](#)
 IPSec (IP Security), [546](#)
 IPsec IKE (Ipsec Internet Key Exchange), [109](#)
 IPTV (IP Television), [611](#)
 IPv6
 address space, [104](#)
 packet payload, [108](#)
 security, [104](#)
 IPv6, [105](#), [109](#), [600](#), [605](#)
 migration from IPv4, [108](#)
 Mobile IP, [111](#)
 IrDA (Infrared Data Association), [5](#), [10](#)
 IS-41, [298](#)
 IS-95
 Architecture, [227](#)
 Authentication and Security, [233](#)
 Call Processing, [232](#)
 Channel Capacity, [277](#)
 Channel Structure, [229](#)
 IS-95, [229](#)
 ISC (International Switching Center), [122](#)
 ISC Reference Point – IMS Service Control Reference Point, [553](#)
 ISDN User Part, [129](#)
 ISDN, [9](#)
 ISI, [606](#)

ISIM (IP multimedia Subscriber Identity Module), [549](#)
 ISM band, [5](#)
 ISM (Industrial Scientific and Medical), [5](#)
 ISO (International Organization for Standardization), [19](#)
 ISP, [616](#)
 iStumbler, [272](#)
 ISUP, [129](#), [289](#), [294](#)
 IT, [601](#)
 ITU (International Telecommunication Union), [5](#)
 IVR (Interactive Voice Response), [8](#), [67](#)
 application development, [71](#)
 programming, [81](#)
 IWMS, [124](#)
 J2EE, [451](#)
 J2ME record management system, [428](#)
 J2ME RMI profile, [395](#)
 J2ME, [429](#)–[431](#)
 J2SE, [395](#), [398](#)
 Jain, [306](#)
 Jar, [590](#)
 Jarsigner, [591](#)
 Java card applet, [114](#)
 java card interpreter, [113](#)
 JCVM (Java Card Virtual Machine), [112](#)
 Java
 card, [112](#), [113](#), [114](#), [115](#)
 in handheld, [392](#)
 message service, [35](#)
 security, [590](#)
 Java, [364](#)
 Javamail, [11](#)
 JCRE (The Java Card Runtime Environment), [112](#), [113](#)
 JSP, [34](#)
 JSR (Java Specification Request), [116](#), [557](#)
 Kannel
 bearerbox, [168](#), [169](#)
 smsbox, [168](#), [169](#)
 Kannel, [168](#)–[201](#)

