KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0.

Last modified: 2003.03.12:18:57

maguire@it.kth.se

Table of Contents

1. Introduction 1

Welcome to the course! 2

Staff Associated with the Course 3

Instructor (Kursansvarig) ---------- 3

Administrative Assistant: recording of grades, registration, etc. ---------- 3

Goals, Scope and Method 4

Goals of the Course ---------- 4

Scope and Method ---------- 4

Prerequisites 5

Contents 6

Topics 7

Examination requirements 8

Project 9

Assignment Registration and Report 10

Literature 11

Lecture Plan 12

Context of the course 13
(Chapters 1-4, and 22) 14
Internet Architecture 15
More complete Architecture 16
Internetworking 17
Personal Communication Systems (PCS) 18
High Tier and Low Tier Cellular, and Cordless 19
Cellular Telephony 20
Low Tier Cellular and Cordless Telephony 21
Mobile Data 23
Paging 24
Specialized Mobile Radio (SMR) 25
Satellite 26
Wideband systems 27
Local Metropolitan Area Networks (LMDS) 28
Point-to-Point Optical links 29
Wireless Local Area Networks (WLANs) 30

Short range radio 31
Ultrawideband ----- 31
Trend: Increasing Data Rates 32
GSM ----- 32
HSCSD ----- 32
GPRS ----- 32
Wireless LAN ----- 32
Basic PCS network architecture 33
Example of PCS Architecture 34
PCS network architecture supporting Mobility 35
Mobility Management 36
Mobility Management Protocols 37
Macro- vs. Micro-mobility 38
Getting Service 39
Locating the user 40
Handoff Management: Detection & Assignment 41
Handoff/Handover/Automatic Link Transfer 42
Handoff Criteria 43
Handoff Goals 44

When to make the decision? 45
Reality is more complex 46
Who makes the handoff decision? 48
Inter-BS Handoff (aka inter-cell handoff) 49
What happens if there are insufficient resources at new AP? 51
Inter-system Handoff (aka inter-MSC handoff) 52
What happens if the mobile moves gain? 53
Fast Mobile IPv4 handoff via Simultaneous Bindings 55
Fast handover timeline 56
Roaming 57
Roaming Management 59
Roaming example 60
Of course it couldn’t be this simple! 61
Call delivery 62
CT2 63
Back to: Who makes the handoff decision? 64
Network controlled handoff (NCHO) 65

Mobile assisted handoff (MAHO) 66
Mobile controlled handoff (MCHO) 67
Handover Failures 69
Channel Assignment 70
Channel Assignment Process 71
Handoff Management: Radio Link Transfer 72
Handoff frequency 74
Soft handoff in multiple forms 75
Paging 76
Paging Architecture 77
Paging Service area 78
Introduction of paging systems 79
Alphanumeric paging systems 80
Mobile telephone systems 81
Mobile but not necessarily wireless 82
Local mobility via wireless (or redirects) 83
Two-way paging and messaging systems 84
Pager 85

Paging Interworking 86
Paging - link level 87
Motorola’s FLEX™ protocol 88
Sleeping for power savings 89
Mobile Telephone Systems Timeline (the first two generations: analog + digital) 90
References and Further Reading 91
Course book 91
Further details concerning physical and link layer wireless communication 91
CDPD 92
LEO 92
Fixed Broadband wireless 93
User profiles 93
Mobile IP 93
Fast handoff 94
Micromobility: Cellular IP, HAWAII, Hierarchical Mobile IP 94
Comparison of IP Mobility protocols 95
TeleMIP 95
Intersystem Handoff 95
2. Network Signaling and CDPD 96
Lecture 2 (Chapters 5-8) 97
Network Signaling 98

Transaction Capabilities Application Part (TCAP) 99
Transaction 2 (T2) - additional details..... 101
Automatic Code Gapping (ACG) 102
TIA TSB-51: Authentication, Signaling Message Encryption and Voice Privacy 103
MIN and ESN 104
Without-Sharing Scheme..... 105
Without-Sharing Call Origination 106
Sharing Scheme 107
Sharing Call Origination..... 108
When should you use Without-Sharing vs. Sharing..... 109
Cellular Authentication and Voice Encryption (CAVE) Algorithm 110
PACS Network Signalling..... 112
PACS Architecture 113
Access Manager (AM)..... 114
AIN/ISDN Switch..... 115
AIN Service Control Point (SCP)..... 116

PACS Intersystem Handoff 117
3 alternative inter-RPCU handoff methods
(Switch Loopback, Direct Connection, Three-way Calling Connection): 118
CDPD..... 119
Motivation for CDPD 120
Goals..... 121
CDPD network architecture..... 122
CDPD Entities 123
other entities 124
Limits..... 125
Handoffs 126
Connectionless Network Services (CLNS) 127
Roaming Management..... 128
Multicast 129
CDPD Modems..... 130
CDPD usage 131
Operators and coverage maps ---------- 131

CDPD phaseout 132
Ricochet 133
Ricochet System Architecture 134
Further reading..... 135
TIA ---- 135
TSB-51 ---- 135
Mobile*IP ---- 136
CDPD ---- 137
Ricochet---- 138
3. GSM, GPRS, SMS, International Roaming, OAM 139
Lecture 3 140
Global System for Mobile Communications (GSM)..... 141
GSM Requirements 142
GSM Architecture 143
Foundation 144
GSM contributions 145
Distinctive features of GSM 146
Mobile Station (MS) 148
Subscriber Identity Module (SIM)..... 149

Mobile Equipment (ME) 150
Power saving and interference reduction ----- 151
Classmark ----- 152
User ID ≠ Device ID 153
Mobile Terminal (MT) 154
Base Station System (BSS)..... 155
Base transceiver station (BTS) 156
Base station controller (BSC) 157
Network and Switching Subsystem (NSS) 158
Databases 159
Equipment Identity Register (EIR)..... 160
Operation Sub-System (OSS) 161
Operation and Maintenance Center (OMC) 162
GSM Interfaces (just some of them!) 163
GSM Layers..... 165
GSM Air interface 166
A_{bis} interface..... 168
A_{bis} protocols..... 169

A Interface 170
A interface protocols..... 171
GSM Audio..... 173
CODECs ---------- 173
MSC interfaces and protocols..... 174
GSM Logical Channels 175
Traffic channel (TCH) 176
Broadcast channels (BCH) 177
Common control channels (CCCH) 178
Dedicated control channels (DCCH)..... 179
GSM Timing..... 180
Incoming Call 181
Mobility Management (MM)..... 182
Security 183
Cipher mode management- ---------- 183
Authentication 184
Authentication and Encryption..... 185
GSM data rates 186

System engineering..... 187
GSM Network Optimization 188
Optimal Cell Planning 189
Features..... 190
GSM Phase 2+ 191
High Speed Circuit Switched Data (HSCSD) 192
General Packet Radio Service (GPRS)..... 194
GPRS nodes..... 195
GSM/GPRS Architecture and Interfaces 196
GPRS Coding Schemes 197
Unstructured Supplementary Service Data (USSD)..... 198
USSD continued 199
Short Message Service (SMS)..... 200
SMS message types 201
Short Message Service Architecture 202
SM-SCs..... 203
Three kinds of SMSs 204

Entering Short Messages 205
SMS shorthand 206
External Application Interface (EAI) 207
Voice Messaging System (VMS) 208
Voice Profile for Internet Mail (VPIM)..... 209
Enhanced Message Service (EMS)..... 210
Multimedia Messaging Service (MMS) 211
SMS over GPRS 212
International Roaming 213
Enhanced Data Rates for GSM Evolution (EDGE)..... 214
GSM/EDGE Radio Access network (GERAN) 215
EGRPS..... 216
Operation/Administration/Maintenance 217
Further reading..... 218
GSM - - - - - 218
GPRS - - - - - 219
USSD - - - - - 220
SMS and Multimedia Messaging Service (MMS) - - - - - 220
International Roaming - - - - - 222

Operation/Administration/Maintenance - - - 222

4. Number portability, VoIP, Prepaid 223

Lecture 4 224

Database lookups 225

Local Number Portability (LNP) - - - 225

Three kinds of Local Number Portability 226

Mobile Number Portability (MNP) 227

Non-geographic number portability (NGNP) 228

Call forwarding at donor end 229

Drop back forwarding 230

Query on release (QoR) solutions 231

Look up type solutions 232

Two stage solutions 233

All call/all network solutions 234

Who knows the mappings? 235

Nummerportabilitet i Sverige 236

EU Document 398L0061 237

Nortel Networks’ Universal NP Master (UNMP) 238

Lookup engines 239
Voice over IP (VoIP) 240
TIPHON 241
Ericsson's GSM on the Net 242
iGSM 243
Prepaid 244
GSM Prepaid 245
Difference between Mobile and Fixed Prepaid 246
Four alternatives for Mobile Prepaid 247
Wireless Intelligent Network (WIN) 248
Calling party pays vs. Called party pays 249
WIN Call termination when called party pays 250
Service Node 251
Hot Billing 252
"**one-call exposure**" in depth 253
Handset-Based 254
Combined Handset-based + Hot Billing 256

Roaming and Prepaid 257
Further reading 258
Number portability ---------- 258
VoIP ---------- 259
Prepaid ---------- 260
5. WAP, Heterogeneous PCS, 3G 261
Lecture 5 262
Wireless Application Protocol (WAP) 263
WAP Model 264
Push services 265
WAP (first round) Summary 266
WAP 2.0 267
WAP 2.0 new & enhanced services 268
Heterogeneous PCS 269
Similar Radio technologies + Same Network technology (SRSN) 270
Different Radio technologies + Same Network technology 271
Different Radio technologies + Different Network technology 272
Tier Handoff 273

Registration for SRSN & DRSN 274
Registration for DRDN 275
Call delivery 276
User identity (identities) and MSs 277
Major forces driving heterogeneous PCS 278
Third Generation Mobile (3G) 279
Paradigm shifts 280
3rd Generation Partnership Project (3GPP) 281
Third Generation Partnership Project 2 (3GPP2) 282
Mobile Station Application Execution Environment (MExE) 283
MExE Classmark 283
Common Language Infrastructure for MExE devices: Classmark 4 284
Service discovery and management 284
CLI MExE Devices 285
3G Physical Layer 286
Gateway Location Register (GLR) 287
3G QoS 288
UMTS Subscriber Identity Module (USIM) 289

Wireless Operating System for Handsets 290
Mobile Virtual Network Operator (MVNO) 291
πG 292
4th generation?..... 293
Further reading..... 294
WAP - - - - - 294
Heterogeneous PCS - - - - - 294
3G- - - - - 294
6. Wireless Local Loop (WLL) and Enterprise Networks 297
Lecture 6 298
Wireless Local Loop (WLL) 299
Deployment issues 300
WLL Technologies 301
Enterprise Networks 302
Cordless PBXs 303
Virtual enterprise networks..... 304
Remoting the office to where the user is 305

Unified Communications 306
7. Bluetooth 307
Lectures 7 & 8 308
Bluetooth™ 309
Bluetooth protocol stack 310
Physical Layer 311
Transmit Power 312
Masters vs. Slaves 313
Frequency Hop Sequence 314
Time Division Multiplexing (TDM) 315
Network Topology 316
Scatternets 317
Voice + Data support 318
Baseband 319
Baseband Packet formats 320
Baseband Packet formats 321
Synchronization Word Algorithm 322

Security 323
Link Control Protocol (LCP) 324
Link Control states 325
Link Manager 326
Host Controller Interface (HCI) 327
HCI Transport Layer 328
Logical Link Control and Adaptation Protocol (L2CAP) 329
L2CAP Signalling 330
L2CAP Command 331
Configuring a Connection 332
Disconnecting and Timeouts 333
For A to talk to B 334
Service Discovery Protocol (SDP) 335
RFCOMM Protocol 336
RFCOMM Frame Types 337
Telephony Control Signaling (TCS) Protocol 338
Bluetooth Profiles 339

Management 340
Low Power Modes 341
IEEE 802.15 standard 342
Further reading 343
8. WLAN 344
Lecture 9 &10 345
Two possible network configurations 346
Terms 347
IEEE 802.11 Basic Access Method 348
Distribution Coordinating Function (DCF) 349
IEEE 802.11 Frame Format 352
IEEE 802.11 Frame Control 353
Startup, then Join a network 354
Discovery Phase 355
Authentication 356
Wire Equivalent Privacy (WEP) 357
Handoff 358

Inter-Access Point Protocol (IAPP) 359
Fast Handoff 360
Point Coordination Function (PCF) 361
Spacing 362
Timing and Power Management 363
AAA 364
IEEE Extensible Authentication Protocol ---- 364
Roaming 365
Clearinghouse ---- 365
Interconnect Provider ---- 365
Proxies 367
HiperLAN2 368
802.11a and 802.11h 369
Multihop 370
QDMA (quad-division multiple access) 371
All IP networks 372
Space Data Corporation 373
Wireless Internet Service Providers (WISPs) 374

MIT’s AI Lab: Project Oxygen.. 377
Intelligent/Smart Spaces 378
Further reading.. 379
WISPs - 379
IEEE 802.11 - 379
AAA - 380

KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

1. Introduction

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Last modified: 2003.03.13:11:56

Welcome to the course!

The course should be fun.

We will dig deeper into Personal Communication Systems - with a focus on their **architectures**, but we will also examine some of the *protocols* which are used.

Information about the course is available from the course web page:

http://www.imit.kth.se/courses/2G1330/

Staff Associated with the Course

Instructor (Kursansvarig)

prof. Gerald Q. Maguire Jr. <maguire@it.kth.se>

Administrative Assistant: recording of grades, registration, etc.

Rita Johnsson <ritaj@it.kth.se>

Goals, Scope and Method

Goals of the Course

- To understand both what Personal Communication Systems are and their basic architectures.
- To be able to read and understand the literature.
- To provide a basis for your own research and development in this area.

Scope and Method

- We are going to examine a number of different systems to understand both the details of the system(s) and to abstract from these details some architectural features.
- You will demonstrate your knowledge by writing a written report and giving an oral presentation describing your project.

Prerequisites

- Internetwork (2G1305) **or**
- Equivalent knowledge in Computer Communications (this requires permission of the instructor)

Contents

The focus of the course is on personal communication systems and their network architecture. This spans the range from piconets to space probes, but the emphasis will be primarily focus on the range from LEO satellites down to personal area networks.

The course consists of 10 hours of lectures and a project of ~50 hours effort.

Topics

- Personal Communication Systems (PCS): handoff, mobility, paging
- CDPD
- GSM, GPRS, SMS, International Roaming, Operation/Administration/Maintenance
- Number portability, VoIP, Prepaid
- WAP
- Heterogeneous PCS
- Wireless Local Loop (WLL), Enterprise Networks
- Bluetooth, Piconets, Scatternets
- Wireless Local Area Networks (WLANs)

Examination requirements

- Written and Oral project reports

Grades: U, 3, 4, 5

Project

Goals: to gain analytical or practical experience and to show that you have mastered some knowledge in this area and to encourage you to find a topic which interests you (since this will motivate you to really understand the material)

- Can be done in a group of **1 to 3** students (formed by yourself). **Each** student must contribute to the final written and oral reports.
- Discuss your ideas about topics with the instructor **before** starting.

Assignment Registration and Report

- Registration: 4 April 2003, to <maguire@it.kth.se>
  - Group members, leader.
  - Topic selected.
- Written report
  - The length of the final report should be 10 pages (roughly 5,000 words) for each student.
  - The report may be in the form of a collections of papers, with each paper suitable for submission to a conference or journal
  - Contribution by each member of the group - must be clear (in the case where the report is a collection of papers - the role of each member of the group can be explain in the overall introduction to the papers.
  - The report should clearly describe: 1) what you have done; 2) who did what; if you have done some implementation and measurements you should describe the methods and tools used, along with the test or implementation results, and your analysis.

Final Report: written report due **2 June + oral presentations: 5th and 6th June**

- Send email with URL link for a **PDF** or **PostScript** file to <maguire@it.kth.se>
- Late assignments will not be accepted

Note that it is permissible to start working *well in advance* of the deadlines!

Literature

The course will mainly be based on the book: *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0.

Although we will not focus on Mobile IP in the lectures (since an introduction was given in the internetworking course), if you want to do a project which involves mobility, the following two books are useful sources:

- Charles E. Perkins, *Mobile IP: Design Principles and Practices*, Addison-Wesley, 1998, ISDN 0-201-63469-4.
- James D. Solomon, *Mobile IP: the Internet Unplugged*, Prentice Hall, 1998, ISBN 0-13-856246-6.
- *http://www.ietf.org/html.charters/mobileip-charter.html*

We will refer to other books, articles, and RFCs as necessary - see notes and web.

In addition, you will be searching & reading the literature in conjunction with your projects. Please make sure that you properly reference your sources in your report.

Lecture Plan

- Lecture 1: Introduction
  - Course arrangement
  - Personal Communication Systems (PCS): handoff, mobility, paging (Chapters 1-4,22)
- Lecture 2 (Chapters 5-8)
  - CDPD
- Lecture 3
  - GSM (9,10,11), GPRS (18), SMS (12), International Roaming (13), Operation/Administration/Maintenance (14)
- Lecture 4
  - Number portability (15), VoIP (16), Prepaid (17)
- Lecture 5
  - WAP (19), Heterogeneous PCS (20), 3G(21)
- Lecture 6
  - Wireless Local Loop (WLL) (23), Enterprise Networks (24)
- Lectures 7 & 8
  - Bluetooth, Piconets, Scatternets
- Lecture 9 &10
  - Wireless Local Area Networks (WLANs)

Context of the course

Personal Communication Systems have been both increasing their number of users and increasing the variety of personal communication systems. Some of these system (such as GSM) have had growth rates of millions of new customers each month!

Europe is in the process of introducing so-called third generation (3G) cellular systems. In many countries the license fees alone are many thousand of euros per potential customer.

There are discussions of what Theo Kanter calls πG systems[1].

There is even discussion of **if** there will be a 4th **generation** of cellular systems or **if** we will see the end of *generational* architectures and systems.

1. Because $3 < \pi < 4$ and π is an irrational number.

(Chapters 1-4, and 22)

Chapter 1: Introduction

Chapter 2: Mobility Management

Chapter 3: Handoff Management: Detection and Assignment

Chapter 4: Handoff Management: Radio Link Transfer

Chapter 22: Paging Systems

Internet Architecture

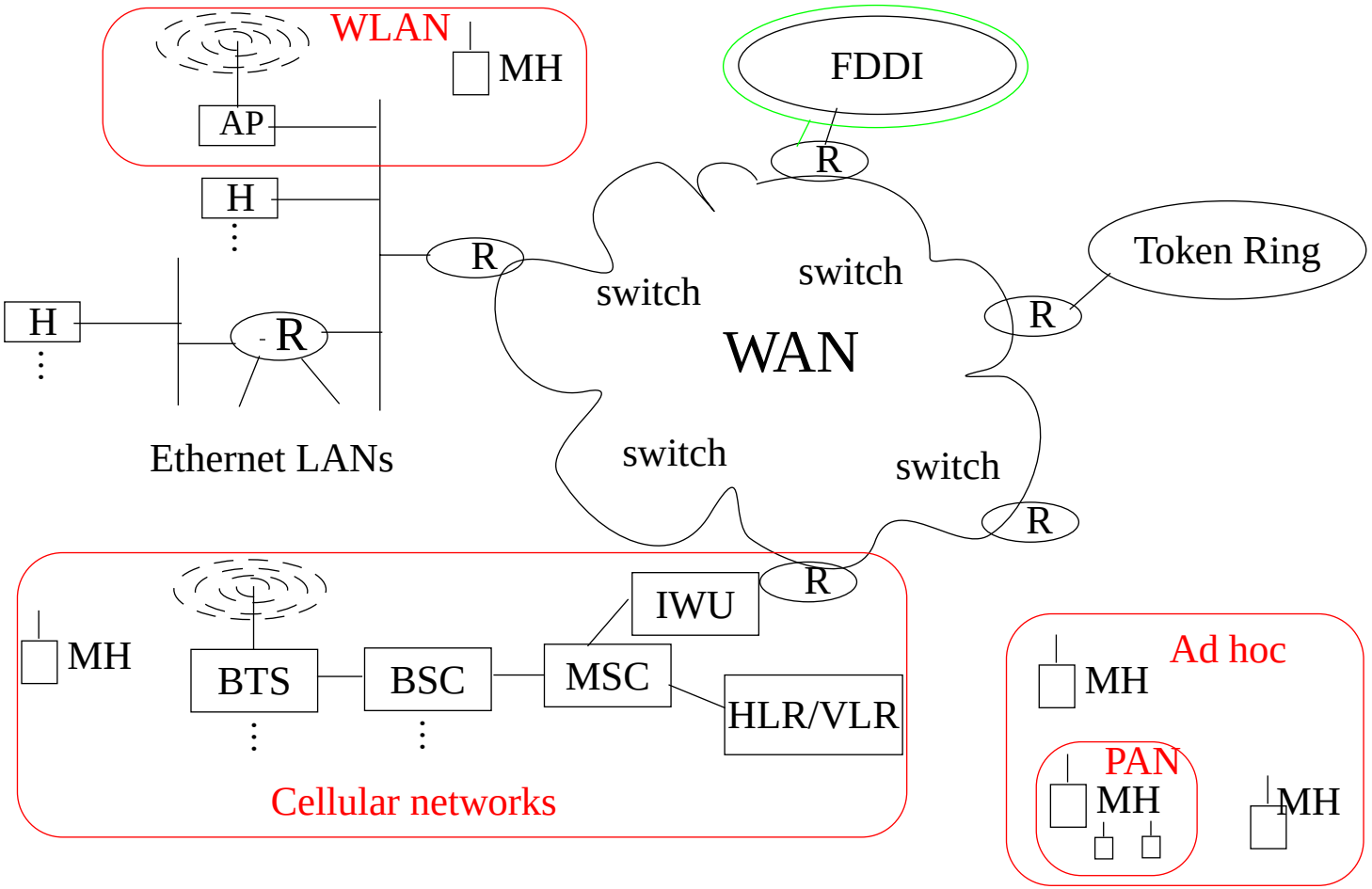


Figure 1: Multiple network technologies - *internetworked* together

More complete Architecture

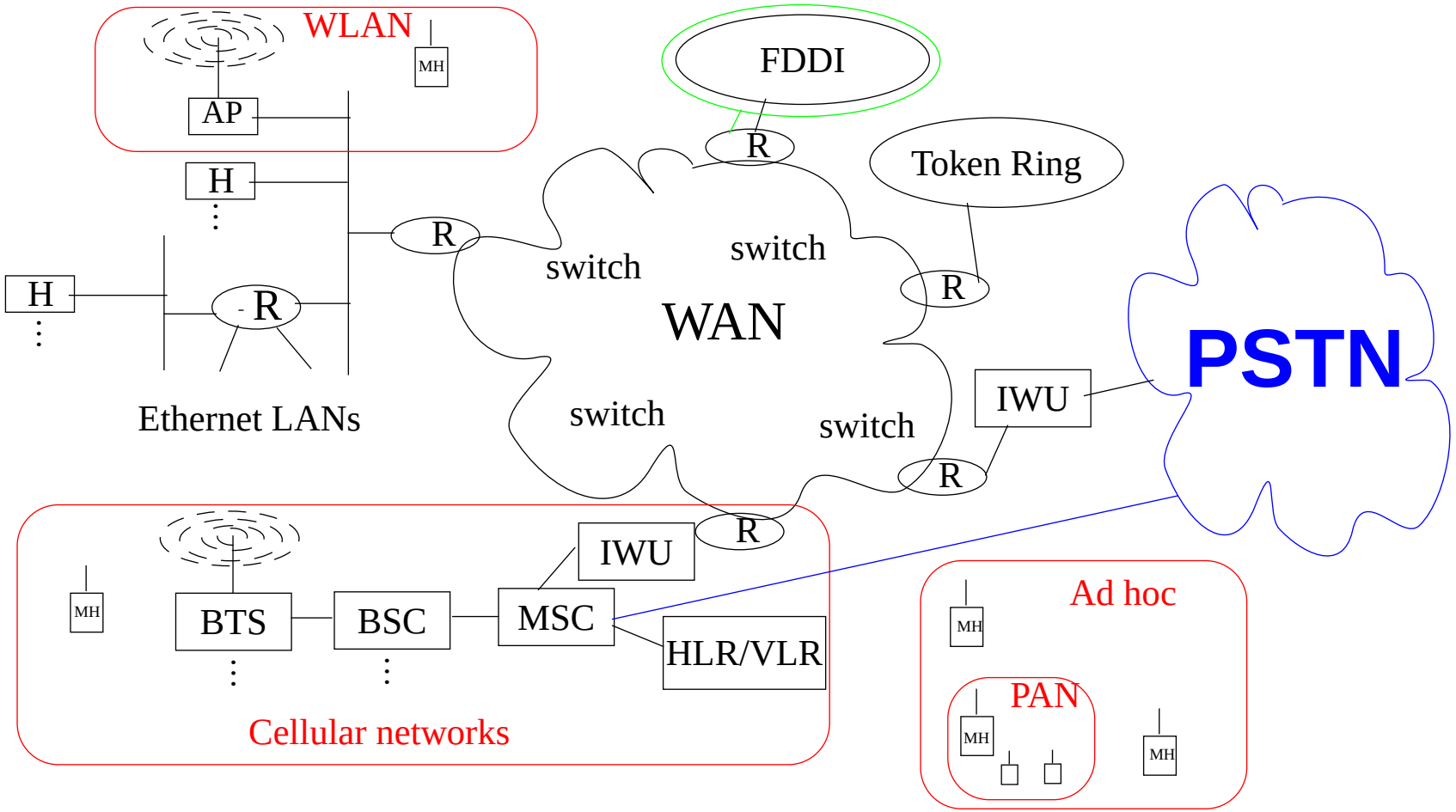


Figure 2: Internet and PSTN

- We will focus on the parts marked in red in the above figure, i.e., Cellular, WLAN, and PAN (and Ad hoc) networks.

Internetworking

Internetworking is

- based on the interconnection (concatenation) of multiple networks
- accommodates multiple underlying hardware technologies by providing a way to interconnect **heterogeneous** networks and makes them inter-operate.

Most of the systems discussed in the course textbook are interconnected to the Public Switched Telephony System (PSTN) - thus there was generally an adaptation to fixed rate (64 kbps) voice coding. Increasingly these systems are also interconnected to the Internet, hence packet based services are becoming an increasingly important part of such systems. In the lectures we will discuss the effects of these interconnections.

Personal Communication Systems (PCS)

The goals of PCS are to provide a mobile user with voice, data, and multimedia at any place, at any time, and in any format.

Thus the system has to *either* provide **universal coverage** or it has to include **interworking with other communication systems**. Thus far, attempts at providing universal coverage by a **globally standard system** have failed (for various technical, historic, economic, and political reasons).

The market has often been fragmented based on: **wide area coverage** (especially for business users), **enterprise** (focused on in-building and on campus), and **homes** (often equated with "personal or free-time usage"). However, this market separation is increasingly **converging** rather than further diverging.

Traditionally, various PCS systems were connected to the Public Switched Telephony System (PSTN) and driven by telephony standards (and at the rate of change of telephony standards). Today, these systems are increasingly connected to the internet and driven by the internet standards & change at internet speeds.

High Tier and Low Tier Cellular, and Cordless

Generally the PCS market has been divided into these three classes:

System	High Tier Cellular	Low Tier Cellular	Cordless
Cell size	large (0.25-38km)	medium (10-100m)	small (10-20m)
User speed	high (≤ 260 km/h)	medium (≤100km/h)	low (≤50km/h)
Handset complexity	high1	low	low
Handset power consumption	high (100-800mW)	low (5-20mW)	low (5-10mW)
Speech coding rate	low (8-13kbps)	high (32kbps)	high (32kbps)
Delay or latency	high (≤600ms)	low (≤10 ms)	low (≤10ms)
Costs	high	medium	low (often flat rate)
Examples	GSM, D-AMPS, PDC, cdmaOne, …	CT2, DECT, PHS, PACS	

Cellular Telephony

Different means of defining channels:

- **F**requency **D**ivision **M**ultiple **A**ccess (FDMA)
  - Advanced Mobile Phone Service (AMPS)
- **T**ime **D**ivision **M**ultiple **A**ccess (TDMA)
  - D-AMPS, Global System for Mobile Communications (GSM)
- **C**ode **D**ivision **M**ultiple **A**ccess (CDMA)
  - IS-95 (developed by Qualcomm)

Low Tier Cellular and Cordless Telephony

- **C**ordless **T**elephony, second generation (CT2) - 40 FDMA channels, within each 100kHz frequency channel the base station⇒user (**downlink**) and user⇒base station (**uplink**) channels are separated with time division duplexing (TDD) (in every 2ms long **frame** there is 64bits of downlink user data followed by 64 bits of uplink user data).
  - Does not support handoffs, primarily supports out-going calls (incoming calls are hard as there is no defined mobility database).
- **D**igital **E**nhanced **C**ordless **T**elephony (formerly **D**igital **E**uropean **C**ordless **T**elephony) (DECT) - utilizes a picocellular design using TDMA with 24 time slots (generally allocated as 12 voice slots for downlink and 12 voice slot for uplink, i.e., TDD) per frequency channel and 12 frequency channels, automatic dynamic channel allocation based on signal strength measurements, a call can move from one time slot in one frequency channel to another time slot in another channel - supporting seamless handoffs.

- **P**ersonal **H**andy Phone **S**ystem (PHS) - another TDMA TDD system also supporting dynamic channel allocation - it has been used in Japan to for a public low tier cellular system.
- **P**ersonal **A**ccess **C**ommunications **S**ystem (PACS) - a TDMA system supporting both TDD and frequency division duplex (FDD); it utilized **m**obile-**c**ontrolled **h**and**o**ff (MCHO). It supports both circuit switched and packet switched access protocols.

Mobile Data

- RAM Mobile Data (now Cingular Interactive, based on the swedish Mobitex system)
  - Backbone behind Xpress Mail with **BlackBerry**, Interactive Messaging PLUS, and Wireless Internet PLUS, … (*http://www.cingular.com/business/mobitex_map*)
  - Coverage maps: http://www.mobitex.org/resources/coverage.html
  - Mobitex had greater national coverage[1] 90% of Sweden and 99.5% of the population, than even the analog 450Mhz cellular system, because the swedish military used it.
  - Both public Mobitex systems (such as that operated by Telia, now Multicom Security AB) and private systems (such as the one at Arlanda Airport).
- **A**dvanced **R**adio **D**ata **I**nformation **S**ystem (ARDIS) {developed for IBM's customer engineers ⇒ offered indoor coverage} (now Motient)
- **C**ellular **D**igital **P**acket **D**ata (CDPD) {developed to provide data as an overlay on analog cellular systems; based on Mobile IP}

Generally low rate systems 2.4 - 8 kbps

1. (see *http://www.mobitex.telia.com/taeckning.htm*)

Paging

Within local paging areas or via satellite.

The key to paging device's high performance is that they **sleep** *most of the time*.

North America utilizes two way paging systems (i.e., the paging system can both send and receive traffic).

Due to the lack of allocation for a return channel two way paging languished in Europe.

Specialized Mobile Radio (SMR)

Taxis dispatching, fleet dispatching, …

The basis for Nextel (*http://www.nextel.com/*) - using a handset built for them by Motorola to operate over the wide variety of SMR channels which Nextel bought (this is a case where the radio design came *after* the frequencies were "assembled").

Satellite

Especially **L**ow **E**arth **O**rbit **Satellite** (LEO)

- numerous attempt to field systems - one problem is that most of the time the satellites are over regions {primarily oceans} with few possible customers. Also each satellite is only are in range for ~10 minutes or so - so there are frequent handoffs.
- 500 - 2000 km orbit
- US DoD Enhanced Mobile Satellite Service (EMSS) {successor to Iridium, features secure phones and US government secure voice gateway}

The footprint (i.e., coverage area of a satellite transponder) for **M**id-**e**arth **o**rbit (MEO) and **Geo**stationary (GEO) satellite - generally cover too large an area and does so with very long delays (due to the distance of these satellites from the earth). However, they are widely used for both their wide coverage area (for example, for paging) and for one way services (often broadcast or spot coverage).