- Kerberos, 271, 277, 278
 Key Recovery, 583
 Keytool, 590
- L2CAP (Logical Link Control and Adaptation Protocol), 86, 87
 LAN Access through Bluetooth, 89
 Legacy application, 17, 34
 Limiting RF Transmission, 274
 Line of sight, 5
 LPC (Linear Prediction Coding), 227
 Link Status Signal Unit, 352, 298
 links, 29
 LLC, 177–179
 LMP (Link Manager Protocol), 86, 87
 Local access tandem, 60
 Local loop, 60
 LMSI (Local Mobile Subscriber Identity), 130
 Local Number Portability, 302, 303
 LA (Location Area), 130, 136, 137
 Location area identity, 130
 Location aware, 14
 Location based software, 154
 Location information, 53
 LSR, 608
- MAC address access control, 275, 577
 MAC layer, 263, 266, 268
 M2M (Machine to Machine), 34
 Managing 802.11 Networks, 271
 Managing access points, 270
 MANET, 256, 272
 MAP (Mobile Application Part), 129, 130, 131
 Mbone, 611
 MCU (Multipoint Control Unit), 481, 482
 MD5, 577
 Media Gateway Controller, 546
 Media Gateway, 548
 Mediation server, 34, 36
- MEGACO (Media Gateway Control Protocol),
 Megaco/H.248, Media Gateway Control Protocol, MGCP, 490
 Memory, 320, 321, 322
 Message centre, 121
 Message queue, 35
 Message Signal Units, 298
 Message-Oriented Middleware, 35
 MexE, 144, 185, 198
 Mg reference point, 555
 MGW (Media Gateway), 548
 Mi reference point, 555
 Microprocessor, 315
 Middleware, 8, 10
 MIDlet event handling, 405
 MIDP, 405, 409, 416
 MiniStumbler, 272
 Mj Reference Point, 555
 Mk Reference Point, 555
 Mm Reference Point, 555
 MMS (Multimedia Message Service), 206, 208–220
 architecture, 208
 configuration, 212
 controller, 208
 device management, 212
 interconnection, 212
 interoperability, 212
 roaming, 212
 MMSC, 199, 208, 212
 MMTEL (Multimedia Telephony), 557
 Mn reference point, 555
 Mobile ad-hoc networks, sensor networks, 273
 Mobile agent security, 596
 MAP (Mobile Application Part), 298
 Mobile computing through telephony, 58
 MCC (Mobile Country Code), 129
 ME (Mobile Equipment), 120, 121, 124
 Mobile execution environment, 246
- Mobile IP discovery, 98
 Mobile IP registration, 98
 Mobile IP tunneling, 98
 Mobile IP, 96–102
 MNC (Mobile Network Code), 129, 130
 Mobile phone virus, 595
 Mobile phone worm, 596
 Mobile phones, 317, 323, 363
 Mobile services, 20
 Mobile subscriber ISDN, 118, 127, 129
 MSC (Mobile Switching Center), 121–122
 Mobile Virtual Private Network, 593
 Mobile VoIP, 503
 Mobility management, 131, 132, 143
 Modification, 566
 Modulation, 125
 Mozilla, 25–29
 Mp reference point, 556
 MPEG, 51, 610
 MPLS, 607
 Mr Reference Point, 556
 MRF (Media Resource Function), 548
 MRFC (Media Resource Function Controller), 548
 MRFP (Media Resource Function Processor), 548
 MS (The Mobile Station), 120–123, 125, 136, 176
 MS (Mobile Station), 120–126
 MSC, 133–138
 MSIN (Mobile Subscriber Identification Number), 129
 MSISDN (Mobile Subscriber ISDN Number), 129
 MSISDN, 118, 127, 129, 136
 MSRN (Mobile Station Roaming Number), 130, 136
 MSP, 616
 MSRN, 137, 144
 MTP (Message Transfer Part), 297–300
 Multifactor security, 594

- Multimedia
 applications, 352
 service, 187
 support module, 549
- Multimedia, 350, 353
- Multiparty call conferencing, 296
- Multipath, 125
- Multiple access procedures, 61
- Multiplexing, 61, 63
- Multitasking, 330, 380
- Mutual and spatial authentication, 595
- MVNO (Mobile Virtual Network Operators), 50, 149, 151
- Mw reference point, 554
- NBS (Narrowband Sockets), 195
- NDC (National Destination Code), 129, 137
- NDP (Network Decision Point), 546
- NDS (Network Domain Security), 560
- NDS/IP (NDS/Internet Protocol), 5
- NetStumbler, 272
- NSS (Network and Switching Subsystem), 120–125
- Network
 mobility, 6
 plug-ins, 346
 probe, 272
- NGN, 600
- NNI (Network to Network Interface),
- Nomadic computing, 6
- Non-repudiation, 46, 568, 570
- OBEX (Object Exchange Protocol), 40, 88
- Object exchange, 40
- Object or semantic transcoding, 48
- OCS (Online Charging System), 552
- OEM, 50
- OFDM spectrum, 606
- OFDM, 605
- Off-card VM, 113
- OMA (Open Mobile Alliance), 20
- OMA digital rights management, 215
- OMC (Operation and Maintenance Center), 120–121
- On-card VM, 112
- One Time Passwords, 278
- Operating System, 315, 319
- Operator independent SMS pull, 151
- Organiser programming language, 358
- Orthogonal variable spreading factor, 242
- Orthogonality, 606
- OS/390, 34
- OSA-SCS (Open Service Access Service Capability Server), 548
- OSS (Operation and Support Subsystem), 34, 120
- OTA, 112
- OTA (Over-The-Air), 112, 141, 173
- Paging
 caches, 103
 channel, 229
 update packets, 103
- Palm
 OS applications development, 355
 OS Architecture, 344
- Palm OS, 41
- PAM (Presence and Availability Management), 23
- Parlay group, 23
- Parlay, 306
- Passive RFID tags, 90
- Payload, 48, 49
- PBX (Private Branch Exchange), 67, 81
- PCI, 69
- PCM (Pulse Code Modulation), 59, 125, 601
- PCS, 10
- P-CSCF (Proxy Call Session Control Function), 547
- PDA (Personal Digital Assistant), 5, 10, 319–320
- PDAP, 392
- PDF (Policy Decision Function), 513
- PDN (Public Data Network), 120
- PDP (Packet Data Protocol), 176, 178, 181
- PDP (Policy Decision Point), 546, 559
- PDUs (Protocol Data Units), 176
- PEAP (Protected EAP), 278
- PEP (Policy Enforcement Point), 546, 559
- Personal basis profile, 453
- Personal communication networks, 246
- Personalization, 49, 50
- Pervasive computing, 6
- Physical entity, 326
- Physical layer, 260, 281
- Physical plane, 300
- PIB (Policy Information Bases), 546
- Piconets, 85
- PICS (Platform for Internet Content Selection), 49, 50, 82
- PIFS (Point Coordination IFS), 266
- Pilot channel, 230, 231
- PIM, 89, 285
- ping6, 109
- PKCS (The Public-Key Cryptography Standards), 23
 #1, 583
 #10, 583
 #11, 584
 #12, 584
 #13, 584
 #15, 584
 #3, 584
 #5, 584
 #6, 584
 #7, 584