Wideband systems

- Wideband Code Division Multiple Access (WCDMA)
  - With data rates in rural areas 1.44kbps, in cities 384kps, and indoors up to 2 Mbps
  - *http://www.ericsson.com/technology/WCDMA.shtml*
  - aka UMTS terrestrial radio access (UTRA)
- cdma200
  - aka IS-2000 an evolution of cdmaOne/IS-95 to 3rd generation services
  - CDMA2000 1X, an average of 144 kbps packet data; 1XEV-DO up to 2 Mbits/sec.; 1XEV-DV even higher peak rates - simultaneous voice and high speed data + improved QoS
- TD-SCDMA - **one** of the chinese 3G standards
  - *http://www.tdscdma-forum.org/nenglish/index.html*

See also:

- 3rd Generation Partnership Project (3GPP) *http://www.3gpp.org/*
  - based on evolved GSM core networks and the radio access technologies
- Third Generation Partnership Project 2 (3GPP2) *http://www.3gpp2.org/*
  - ITU's "IMT-2000" initiative:
    - high speed, broadband, and Internet Protocol (IP)-based mobile systems
    - "featuring network-to-network interconnection, feature/service transparency, global roaming and seamless services independent of location."
  - including cdma2000 enhancements

Local Metropolitan Area Networks (LMDS)

Point-to-point or Point-to-multipoint (generally wide band) links

- some operators have more than 700MHz worth of bandwidth available (in aggregate) in a given market (geographic) area
- line-of-sight coverage over distances up to 3-5 kilometers
- data rates from 10s of Mbps to 1Gbps or more
  - Ericsson's MINI-LINK BAS up to 37 Mbit/s per sector
    http://www.ericsson.com/transmission/wba/
- Frequency bands between 24 to 31 GHz (licensed spectrum)
  - UK: 28 GHz band and 10 GHz band
  - Rest of Europe: 26 GHz band
  - US: 24 GHz used by Teligent and 39 GHz band licensed by Winstar
    - at least one experimental license in the US in 41.5 GHz to 43.5 GHz
  - Biggest problem is price of such high frequency components!

For further info see: *http://www.lmdswireless.com/* and

http://www.networkcomputing.com/netdesign/1223wireless13.html

See also the recent IEEE 802.16 standard for fixed Broadband Wireless Access (BWA) systems in the 10 to 66 GHz - to try to facilitate interoperability.

Point-to-Point Optical links

Free-Space Optics (FSO)

- using laser light sources it is possible to achieve very high speeds (typically OC-3 (155Mbps), OC-12 (622Mbps), or 1.25Gbps; but some systems at 2Gbps and 10GBps) for such point-to-point links
- uses Terahertz (THz) spectrum range
- short ranges - typically below 2km

See also: *http://www.comm.toronto.edu/woc/freesp/terrestrial.html*

Wireless Local Area Networks (WLANs)

- **F**requency **H**opping **S**pread **S**pectrum (FH-SS)
- **D**irect **S**equence **S**pread **S**pectrum (DS-SS)
- **O**rthogonal **F**requency **D**ivision **M**ultiplexing (OFDM)
- IR links

Most of the radios have either used the **I**nstrumentation, **S**cientific, and **M**edical (ISM) bands, **N**ational **I**nformation **I**nfrastructure (NII) bands, or the HiperLAN band.

Data rates have ranged from 100s of kbps to 54 Mbps.

See IEEE 802.11 (in its many variants) - some of the standards are available at (those published more than 6 months ago are free):

http://standards.ieee.org/getieee802/

Short range radio

low speed wireless links (door locks, wireless sensors, RF ID tags, …)

Personal Area Networks (PANs) - these have generally be relatively low data rate systems, such as Bluetooth (1Mbps in aggregate).

Ultrawideband

- US FCC gave regulatory approval 14 Feb. 2002
- Intel demo'd transmitter and receiver at 100Mbps
- they expect to be able to get 500Mbps at a few meters dropping to 10Mbps at 10m.

Trend: Increasing Data Rates

GSM

- 14.4kbps per channel

HSCSD

- combining multiple GSM channels to achieve a higher aggregate rate for a single user

GPRS

hundreds of kbps - by using the GSM time slots in a packet oriented manner

Wireless LAN

- 802.11 Wireless LAN - 11Mbps headed for 54 Mbps
- 802.15 Wireless Personal Area Network (WPAN) ~1Mbps
- 802.16 Metropolitan Area Networks - Fixed Broadband Wireless (10 .. 66 GHz) 10s to 100s of Mbps/channel

Basic PCS network architecture

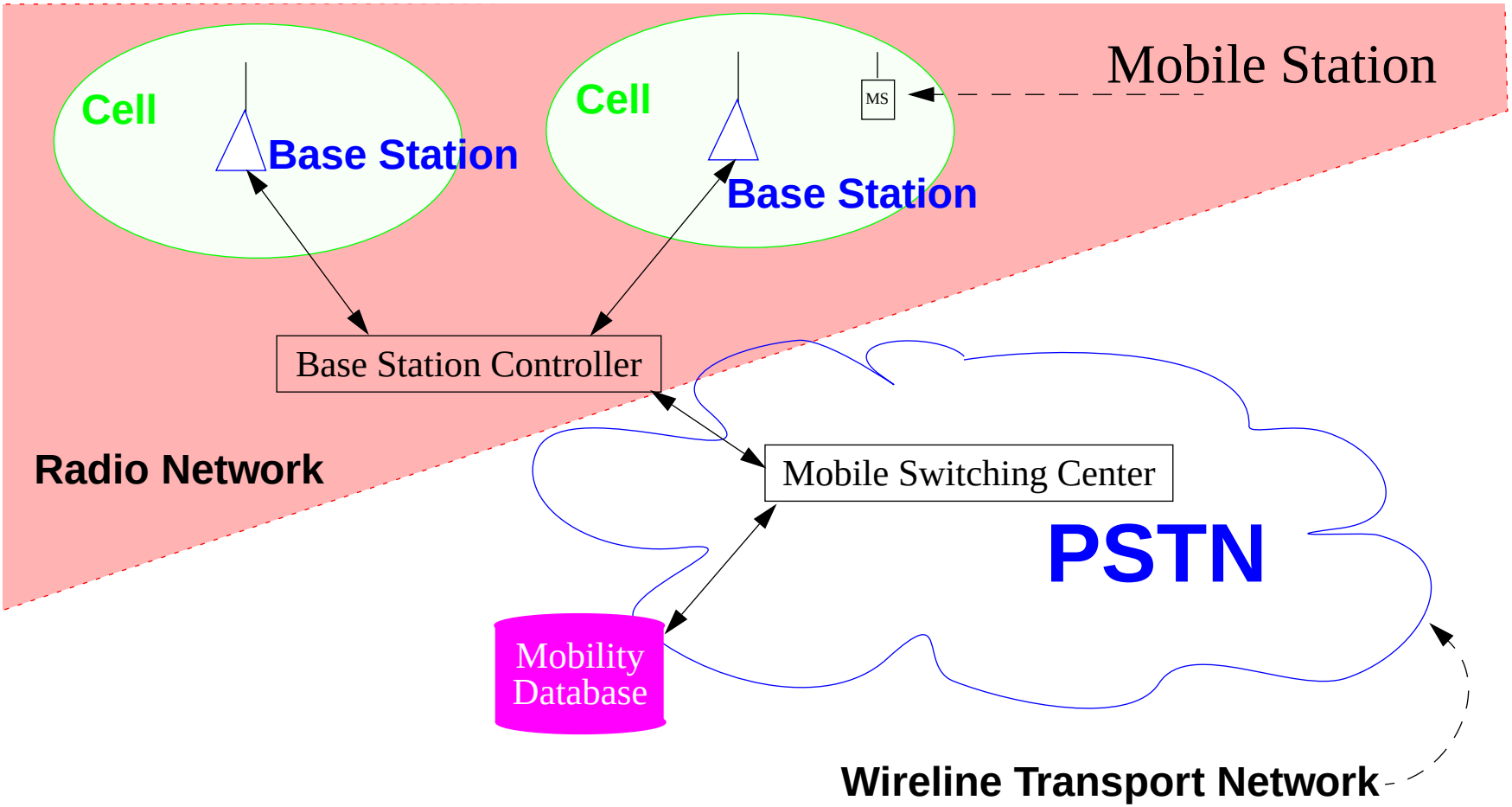


Figure 3: Basic PCS network architecture

Example of PCS Architecture

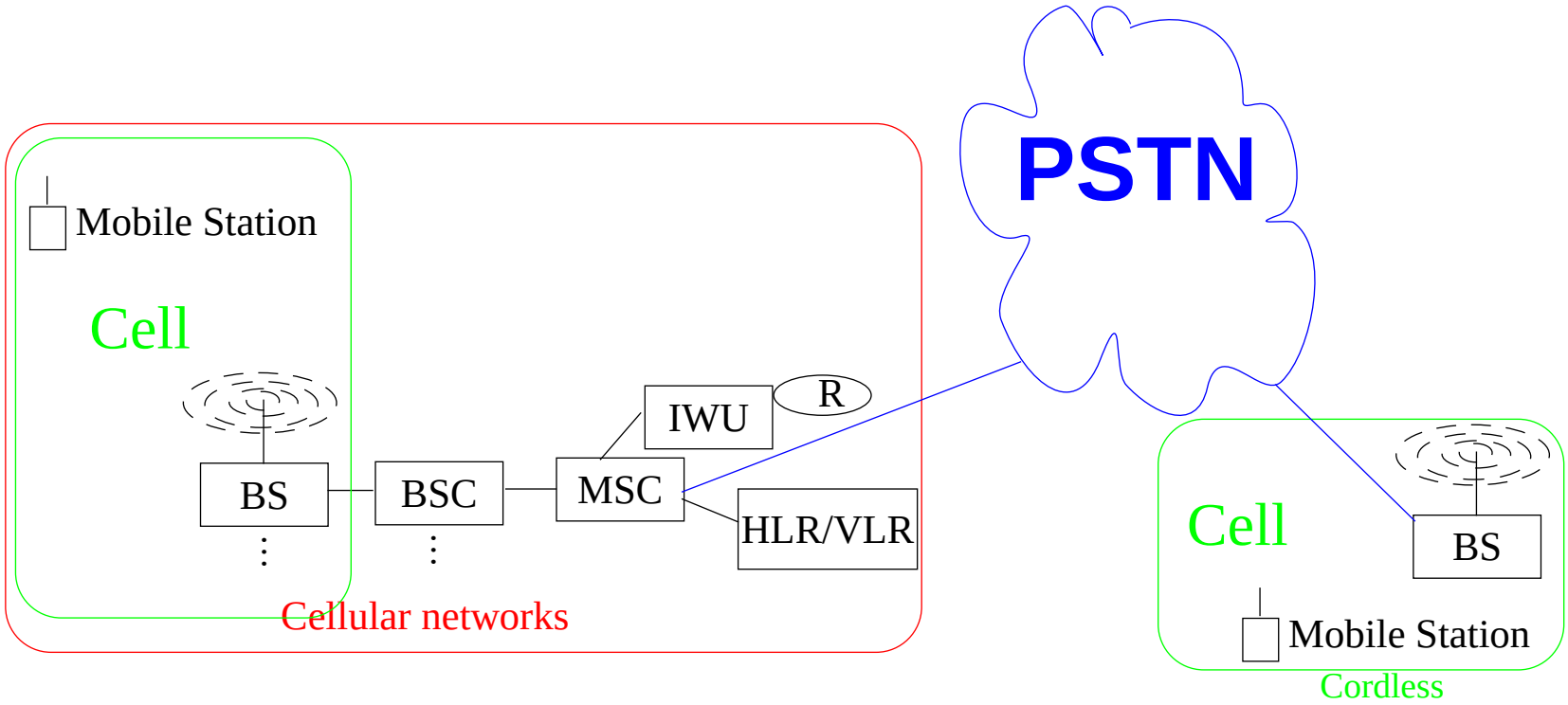


Figure 4: Cellular and Cordless networks

B(T)S = Base (Transceiver) Station, **BSC** = Base Station Controller, **MSC** = Mobile Switching Center, Home Location Register (**HLR**)/Visitor Location Register (**VLR**) provides a Mobility Database, and the PSTN provides the wireline (**backhaul**) transport network.

PCS network architecture supporting Mobility

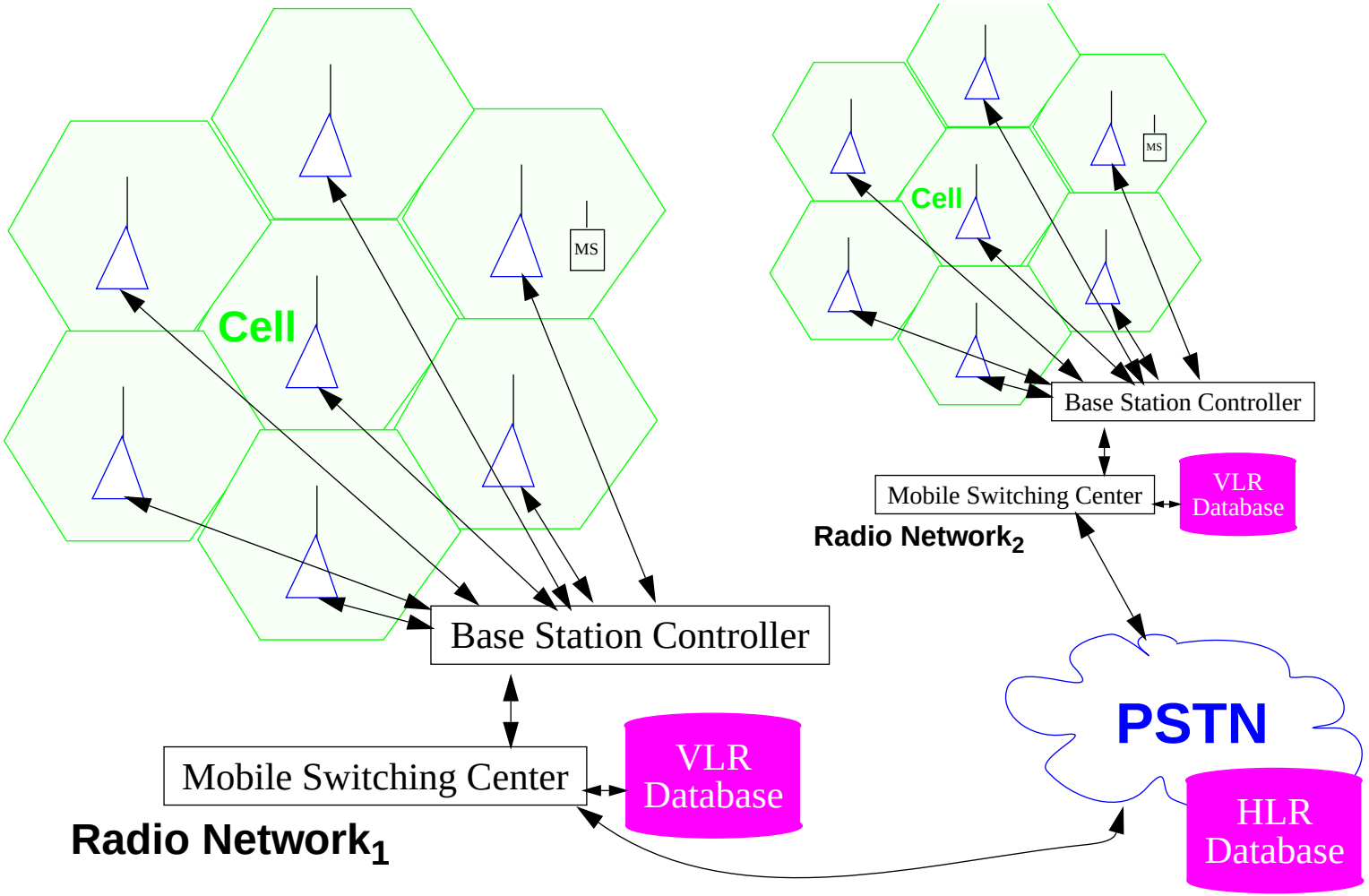


Figure 5: Basic PCS network architecture

Mobility Management

If mobile only **originates** traffic, then you don't have to know where the mobile is *to send traffic to it* - but rather you only have to decide if you will give it service.

If a mobile is to **receive** traffic (without having originated traffic), then someone must know where to send this traffic. This someone can be:

- a server **in** the network (where the user is)
- a server **attached** to the network (where the user is)
- a server **attached to another network** (different from where the user is right now)

We will examine mobility management with respect to the **static** decision of where to send traffic, the **dynamics** of maintaining communication despite change in access points (**Handoff**), and the use **paging** (both in conjunction with mobility management, as an alternative architecture, and as a component of other architectures).
See also: §1.4 The Essential Challenge of Mobility Management [31]

Mobility Management Protocols

Include:

- Mobile IP
- EIA/TIA Interim Standard 41 (IS-41 or ANSI-41)
- Global System for Mobile Communications (GSM) Mobile Application Part (MAP)

Macro- vs. Micro-mobility

Macro-mobility == Inter-domain mobility
(a domain is {as usual} a single administrative entity)

Micro-mobility == Intra-domain mobility

Another way of looking at it is that in micro-mobility entities outside of the current domain can not (and need not) see any changes when the mobile moves **within** the domain, while with macro-mobility others can see when a mobile moves, even within a domain.

Getting Service

Once a mobile's identity is know, the policy question is: Should this mobile get service?

The policy question and its answer may involve:

- roaming agreements (generally reciprocal agreements),
- current traffic loads,
- anticipated traffic loads,
- mobile user's priority/class/… ,
- … .

The question of authentication, authorization, and accounting (AAA) for mobile users are topics of a recent thesis: Juan Caballero Bayerri and Daniel Malmkvist, *Experimental Study of a Network Access Server for a public WLAN access network*, M.S. Thesis, KTH/IMIT, Jan. 2002.

See also IEEE 802.1x Port Based Network Access Control
http://www.ieee802.org/1/pages/802.1x.html

Locating the user

- we can **track** the user continuously, or
- we can start looking for the user where we last saw them and then expand our **search**, or
- we can **guess** where the user might be - based on their patterns of movement (past behavior)
- the **user tells us** where they are
  - based on a **schedule** the user can tell us where they are (e.g., every one minute tell the system where you are now) or
  - the **user can listen** for something which causes them to check in (for example a page) or to report their location

Handoff Management: Detection & Assignment

- Who initiates handoff?
- How do you detect that you should handoff?
- **Handover** (Europe) ≡ **handoff** (North America)

Handoff/Handover/Automatic Link Transfer

Handoff is the process that occurs when a mobile is “handed over” from one access point to another, i.e., the access point which the mobile is using changes. This is generally one of several types:

soft handoff	the mobile can communicate with both the **old** and the **new** AP[a]
hard handoff	the mobile can only communicate with one AP or the other
seamless handoff	If neither the user nor running applications notice the handoff (i.e., there is *no effect on content of data streams* coming arriving to or departing from the mobile)[b] (includes both smooth and fast handoffs)
glitchless handoff	in this case the delays due to the handoff are hidden/eliminated from the data stream
smooth handoff	buffering of traffic to the mobile when it is in the process of changing from one AP to another is buffered and then delivered to the new AP[c]
fast handoff	only a short interruption time between disconnection at the old AP and connection to the new AP
vertical handoff	when the new cell is larger than the current cell (i.e., microcell to macro cell)
horizontal handoff	when the new cell is similar to the current cell (i.e., microcell to micro cell)

a. Generally I will refer to such devices as access points, except when their being a Base Station is particularly important.

b. For seamless and glitchless handoffs see for example, work by R. Cáceres and V.N. Padmanabhan.

c. See C. Perkins and K-Y. Wang’s scheme for buffering with Mobile IP, requires per mobile buffering associated with the (former) access points.

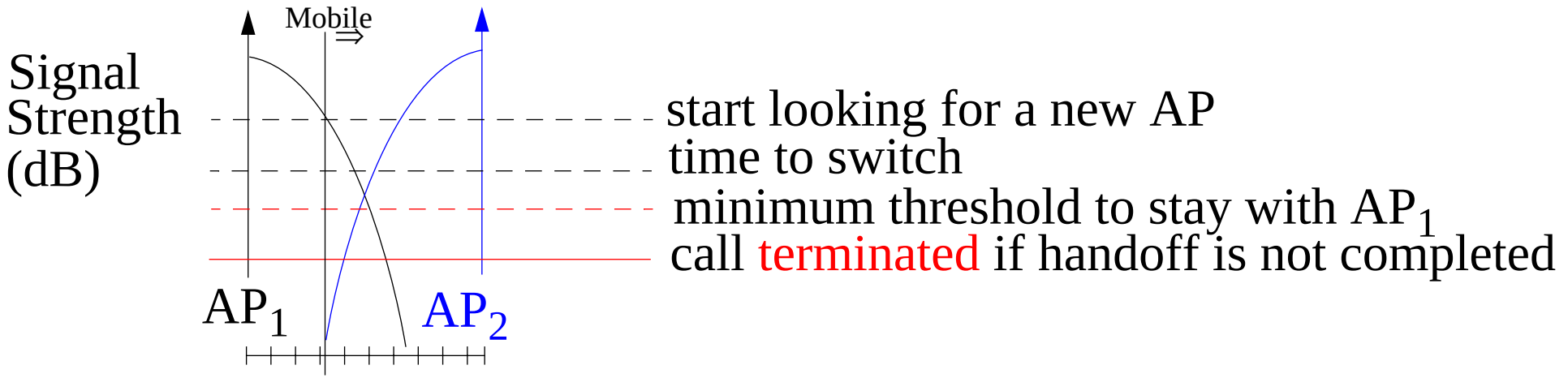
Handoff Criteria

Signal quality - due to its effect on the ability to deliver data via the link

Data quality - the effect of errors on the delivered traffic

With respect to signal quality we can exploit knowledge of general radio signal properties or we can exploit specific situation knowledge (based on our earlier experience or the experience which other mobiles have reported and which we have learned).

A simplified view with respect to signal strength (reality is much more complex):

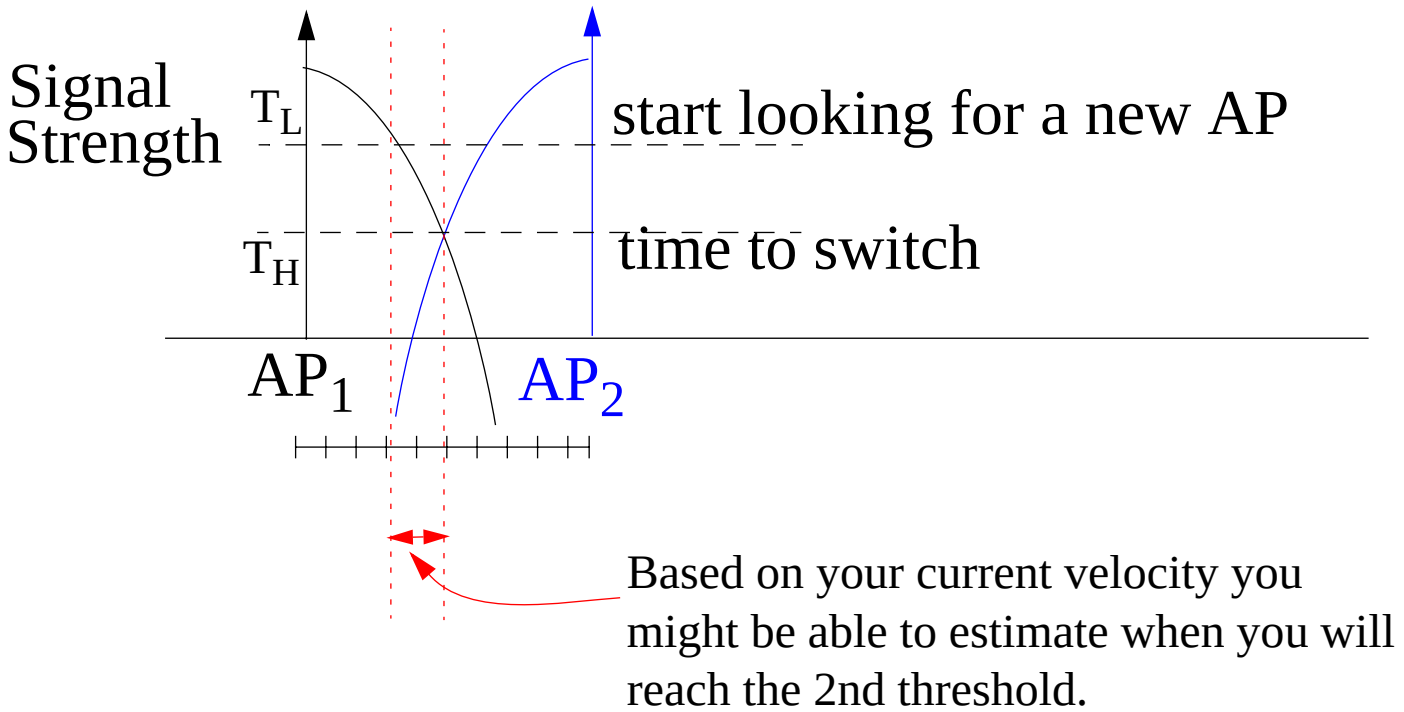


Handoff Goals

- minimal impact on traffic - making a handoff at the “right” time
- tolerance/adaption for congestion and capacity - the new and old cells may have different levels of utilization, available bandwidth, … - handoff has to deal with this
- efficiency - the handoff should result in improved efficiency (in terms of traffic, energy consumption, reduced interference, …) - this, of course, means that the handoff process itself should try to minimize the resources it consumes
- improve availability - handoff should result in using an AP which provides better bandwidth, lower cost, lower delay, low delay variance, …
- the mobile should be able to use the maximum set of APs (which may involve changing spreading code, modulation, coding, … or changing to a different radio module) in order to achieve a better system optima, rather than be restricted to a local single system optima

When to make the decision?

By starting to look for a new AP **before** you need it, there is time to make a decision:



T_L - Threshold for **Looking** around, T_H - threshold for **Handoff**

Reality is more complex

The Mobile Station (MS) and the Base Station (BS) experience a channel which varies - due to user movement, movement of other users, reflections, diffractions, … :

- Rapid-fading
  - Rayleigh-distributed envelope of the signal strength (often called Multipath fading)
  - If there is also a light-of-sight component, then the distribution is Rician
- Slower fading
  - Shadow fading - a lognormal distribution

Three common measurements of the channel:

- **W**ord **E**rror **I**ndicator (WEI) - based on the receiver being able to decode the received signal correctly
- **R**eceived **S**ignal **S**trength **I**ndication (RSSI) - a measure of the received signal strength (in units of dB)
- **Q**uality **I**ndicator (QI) - related to the signal to interference & noise ratio (S/I) (in units of dB)

As the channel is varying in time and making the measurements takes time - various techniques are used to filter the RSSI and QI measurements:

- window averaging - simply average the last w measurements
- leaky-bucket integration - a simple one-pole low-pass filter

Various schemes exist to try to combat channel problems:

- **diversity techniques** (frequency hopping, multiple receivers, multiple correlators with variable delay lines, multiple antennas, …)
- **signal processing techniques** (bit interleaving, convolutional coding, equalizers, …)

For further information about these techniques - see: [2] .. [6].

Who makes the handoff decision?

- **N**etwork **c**ontrolled **h**andoff (NCHO) - the network makes the decision
  - used in CT-2 Plus and AMPS
- **M**obile **a**ssisted **h**andoff (MAHO) - the mobile provides data which the network uses to make the decision
  - used in GSM and IS-95 CDMA
- **M**obile **c**ontrolled **h**andoff (MCHO) - the mobile decides for itself
  - used in DECT, PACS, Mobile IP
    - **forward handoff** - mobile initiates handoff and sends the request to the ***new*** AP
    - **backward handoff** - mobile initiates handoff and sends the request to the ***old*** AP

Inter-BS Handoff (aka inter-cell handoff)

When both cells are connected to the same MSC the mobile node (MN) can signal that it is going to change cells and identifies the new cell, then the MSC sets up the correct resources in the new cell, and can now deliver traffic to the mobile's new cell. In telephony systems this often involves setting up a "bridge" to copy traffic to both the new and the old channels.

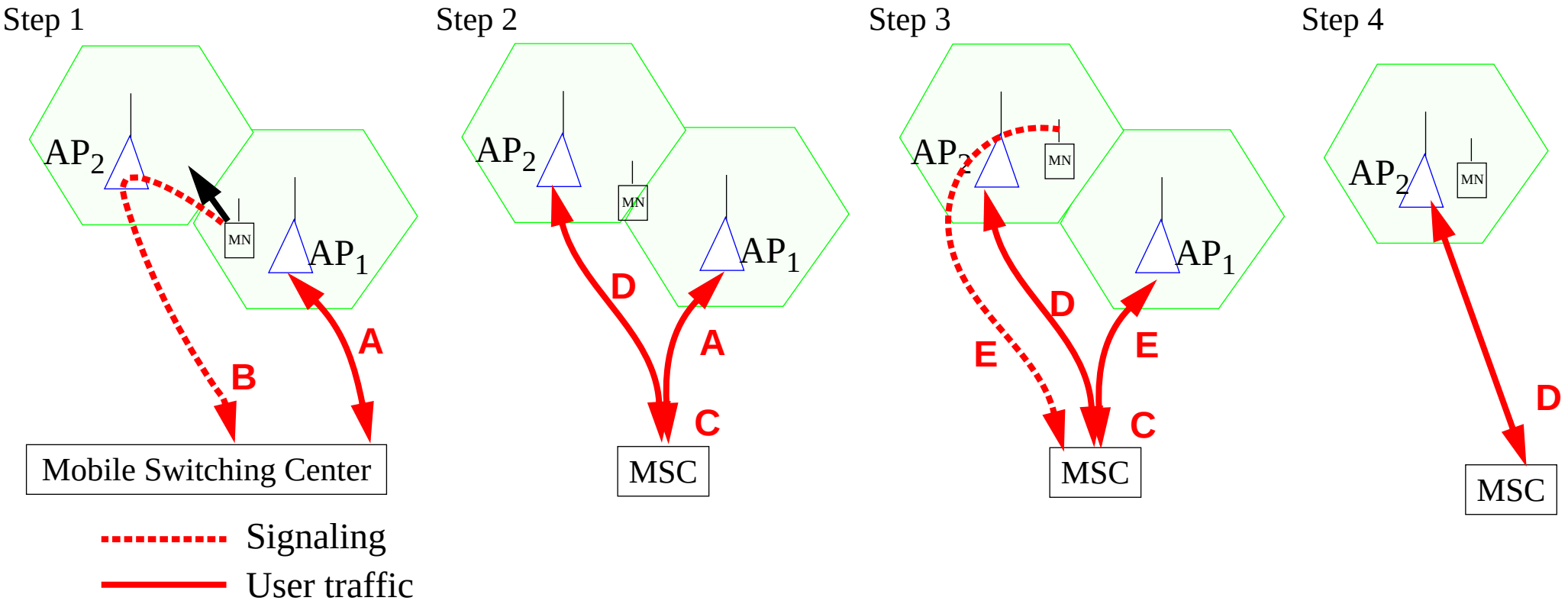


Figure 6: Steps in handoff within the control of one MSC (not showing the BSC)

1. Mobile (MN) is using AP_1, all traffic is going via a channel (A) between MSC (via BSC) and AP_1; MN signals via AP_2, its intention for upcoming handoff (via B)
2. MSC creates a bridge (C) and traffic is now sent via both channels (A) and (D)
3. MN signals (via E) that it is ready to use channel D
4. MSC eliminates bridge C and frees channel A, the MN now uses only channel D.

What happens if there are insufficient resources at new AP?

Nonprioritized scheme (handoffs are treated the same as new calls)

- handover is blocked - keep using the existing channel until either:
  - call is over or
  - link fails (or forced termination)

To reduce forced termination and improve “call completion”:

- **Reserved channel scheme** - keep some resources available for handovers (i.e., under commit)
- **Queuing priority scheme** - exploit cell over lap (called a “handover area” if it exists) to enqueue mobiles waiting for handover
- **Subrating scheme** - downgrade an existing call in the new cell and split the resources with the call being handed over ($\Rightarrow$ the call being handed over is also downgraded). Downgrading often involved changing from a full-rate to a half-rate CODEC.

Some operators base their decision on what to do on **how valuable the handoff customer is** vs. current customers being served in the new cell, i.e., high value customers can cause existing calls of other customers to be terminated.

Inter-system Handoff (aka inter-MSC handoff)

When the two cells are connected to different MSCs the situation is more complex.