- #8, 584
 #9, 584
Platform for Privacy Preference Project (P3P), 47
PLCP (Physical Layer Convergence Procedure), 260
PLMN (Public Land Mobile Network), 10, 118
PLMN interface, 124
 Plug-ins, 346, 347
PMD (Physical Medium Dependent), 262
 Pocket PC, 465, 466, 475
 PocketWarrior, 272
 Point of initiation, 301
 Point of return, 292
 Policy based security, 590
 Policy manager, 45, 560
 Policytool, 591
POP3, 11, 40
 Portal, 258
POS, 31
 POTS, 600
 Power saving, 267
PPP (Point-to-Point Protocol), 88
PR (Policy Repository), 546
 Presence server, 554
 Presentation tier, 32
 PrismStumbler, 272
Privacy, 47, 49
 Private user identities, 549
 Profiles, 345
 Programmable networks, 305
 Prompts, 78
 Proto, 109
 Proxy server, 484
 PSDN, 600
PSI (Public Service Identity), 556
PSTN (Public Switched Telephone Network), 60, 600
 Public key cryptography, 573
 Public key, 278
 Public user identities, 549
 Pull, 149, 151, 153
 Push access protocol, 202
 Push over-the-air protocol 202
 Push, 150, 153, 154
 Q.922, 179
 Q.931, 86, 87, 131
 Quadruple play, 612
QoS (Quality of Service), 539, 600
 QoS based charging, 551
QPSK (Quadrature Phase Shift Keyed), 225, 226, 241
 Quality of service and security, 485
 Quantization, 59
RFID (Radio Frequency ID), 84
 Radio Resources Management, 131
 Radio subsystem, 121, 133
RADIUS (Remote Authentication Dial In User Service), 271, 277, 544
 Reassembly, 266
 Redirect server 484
 Regular pulse excited-linear predictive coder, 124
 REL, release message, 289
 Replay attack, 561
Resaca, 49
 Resource description framework, 44, 46
 Reverse traffic channel, 232
RFCOMM (Radio Frequency Communication), 87, 88
RFID applications, 94
 Security 595
 Technology, 603
 Ring generator, 60
 Ring tone, 60
RLC (Release Complete Message), 289
RLL (Radio Local Loop), 280
Roaming 136, 268
 Routing caches, 103
RPCU (Radio Port Control Unit), 280
RPE-LPC, 124
RS-232, 87
RSA, 574–577, 580, 583, 585–587
RSACI (Recreational Software Advisory Council–Internet), 49
RSU (Radio Subscriber Unit), 280
RSVP (Resource ReSerVation Protocol), 524, 525, 527
RTCP (RTP Control Protocol), 545
RTCP (Real-Time Control Protocol), 487, 488, 502
RTP (Real-Time Transfer Protocol), 545
RTP/RTCP, 481, 611
RTSP (Real-Time Streaming Protocol), 524
RTTP (Real-Time Transport Protocol), 524
SA (Security Associations), 563
SAFER+, 88
SAP/SDP, 488
SAPI (Speech Application Programming Interface), 81
SAT (SIM Application Toolkit), 122
SC, 119, 121, 124
 Scaling capacity, 269
 Scatternet, 85
SCCP (Signaling Connection Control Part), 297
SCF (Service Capability Feature), 144, 246
SCO (Synchronous Connection-oriented Link), 85
SCP (Service Control Point), 148, 290
S-CSCF (Serving Call Session Control Function), 547
SDMA (Space division multiple access), 63, 607
SDP (Session Description Protocol), 546
SDP (Service Discovery Protocol), 485
SDTV, 611
Seamless communication, 57