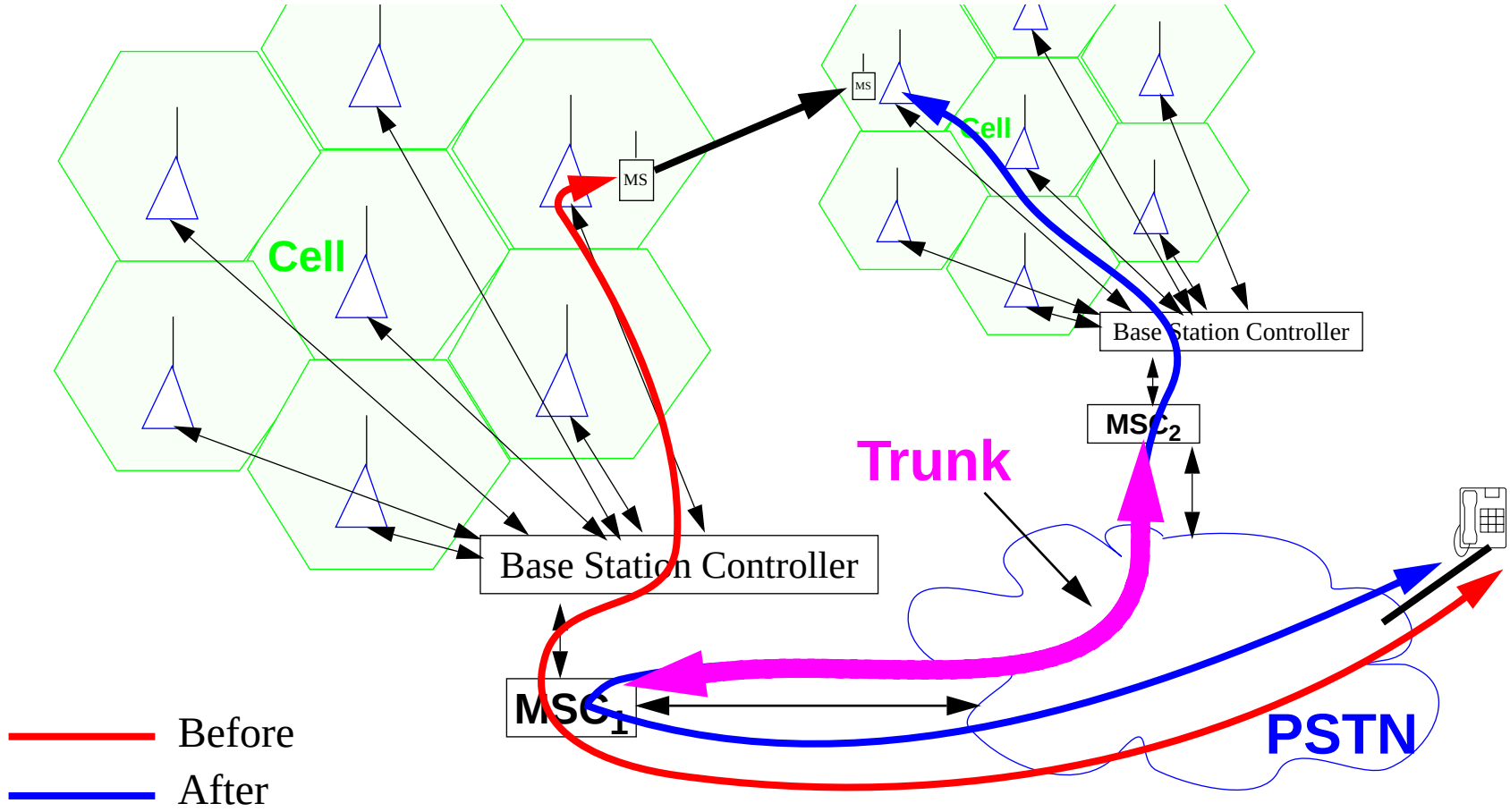
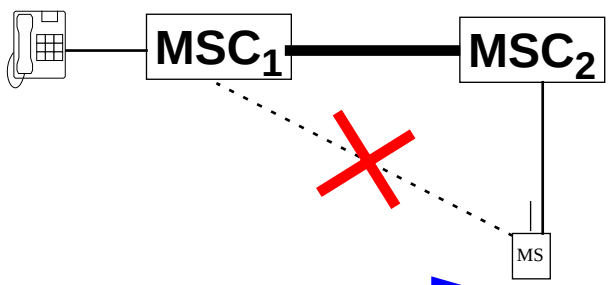
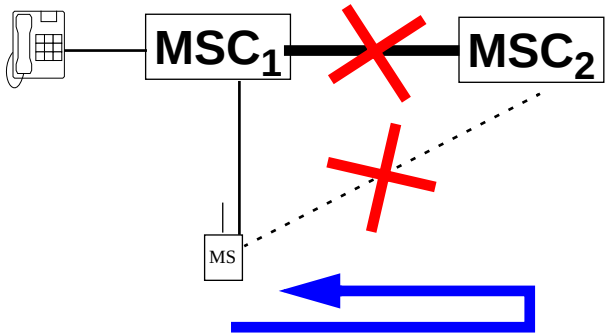


Figure 7: Handoffs between two MSCs

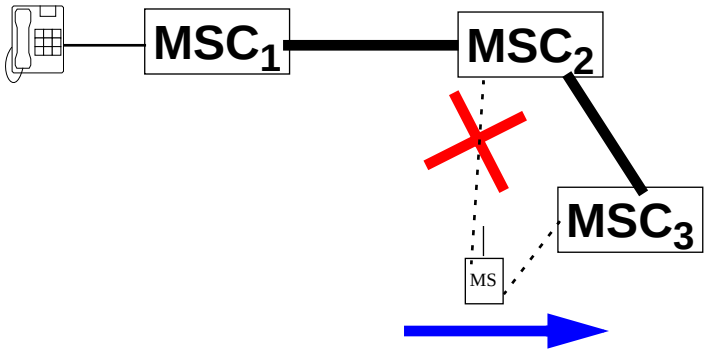
What happens if the mobile moves gain?



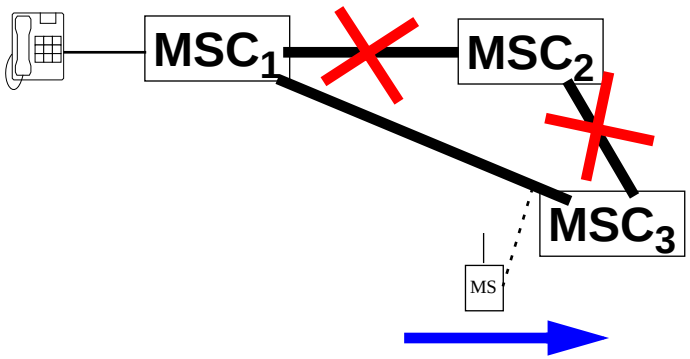
a. Forward handoff



b. Backward handoff



c. Handoff to a third MSC



c. Path minimization

Figure 8: Handoffs between multiple MSCs

Note that the call always goes via the so-called **Anchor MSC** (in this case MSC_1). This is of course because the phone attached to the PSTN knows nothing about mobility and the originating exchange thinks the call is still in existence (i.e., there was no termination and set up of a new call to or from the fixed phone).

Note that without path minimization the chain of trunks between MSCs could continue to grow *as long as the call lasts* **and** the *mobile keeps moving* to new MSCs. With voice calls, the call duration is generally rather limited, but with data communication it could continue for a very long time. Hence we will need to use another model for dealing with data (this will be addressed later in the lectures).

Fast Mobile IPv4 handoff via Simultaneous Bindings

The **Simultaneous Binding** option in Mobile IPv4 allows the Mobile Node to establish a binding for the new AP with its home agent (*before* a handoff). The Home Agent now duplicates all packets destined for the MN for the time of the handoff and relays all data to **both** the old and the new APs. Thus the MN performs the handoff by simply reconfiguring its interface -- which it can generally do within a very short interruption time, i.e. less than 10ms. When the MN physically connects to the new network, it will find that the packets destined for it are already arriving there!

Fast handover timeline

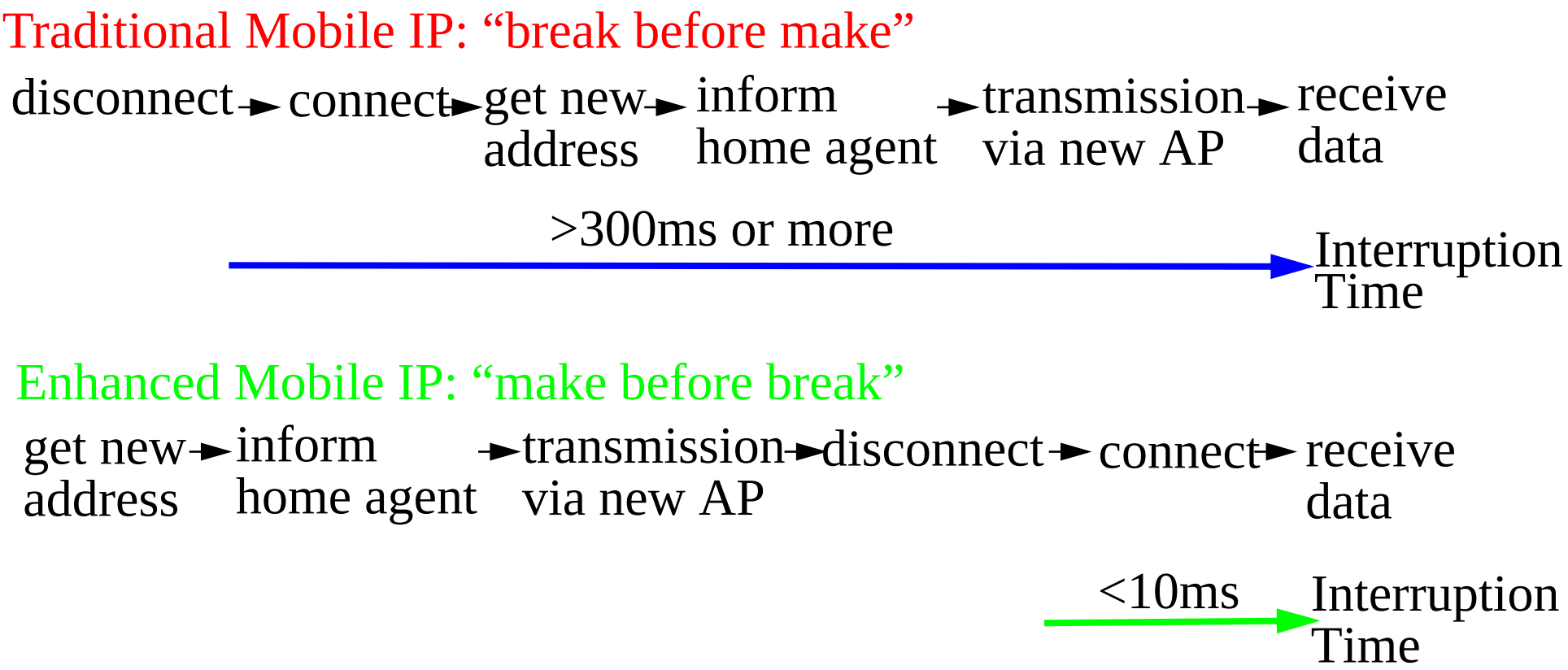


Figure 9: Fast handover timeline [a]

a. Figure adapted from http://www.ccrle.nec.de/Figure3.gif which is part of *http://www.ccrle.nec.de/Handoff.html*

Roaming

Roaming occurs when a user of one PCS is using the services of **another** PCS.

Roaming is generally based on “roaming agreements” between the operators of the involved PCS systems; basing the user’s home operator agrees to pay the other PCS operator(s) for carrying this **mobile user’**s traffic.

Note that the agreement is generally about the **user** - not a specific device, thus a user is free to change devices to access the new PCS network. This of course may complicate the authentication, authorization, and accounting (AAA) processes.

As a side of effect of authenticating and authorizing the user to access the new PCS, the home PCS’s mobility database is updated to reflect the fact that this user in located in the other PCS - thus traffic arriving for this user can (should?) be forwarded/redirected to the user’s current location. Clearly this raises both policy decisions (Should *this* specific traffic be redirected? Should *all* traffic be redirected? Should this location be reported? …) and accounting questions (*Who pays* for carrying the redirected traffic? Is there a *base charge for roaming*? …)

When the mobile moves to PCS_2 the local VLR is updated, the HLR is updated, and the former VLR is also updated.

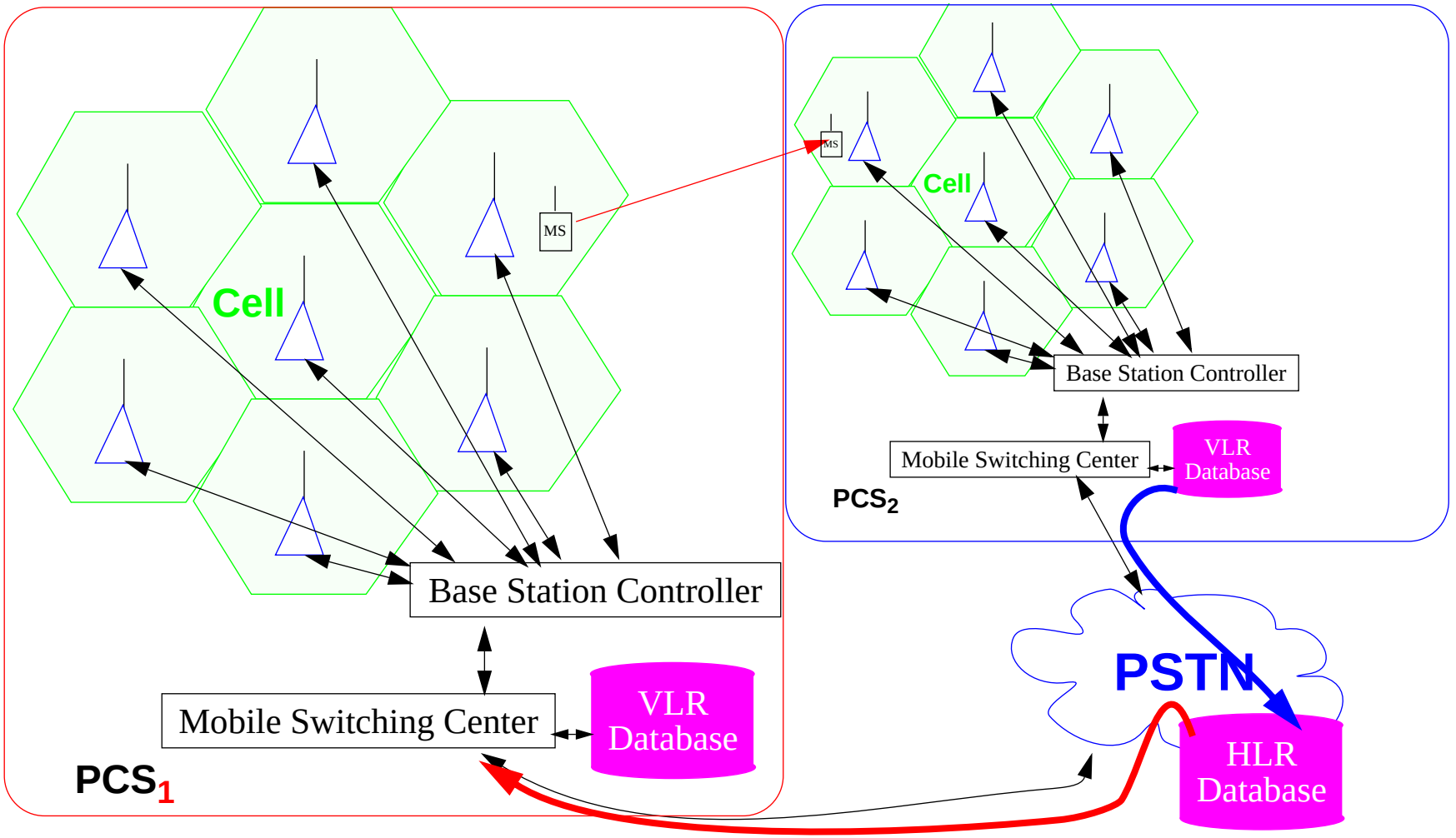


Figure 10: Mobile roams from PCS_1 to PCS_2

Roaming Management

Two parts:

- **registration** (location update) - process whereby MS informs the system of its **current** location
- **location tracking** - the process of locating the user to deliver a call

EIA/TIA Interim Standard 41 (IS-41 or ANSI-41) and Global System for Mobile Communications (GSM) Mobile Application Part (MAP) both define a two-level strategy - which uses two tiers of databases:

- **home location register** (HLR) - exists at the user's *home system*
- **visitor location register** (VLR) - a temporary record at the *visited system*