- Sectorization for capacity, 235
 Security, 18
 Security
 algorithms, 142, 598
 attacks, 307
 considerations, 356
 manager, 46, 113
 on Symbian,
 protocols, 563
 Self
 configurable, 52
 healing, 52
 optimizing, 52
 protecting, 52
 upgradeable, 53
 Semantic web, 46, 57, 596
 Separate delivery, 252
 Serial plug-ins, 346
 Service based charging, 552
 Service
 feature, 300, 355
 independent Building Block,
 301
 Service mobility, 499
 Service plane, 300, 342
 Service management system,
 294
 Services node, 294
 SGSN (Serving GPRS Support
 Node), 144
 SGW (Signaling Gateway), 548
 Sh reference point, 554
 SHA, 577
 SIP (Session Initiation Protocol)
 306, 480, 483
 Session mobility, 7
 Session oriented transaction, 9
 Short message service, 124
 Short transaction, 152
 Si reference point, 555
 SIFS (Short Inter Frame Space),
 260
 Signaling gateway, 488–496
 Sigtran and SCTP, 491
 SIM (Subscriber Identity
 Module), 120, 121
 Simple PKI, 588
 SIP (Session Initiation Protocol),
 539
 SIP AS (SIP Application Server),
 548
 SIP CGI, 486–487
 Skipjack, 572
 SLF (Subscriber Location
 Function), 547
 SM MO (Short Message Mobile
 Originated), 124, 148
 SM MT (Short Message Mobile
 Terminated), 124, 147
 Smart cards, 112, 122
 Smartcard security 529
 SME (Short Message Entity),
 147–151
 SMG (Special Mobile Group),
 538
 SMIL (Synchronization
 Multimedia Integration
 Language) 208, 210
 SMPP, 149, 152, 238
 SMS (Short Message Service), 4,
 194, 471, 600
 SMS
 alert, 153
 architecture, 124
 gateway, 147
 SMS PDU mode, 157, 160, 161,
 187
 SMS peer-to-peer, 39, 87
 SMS pull, 149
 SMS push, 150
 SMS strengths, 172
 SMS text mode, 157
 SMSC (Short Message Service
 Center), 142, 147
 SMS-GMSC, 147
 SMS-IWMSC, 147
 SMTP (Simple Mail Transfer
 Protocol), 40, 544
 SN (Subscriber Number), 137
 SNDCP, 178, 179
 SOAP, 149
 Soft handoff, 234, 236
 Softswitch 304, 305, 311
 Software development kit, 477
 SONET, 608
 SP (Signaling Point), 129, 130
 Spatial transcoding, 48
 SPC (Signaling Point Code),
 129, 130
 Speech and channel coding, 227
 SPI (Service Provider Interface),
 Spontaneous network, 10
 Spread spectrum technology,
 218, 219
 SS#7 protocol stack, 294
 SS#7 signalling, 291
 SS#7, 130
 SS7 (Signaling Stack), 7, 544
 SS7 security, 307
 SS7 signal unit, 298
 SS7 user parts, 294
 SS7, 123, 130, 131, 137, 140
 ssidsniff, 272
 SSID (Service Set Identifier),
 271, 274
 SSL (Secured Socket Layer), 472
 SSO (Single Sign On), 557
 SSP (Service Switching Point),
 293
 Standards, 18
 Standards for intelligent
 networks, 290
 Stations synchronization, 267
 STB, 612
 STP (Signaling Transfer Point),
 292–294
 Stream ciphering and block
 Ciphering, 571
 Supplementary services, 294,
 295, 304, 311
 Surrogate, 38
 Symbian architecture, 360
 Symbian development
 environment, 364
 Symbian OS, 358
 Symmetric key cryptography,
 571
 Sync channel, 231
 Synchronization, 89
 SyncML, 40, 56
 System level security, 589
 System managers, 333
 System software, 363