Roaming example

Gunvor (from Kiruna) has been visiting in Göteborg, now arrives in Stockholm

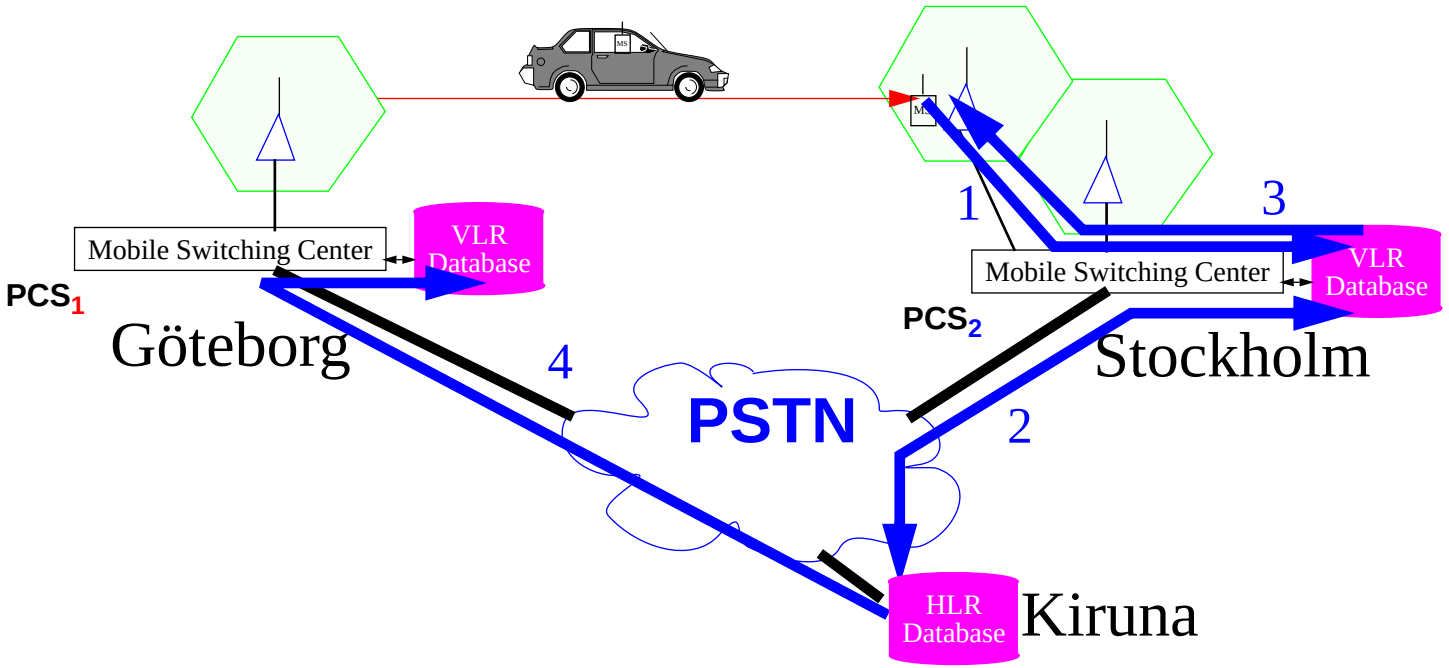


Figure 11: Mobile roams from PCS_1 to PCS_2

1. When the user (and her MS) arrives in Stockholm, her MS has to register with the VLR for PCS_2.
2. PCS_2's VLR informs the user's in Kiruna HLR of the user's current location (i.e. that the HLR should point to the VLR in PCS_2). The HLR sends the user's profile to PCS_2's VLR.
3. PCS_2's VLR informs the mobile (MS) that is has successfully registered.
4. HLR informs PCS_1's VLR to remove their entry for the user.

Of course it couldn't be this simple!

Discussion left out all the interactions within the PCS (i.e., details of channel assignment & signaling within the cells, between the base station & base station controller, and between the BSC & the MSC) -- it also left out all the interactions with the PSTN. Section 2.3 "Roaming Management under SS7" describes some of the details of the later. To *reduce the cost of registration* one can utilize a **forwarding pointer scheme**:

- Move operation (**registration**) - when moving from VLR to VLR, enter a forwarding pointer into the previous VLR, rather than notifying the HLR
- Find operation (**call delivery**) - when a call comes to the home system, walk the chain and then update the HLR.

Reducing the cost of deregistration:

- **implicit deregistration** - only delete records from the VLR when you need the space
- **periodic reregistration** - MS periodically registers with the VLR, if no reregistration within a timeout period, then their record is deleted

Call delivery

An originating Switching Point (**SSP**) (or alternatively a Signal Transfer Point (**STP**)) maintains a cache of the **Mobile Identification Number** (MIN) and the current VLR) - it examines this cache - there are three outcomes:

1. Cache entry not found ⇒ do the lookup of MIN's HLR via **Global Title Translation** (GTT)
2. Cache entry exists **and** is current ⇒ do a lookup in the VLR
3. Cache entry exists, but is **obsolete** ⇒ do the lookup of MIN's HLR via **Global Title Translation** (GTT)

Determining that the cache entry is (probably) current is generally done with heuristics.

CT2

Section 2.4 describes how CT2 as a call **originating only** system didn't need location services, but that it could be extended via:

1. sending a page to a user and the user call in
2. calling into a meeting point - which patches the two (or more) callers together

Back to: Who makes the handoff decision?

Network controlled handoff (NCHO)

Network controlled handoff (HCHO) - the network makes the decision

- BS monitors the signal strength and quality from the MS
- Network uses multiple (current and surrounding) BSs to supervise the quality of all current connections by making measurements of RSSI
- MSC makes the decision when and where to effect the handoff
- Heavy network signaling traffic and limited radio resources at BSs prevent frequent measurements of neighboring links $\Rightarrow$ long handoff times.

Handoff times: upto 10sec or more

Mobile assisted handoff (MAHO)

Mobile assisted handoff (MAHO) - the mobile provides data which the network uses to make the decision; essentially it is a variant of network controlled handoff - but uses the mobile to help reduce the handoff times.

For example, in GSM the MS transmits measurements twice a second
$\Rightarrow$ GSM handoff execution time ~ 1sec

Note in both NCHO and MAHO - if the network can't tell the mobile about the new channel/time slot/… to use *before* the link quality has decayed too far, then the call may be terminated.

Mobile controlled handoff (MCHO)

The mobile decides for itself (by monitoring signal strength and quality from the current and candidate base stations), when it finds a “better” candidate it initiates a handoff. In MCHO most of the work is done by the mobile (as it knows who it can hear, how well it can hear them, and can even consider its battery level, etc.)

Two common handoffs:

- **automatic link transfer** (ALT) - transfer between two base stations
- **time slot transfer** (TST) - transfer between channels of a single BS

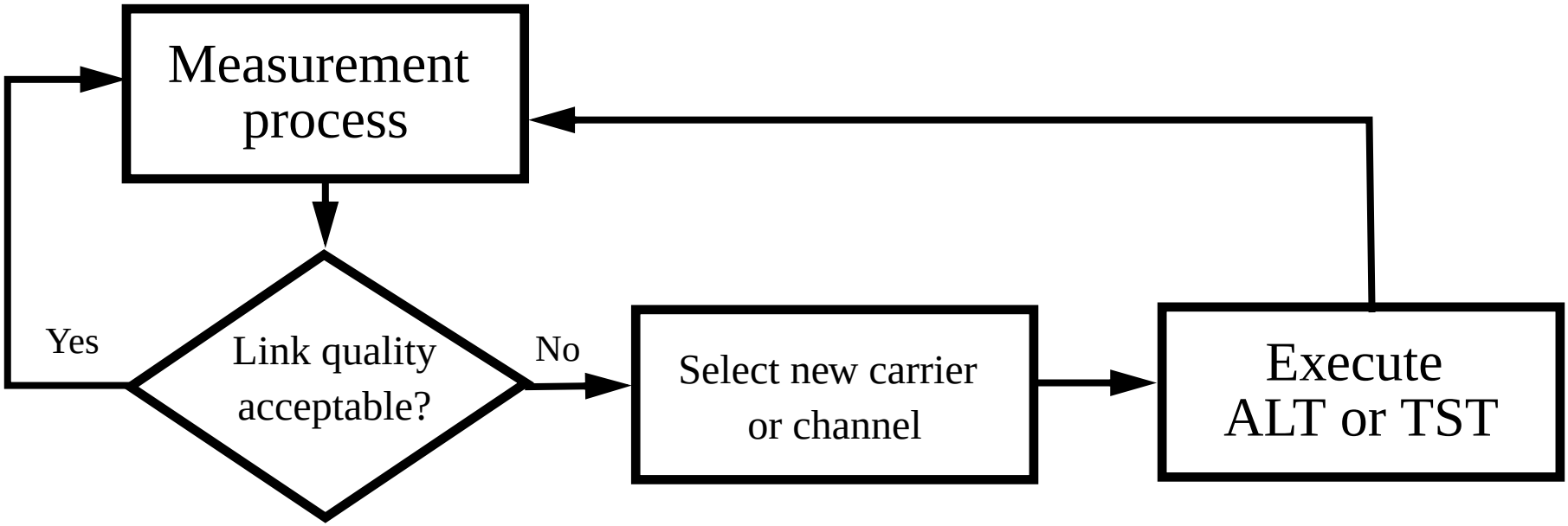


Figure 12: MS-quality maintenance processing

Different systems use different approaches to the measurement process. For example, some DECT implementations can measures the RSSI of all channels simultaneously. In other systems, the measurement of other channels is done when the device is itself not transmitting or receiving.

Handoff times: DECT 100-500ms, PACS 20-50ms.

Handover Failures

- No available channel/link resources in the new **BS**
- Insufficient resources as determined by the **network** (for example, no available bridge, no suitable channel card {for example, none supporting the voice CODEC in use or radio link coding}
- It **takes too long** for the network to set up the new link
- **Target link fails** during handoff

Channel Assignment

Goals:

- achieve high spectrum utilization
- maintain a given service quality
- use a simple algorithm
- require a minimum number of database lookups

Unfortunately it is hard to do all of these at once!

If there is no available channel, then

- new calls are **blocked**
- existing calls that can't be handed over $\Rightarrow$ **forced terminations**

Channel Assignment Process

- **Fixed Channel Assignment** (FCA)
- **Dynamic Channel Assignment** (DCA)
- **Quasi-static autonomous frequency assignment** (QSAFA)
- …

Lots of schemes have been introduced to reduce the number of forced terminations, at the cost of increased blocking or decreased efficiency:

- **Nonprioritized scheme** (NPS) - handoff call treated the same as a new call
- **Reserved Channel scheme** (RCS)- reserves some resources for handoffs
- **Queuing Priority scheme** (QPS) - exploit the over lap (handoff area)
- **Subrating scheme** (SRS) - switching CODECs of one or more calls to free resources

Handoff Management: Radio Link Transfer

We will not cover the details of the radio link, but will examine some key ideas.

hard handoff	mobile connects only to a single base station at a time
soft handoff	mobile receives/transmits from/to multiple BSs simultaneously

In soft handoff, the network and perhaps the mobile have to figure out how to combine the information from the multiple basestations (in the up and down links respectively).

Link transfers:

1. Intracell
2. Intercell or inter-BS
3. Inter-BSC
4. Intersystem or inter-MSC
5. Intersystem between two PCS networks

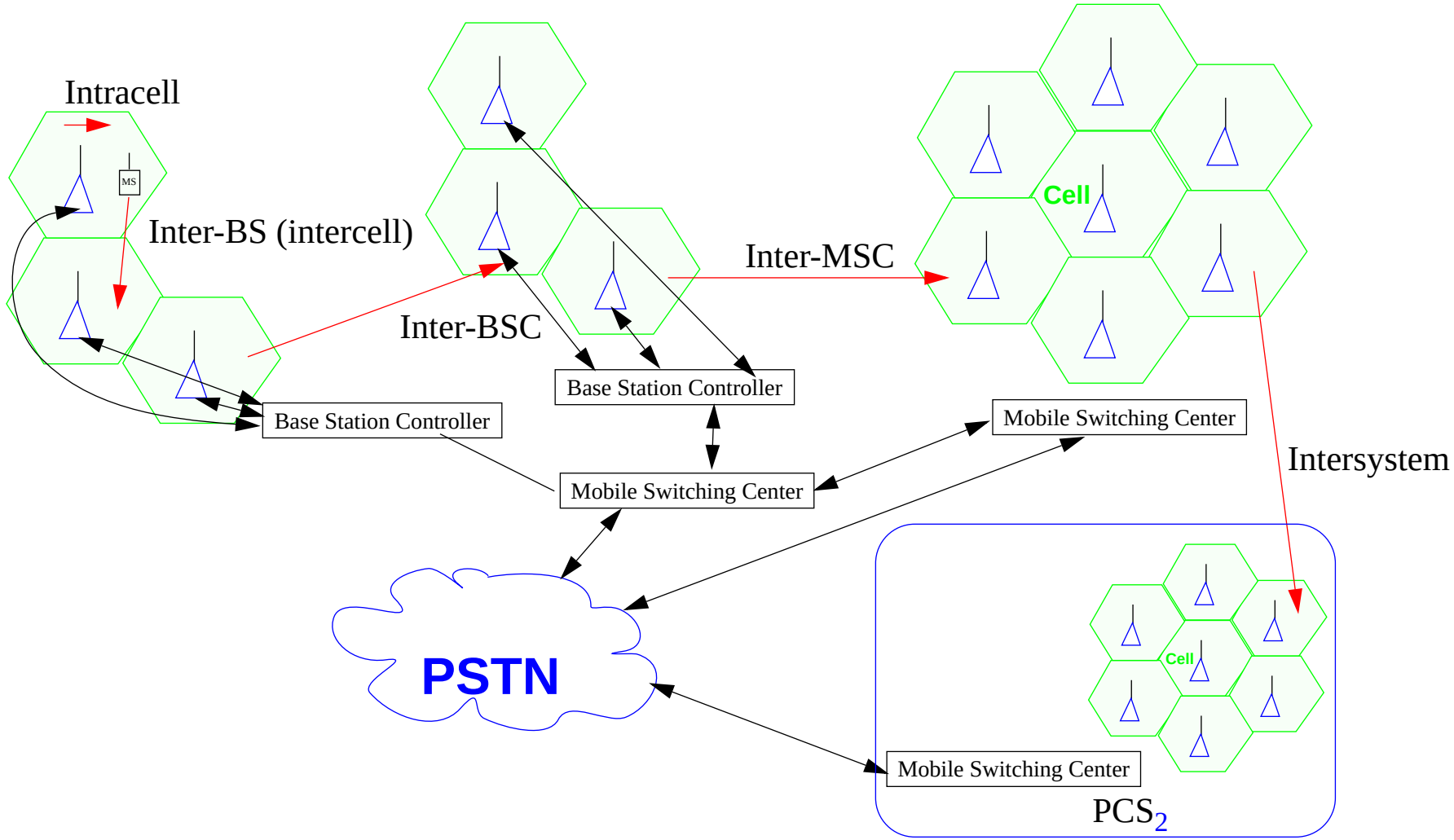


Figure 13: Handoffs, mobile moves within PCS_1 and then on to PCS_2

Handoff frequency

With a cellular voice call of 1 minute duration:

Type of handoff	Probability
inter-BS	0.5
inter-BSC	0.1
inter-MSC	0.05

Soft handoff in multiple forms

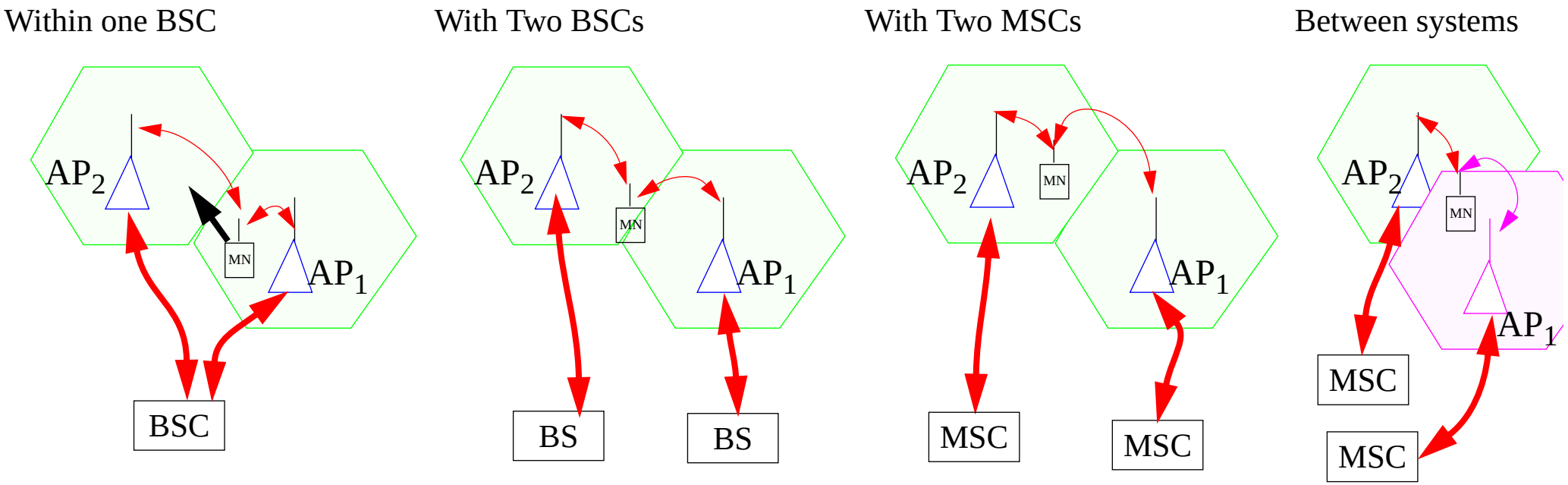


Figure 14: Soft handoffs

Some CDMA systems use very precise link level timing to enable the signals from multiple BSs to arrive additively at the mobile - thus leading to a physically stronger signal.

Soft handoffs between systems generally will require that the mobile be able to receive multiple signals - which will use different codes, frequencies, … .

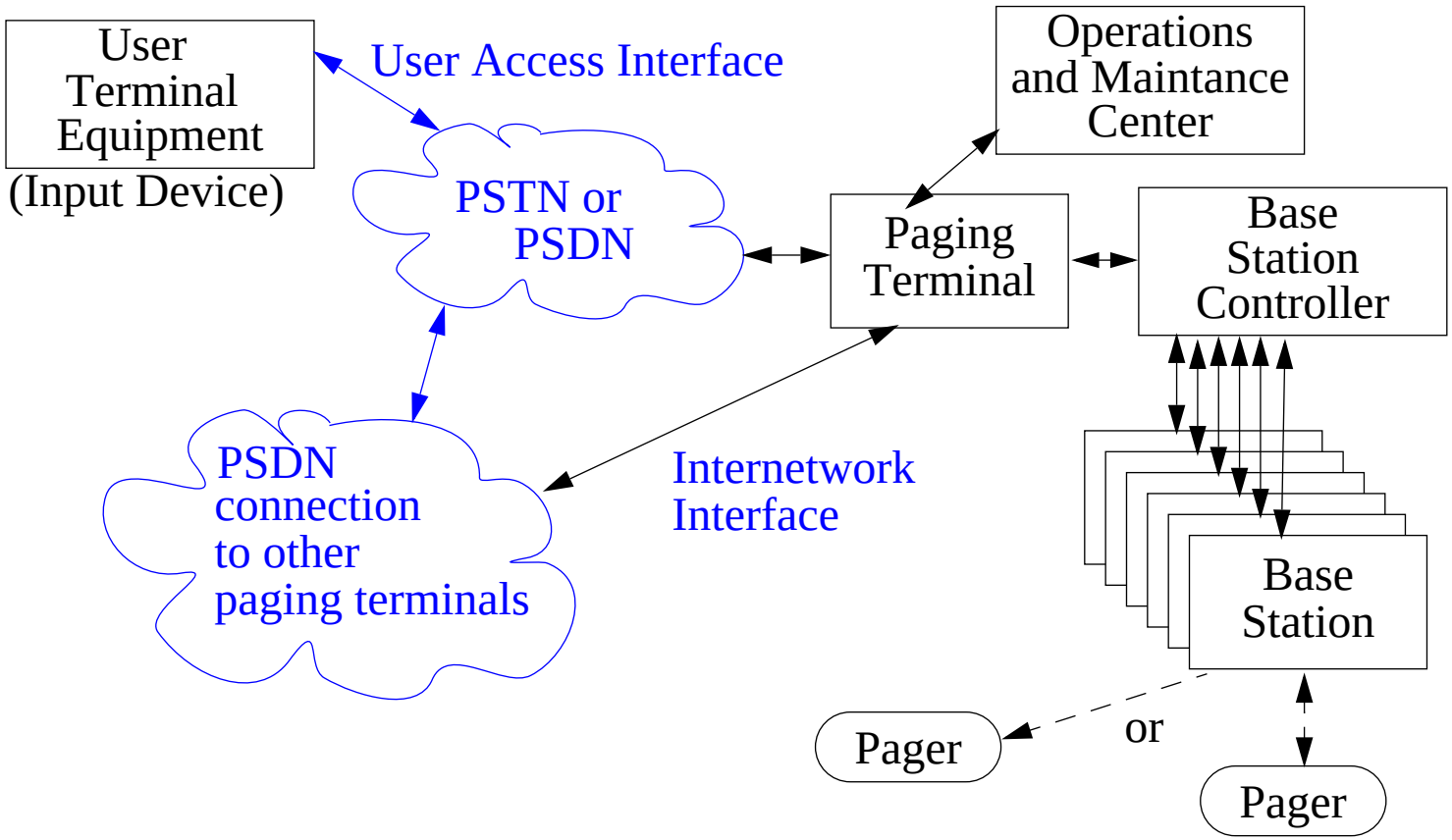
Paging

Originally a one-way personal altering/messaging system invented by Charles Neergard in 1949 (annoyed when hospitalized by the voice paging over the public address system).

A transmitter sends a stream of addresses and messages. **Pagers** listen for their address (also called a cap code).

Cap Code	beep (one of ~4 tones) when the pager's address is received by the pager
Tone voice	1970's, allows the sender to record and send a short voice message
Digital display	early 1980's, a callback number (or code) is entered by the sender, which then appears on the pager's display
Alphanumeric	late 1980's, display a text message

Paging Architecture



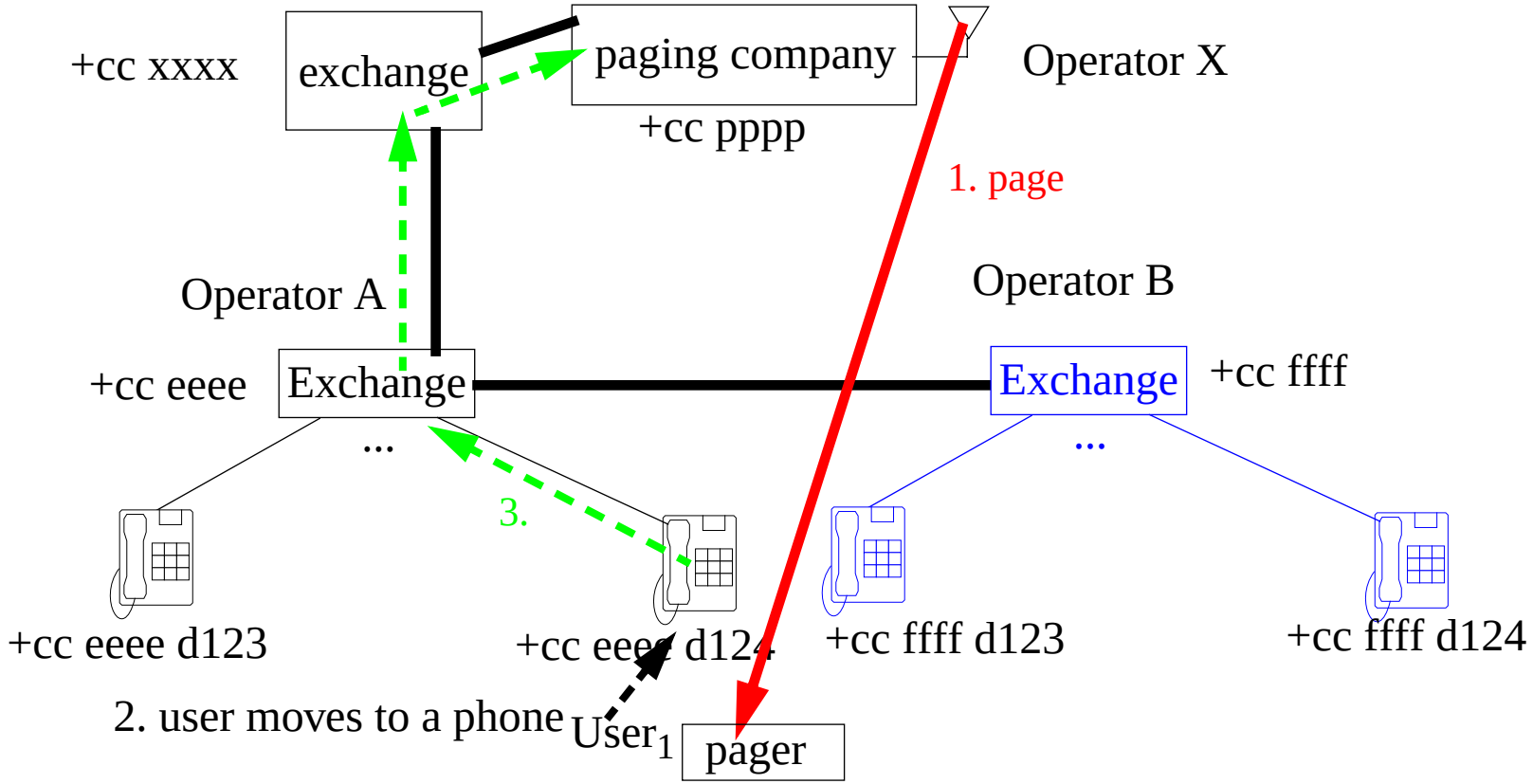
Paging terminal has database of customers, cap code, pager number, types of messages, …; converts voice message to text (for alphanumeric pagers); store in mailbox for pager; forward to other paging terminals; send to relevant Base Station Controller(s)

Paging Service area

Service areas: site, local area, region, national, international

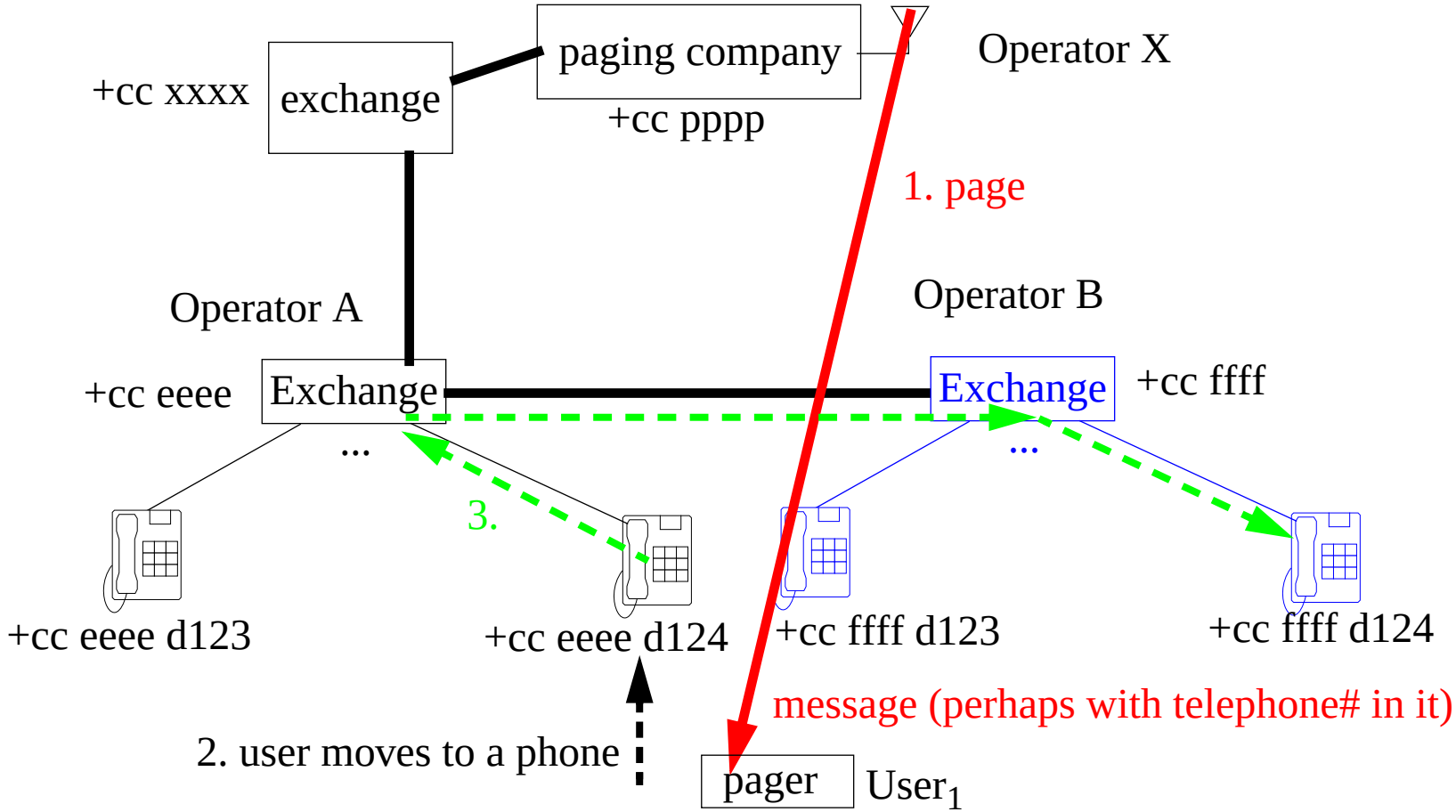
If the user temporarily left the paging service area or if the signal could not reach them, then they would miss it. Motorola's ReFLEX technology, a two-way paging system, keeps transmitting a paging message until the user's pager sends a confirmation that it has been received.

Introduction of paging systems



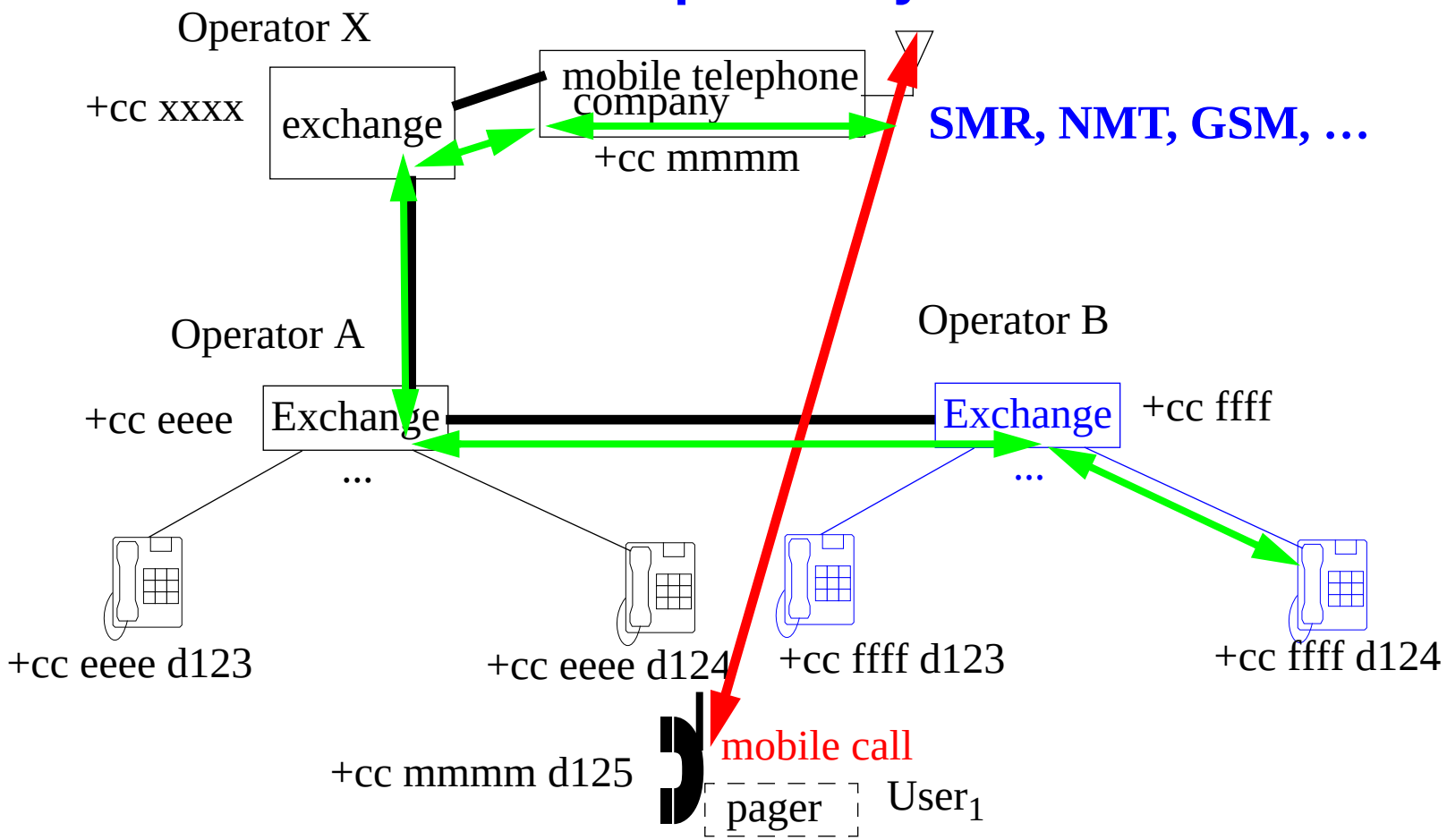
Upon a page (1), user moves to nearest phone (2), calls paging company (3), company operator tells the user what telephone number to call - perhaps they (also) convey a short message. The mobile user can be contacted and told by the operator at the paging company to connect to the fixed telephone network. [i.e., make a temporary connection to the (voice) network.]