- [T.120](#) [T.38](#), [H.235](#), 481
[T1](#), [25](#)
[Tablet PC](#), [8](#)
[TAPI](#) ([Telephony Application Programming Interface](#)), [81](#)
[TCAP](#) ([Transaction Capabilities Application Part](#)), 130, 297, 299
[TCP/IP Protocol](#), [88](#)
[TCP/IP](#), [2](#), [30](#)
[tcpdump](#), 109
[TCS binary](#), 86, 87
[TD-CDMA](#) ([Time Division Code Division Multiple Access](#)), 538
[TDD](#) ([Time-division duplexing](#)), 94, 605
[TDMA](#) ([Time Division Multiple Access](#)), [4](#), [61](#), [62](#), [63](#), [607](#)
[Telematics](#), 188
[Telephony API](#), 387, 413
[Telephony call processing](#), 337
[Telephony control specification](#), 101, 103
[Telephony—evolution of](#), 73
[Telnet](#), 110
[Temporal transcoding](#), [48](#)
[THC-WarDrive](#), 272
[The MIDlet life-cycle](#), 399
[The MIDlet model](#), 397
[The network and switching subsystem](#), [120](#), [122](#)
[The push framework](#), [202](#)
[THIG](#) ([Topology Hiding Interworking Gateway](#)), 548
[Third Generation Networks](#), 238
[Three-tier application](#), [34](#)
[Three-tier architecture](#), [32](#)
[Time based charging](#), [551](#)
[Time hopping](#), 220
[Time-division duplex](#), 242
[TINA](#), 306
[TKIP](#) ([Temporal Key Integrity Protocol](#)), 279
[tlntsvr](#), 109
[TLS](#) ([Transport Layer Security](#)), [579](#), [580](#)
[TMSI](#) ([Temporary Mobile Subscriber Identity](#)), 130
[TN3270](#), [11](#), [34](#)
[TN5250](#), [34](#)
[Toll Free number Interactive Voice Response](#), IVR, 67–72
[Touchtone](#), 69
[TP monitor](#), [31](#)
[Tracepath](#), 109
[Traceroute](#), 109
[Tracert](#), 109
[TRAI](#) ([Telecom Regulatory Authority of India](#)), [2](#)
[Transaction processing middleware](#), [35](#), [36](#)
[Transaction processing](#), [11](#), [17](#)
[Transcoding middleware](#), [32](#)
[Transcoding](#), [48](#)
[Transit exchanges](#), [60](#)
[Trapdoor attacks](#), 568
[Triple play](#), [612](#)
[Trust](#), [46](#), 598, 605
[TSP](#), 616
[ttcp](#), 109
[TTML](#) ([Tagged Text Markup Language](#)), 195, [196](#), 227
[TTS](#) ([Text to Speech](#)), [75](#), 78–80
[Tunneling mode](#), 243
[TUP](#) ([Telephone User Part](#)), 297, 350

[U100](#), [31](#)
[UAProf](#), 198
[Ubiquitous computing](#), [6](#)
[Ubiquitous network](#), [30](#)
[UICC](#) ([Universal Integrated Circuit Card](#)), 549
[UMTS](#) ([Universal Mobile Telecom System](#)), [4](#), [22](#), 239, 244
[UMTS](#), 601
[UMTS/WCDMA](#), 238, 240
[UMTS](#) ([Universal Mobile Telecommunications System](#)), [22](#)
[UNI](#) ([User to Network Interface](#)), [124](#)
[Unicode SMS](#), [124](#)

[Unified messaging](#), 188
[Unsolicited response](#), [35](#)
[User agent profile](#), 188, 216
[User mobility](#), [6](#)
[USIM](#), [112](#), 247–250
[Using the connection manager](#), 347
[USSD](#) ([Unstructured Supplementary Service Data](#)), [10](#)
[Ut reference point](#), 556
[UTRAN](#), 605

[V.250](#), 87
[VAS](#), [value added service](#), [151](#)–[153](#)
[vCalendar](#), [88](#)
[vCard](#), [88](#)
[VDU](#), [31](#)
[VHE](#) ([Virtual Home Environment](#)), [6](#), 244, 245
[Virtual calling card service](#), 302
[Virtual carrier sense](#), [264](#), [266](#)
[Virus and worms](#), 567
[Visual basic](#), 477, 478
[Visual studio](#), 477
[VLR](#) ([Visitor Location Register](#)), [120](#), 123, 280
[Voice activity detection](#), 235
[Voice API](#), 71
[Voice browser](#), [76](#), [77](#)
[Voice driver](#), 70
[Voice mail](#), 296
[Voice portal](#), [76](#), [77](#)
[Voice software](#), 69
[VoiceXML architecture](#), [76](#)
[VoiceXML elements](#), [80](#)
[VoiceXML interpreter context](#), [25](#)
[VoiceXML interpreter](#), [75](#)
[VoiceXML](#), [75](#)–[81](#)
[VoIP](#) ([Voice over IP](#)), [81](#), [480](#), 601
[Volume based charging](#), 539
[VPN](#) ([Virtual Private Network](#)), [46](#), 67, 87, 608
[VRU](#) ([Voice Response Unit](#)), 67
[VT3K](#), [34](#)
[vxmxml](#), [77](#), [79](#)

- WAE user agents**, 198
WAE (WAP Application Environment), 197
WAFU (Wireless Access Fixed Unit), 280
Walsh function, 224
WAP (Wireless Application Protocol), 186, 194, [196](#)
WAP Forum (Wireless Application Protocol Forum), [20](#), 195
WAP gateway 205, 206
WAP push architecture, 197
WAP user agent, 198
WATM working group, 609
WATM, 609
WaveMon, 272
WaveStumbler, 272
WCDMA (Wideband Code Division Multiple Access), 538
WDP (Wireless Data Protocol), [204](#)
Wearable computer, [6](#)
Web scraper, [34](#)
Web services, [39](#)
WebTV, [31](#)
Wellenreiter, 272
WEP (Wired Equivalent Privacy), 276, 326, [328](#)
Wideband OFDM, 600
WiFi versus 3G, 283
WiMAX, 602
WiMax, [84](#), [92](#)
- Windows**
 CE 463, 465
 CE Architecture, 467
 CE Development, 476
 CE Storage, 469
 CE.NET, 465
 mobile for phones, 465
wininet, [108](#)
 Wireless broadband, 91
 Wireless data, 91
 Wireless data–evolution of, 240
 Wireless in local loop, [10](#)
 Wireless intelligent network, 304, 310
Wireless
 LAN applications, 253
 LAN architecture, 256
 LAN evolution [6](#), 252
 LAN mobility, 267
 LAN network fesign, 268
 LAN security, 279
LAN, [4](#)
 Wireless network–evolution, [2](#)
 Wireless PAN evolution, [5](#)
Wireless PAN, [4](#)
 Wireless sensor networks, 273
WSP (Wireless session protocol), [196](#), [202](#)
 Wireless technology, 601
 Wireless Telephony Application (WTA, WTAI), 188, 197, 228, 230, [234](#)
 Wireless VPN, 278
- Wireless WAN**, [4](#)
Wireless, [2](#)
WirelessMAN, [92](#), 94, [114](#)
WirelessMAN-OFDM, 94
WirelessMAN-OFDMA, 94
WirelessMAN-SC2, 94
Wireline network, [9](#)
WLAN, [5](#), 605
WLL (Wireless in Local Loop), 280
WML (Wireless Markup Language), 186, [196](#), 198
WML card, 199
WML deck, 199–201
WMLScript, 197, 198, [201](#), 216
W3C (World Wide Web Consortium), [21](#)
WorldWideWeb (www), [2](#), [21](#), [29](#)
WPAN, [5](#)
wship6, [108](#)
WSP, [40](#)
WTAI, 188
WTLS, [579](#), 581
WTLS (Wireless Transport Layer Security), [196](#), 216
WTP (Wireless Transaction Protocol), [196](#), [204](#)
WWAN, [52](#)
WWW, 602
X.25, [2](#)
XML, [22](#), [39](#), [40](#), [41](#), [44](#)

Authors' Profiles



Dr. Asoke K. Talukder is Chief Scientific Officer and Director of Geschickten Solutions, Bangalore. He is also Adjunct Faculty, ABV Indian Institute of Information Technology and Management, Gwalior; Adjunct Professor, Department of Computer Science and Engineering, NIT Warangal; and, Adjunct Faculty at Department of Computer Engineering, NITK, Surathkal. He was also the DaimlerChrysler Chair Professor at IIIT, Bangalore and Visiting Professor at VIT University, Vellore.

Dr. Talukder has been with the IT industry for about 30 years. He has held senior positions in different technology companies in India, USA, UK, and Singapore. He was the founder CTO of Cellnext, the pioneering wireless and Mobile Web technology company in India offering technology and solutions in the domains of GSM, GPRS, SMS, MMS, Intelligent Networks, CDMA, and 3G. He has been Corporate Advisor to SaharaNext, Lucknow; Advisor to the Expert Committee, HCL Bangalore; and the CTO and Executive Director–Telecom, Sobha Renaissance Information Technology, Bangalore. He has also worked in complex projects for companies like Fujitsu-ICIM, Microsoft, Oracle, Informix, Digital, Hewlett Packard, ICL, Sequoia, Blue Star Infotech, Northern Telecom, NEC, KredietBank, iGate, and many more.

Dr. Talukder did his Ph. D. (Computer Engineering) in Telecom Routing after completing his post graduation in Physics from the University of Calcutta (1976). He set up the first X.25 network in India for the Department of Telecommunications in 1986. Later, he set up the first Java Centre in India in 1998. He was a key engineer for the Oracle Parallel Server for Hewlett-Packard HP-FX fault tolerant computers, as well as the architect for the 64 bit Informix database for DEC Alpha.

He is the recipient of many international awards including All India Radio/Doordarshan Award, ICL Services Trophy, ICL Chief Executive Excellence Award, Atlas Club Excellence Award, ICIM Professional Excellence Award, ICL Excellence Award, IBM Solutions Excellence Award—one of his ubiquitous middleware products was the recipient of this award in 2001, and the Simagine GSM World Congress Award—one of his products on Java Card security was recipient of this award in 2003.

Mobile Computing

Second Edition

Technology, Applications and Service Creation

Mobile computing technology addresses challenges that enable the realization of a global village concept where people can seamlessly access any information anywhere anytime through any device. Written by professionals who have worked on several technologies, the book covers all communication technologies starting from First Generation to Beyond Third Generation (B3G) mobile technologies, wired telecommunication technology, wireless LAN (WiFi), and wireless broadband (WiMax). Also, Intelligent Networks (IN) and emerging technologies like mobile IP, IPv6, and VoIP have been included.

The revised edition has been thoroughly updated to reflect the technology changes from 2005 to 2010. Three new chapters covering Multimedia, IP Multimedia Service (IMS), and Next Generation Networks (NGN) have been added. Besides these, the book additionally covers:

- Mobile Computing Principles and Architecture
- Computer Telephony Interface and VoiceXML
- Personal Communication System-Architecture--Handoff--Roaming
- Mobility Management, GSM, and GPRS networks
- Short Message Service (SMS) technology and application creation
- IMT 2000—Evolution of 3G & 2G Vs 3G
- CDMA 2000 & WCDMA—Protocol Architecture—Physical Channels and Logical Channels
- SS7, Telecommunications, and Intelligent Networks
- Wireless LAN, WiFi, and WLL (Wireless Local Loop) Architecture
- IPsec and VPN (Virtual Private Network)
- Bluetooth, RFID, and Satellite Communications System—Infrastructure
- Mobile application development environments like J2ME, Symbian, SIM card, etc.
- Security issues in Mobile Communications and Mobile Computing environment

Packed with illustrations, examples, programs, and questions, *Mobile Computing* will serve the needs of professionals, teachers and students.

Updates, Powerpoint slides and much more available on

<http://highered.mcgraw-hill.com/sites/0070144575>

Visit us at : www.tatamcgrawhill.com

The McGraw-Hill Companies



Professional

ISBN-13: 978-0-07-014457-6

ISBN-10: 0-07-014457-5



9 780070 144576