Alphanumeric paging systems



Upon a page (1), user moves to nearest phone (2), calls a number based on the content of the (page) message (3); or perhaps they just consume the short message they received. The mobile user can be contacted and told by a message to connect to a given number on the fixed telephone network.

Mobile telephone systems

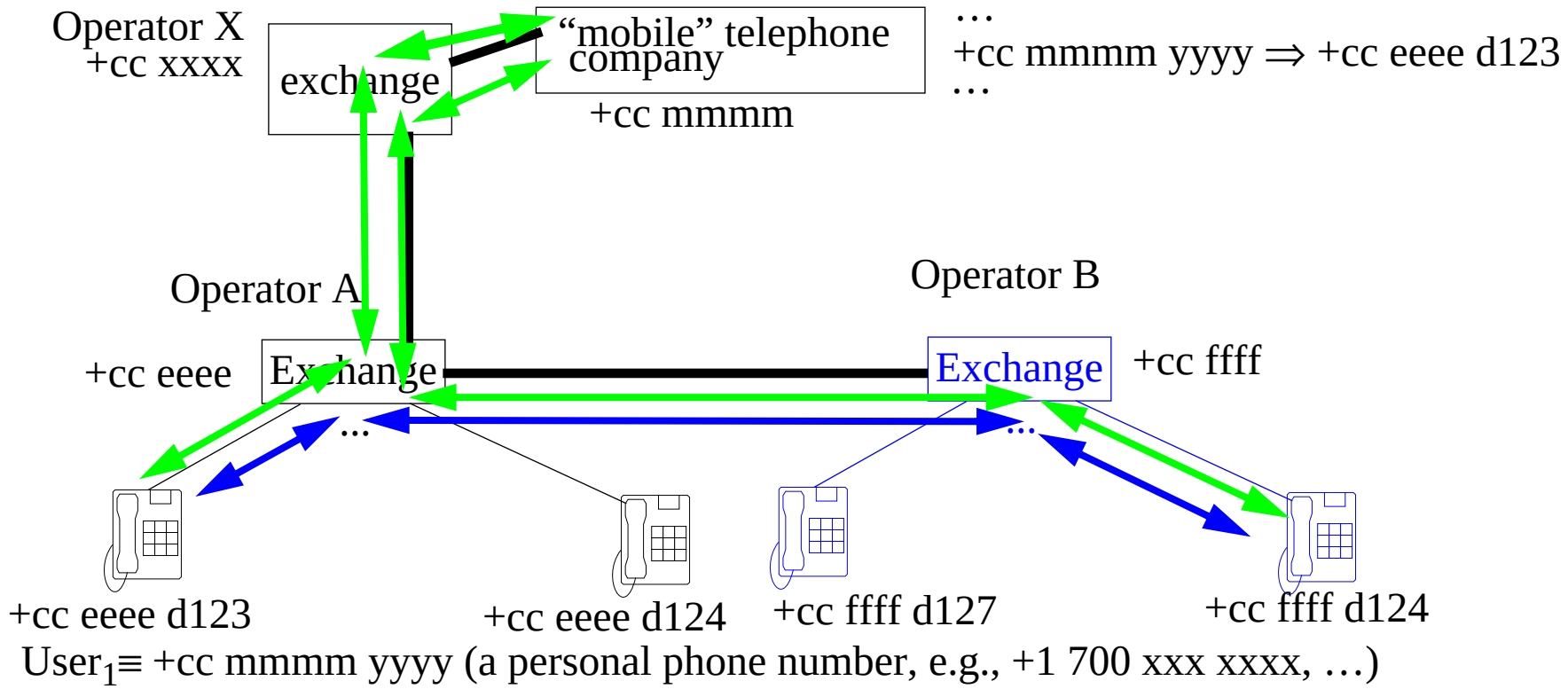


The mobile user is directly reached by the call through the mobile telephone network.

SMR (Specialized Mobile Radio) is a non-cellular radio system.

NMT (Nordic Mobile Telephone), GSM (Groupe System Mobile), and PCS are cellular radio systems.

Mobile but not necessarily wireless

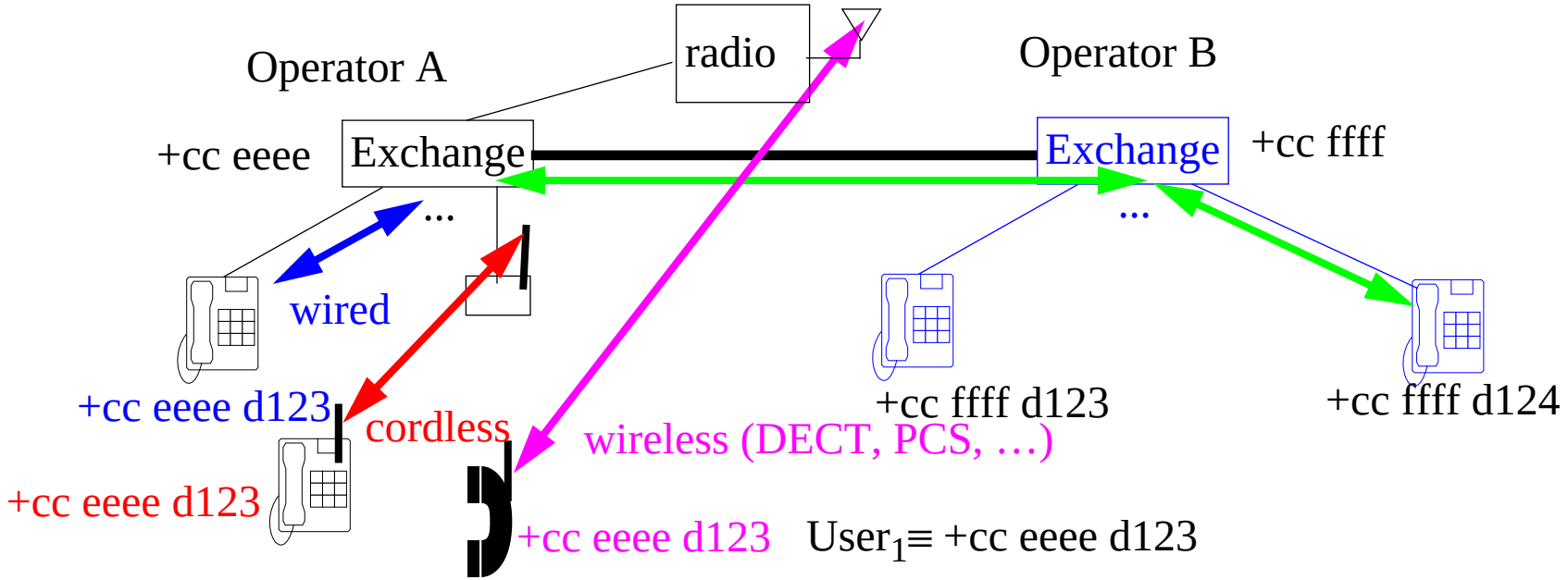


The mobile user is indirectly reached through the fixed telephone network.

- The connection can be via the "mobile" company (hiding the actual location of the user) or
- via redirect directly to the current location of the user.

Thus the mobile operator turns +cc mmmm yyyy into +cc eeee d123 [dynamic address translation].

Local mobility via wireless (or redirects)

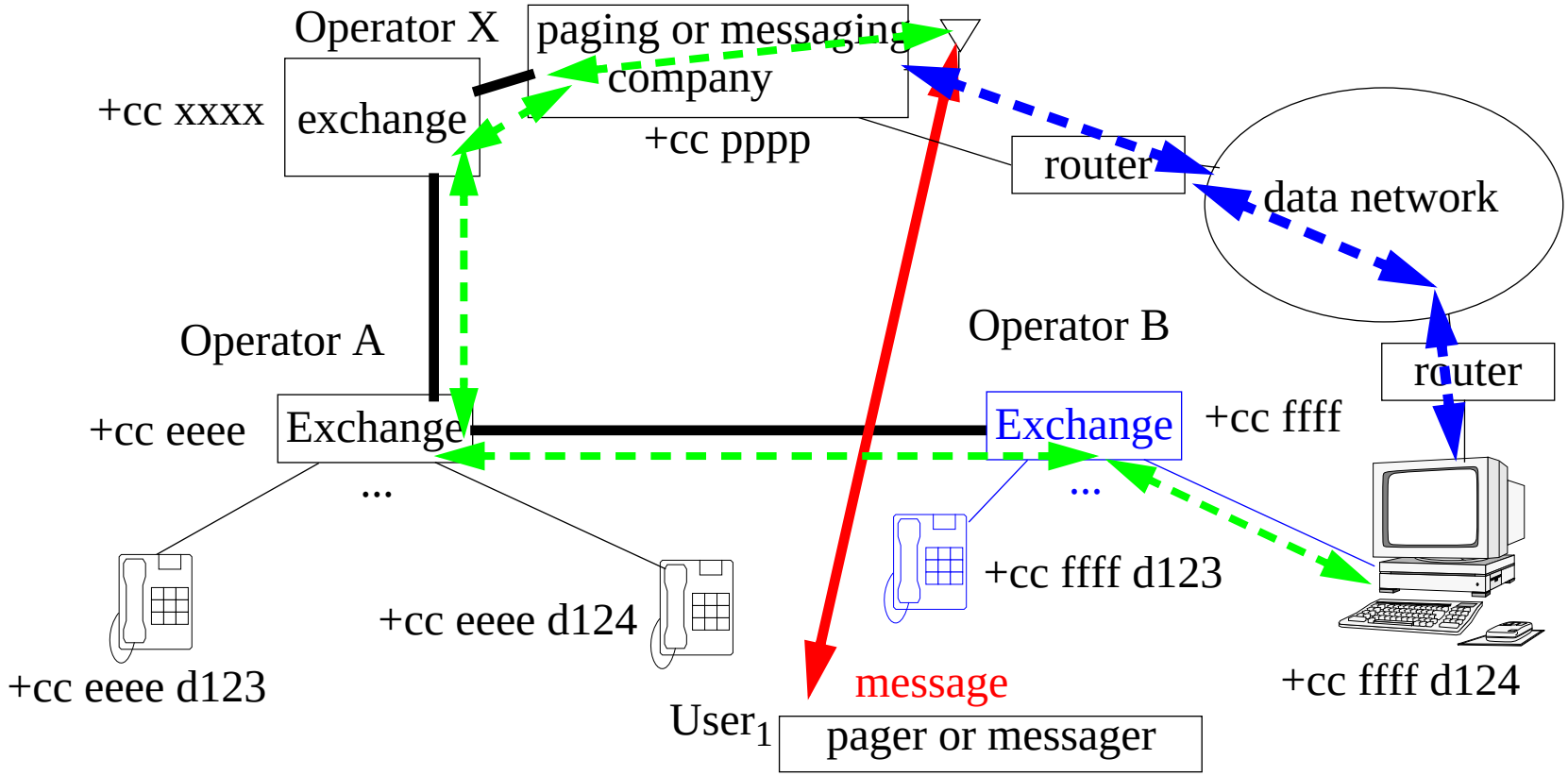


The mobile user is reached by **local redirection** (which may utilize local wireless links) of the call coming from the fixed telephone network.

- The local exchange is playing the role of the "mobile" company (hiding the actual location of the user).
- There are multiple instruments (terminals) and user is currently associated with a list of them
- Could involve a non-local redirect

To the external world the user looks like they are always at +cc eeee d123, which the local PBX maps into a specific extension (at the time of the call).

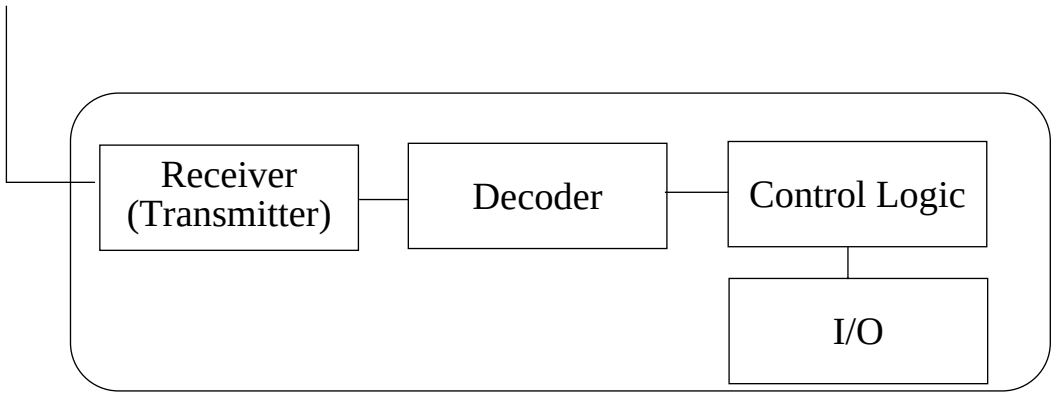
Two-way paging and messaging systems



Two-way paging or messaging allows exchange of digital messages.

- Traditionally the paging or messaging system was a separate data network, but GSM's **Short Message Service** provides alphanumeric messaging via the GSM infrastructure.
- The messaging device can also be a computer (PDA/notebook/…)
- Connection between the two users can be via the PSTN or a (public) data network

Pager



I/O can be a display, a beeper, keypad, audio input/output, vibrator, … .

Control logic supports:

- duplicate message detection
- message locking (to keep message from being overwritten)
- message freezing (to keep message on the screen)
- altering modes (beep, vibrate, …)
- power management

Paging Interworking

- **Telocator Alphanumeric Protocol** (TAP), also known as IXO or PET, defines a 7-bit alphanumeric text message to be sent to paging receivers, with a block size of 256 characters and an effective message length of 1,000 characters
- **Telocator Data Protocol** (TDP) suite: a functional superset of TAP; adopted 1995; **Telocator Message Entry** (TME) protocol - the input protocol for TDP: two-way paging, priority paging, deferred paging, periodic paging, message forwarding, and message deletion.
- **Telocator Network Paging Protocol** (TNPP) used to create networks of paging terminals from different manufacturers (overcomes the proprietary protocols to/from paging terminals - such as Glenayre Link Module, Spectrum Data Link Handler)

Software:

ftp://ftp.cs.unm.edu/pub/chris/paging/ixo.txt

http://en.tldp.org/HOWTO/mini/Pager/

Paging - link level

- Older format: British Post Office Code Standards Advisory Group (**POCSAG**)
  - single operator, single frequency
  - maximum of 2 million users
  - two separate tones and then a burst of data; 576 bit preamble then multiple 544 bit batches
- ETSI's European Radio Message System (**ERMES**)
  - 35 bit radio identity code
  - effective transmission rate of 3750 bps
  - each hour is partitions into 60 cycles, each cycle partitioned into 5 subsequences, each subsequence is partitioned into 16 batches
- Philips Telecom's Advanced Paging Operations Code (**APOC**)
- Motorola's **FLEX** (further described on next slide)
  - signals have only a single tone preceding the data burst.
  - Interestingly FLEX paging data is _not_ encrypted.
- Motorola's **Generation II FLEX**
  - FLEX G1.9 protocol supports full roaming, time of day updates accurate to one hundredth of a second, and dynamic group messaging
  - Motorola's FLEXsuite™ applications, such as over the air programming, encryption, and compression utilize FLEX G1.9.
  - 1600 and 3200 symbols-per-second

Motorola's FLEX™ protocol[1]

http://www.motorola.com/MIMS/MSPG/FLEX/protocol/solution.html

Supports upto five billion individual addresses and up to 600,000 numeric pagers per channel. Channel can run at 1600 to 6400 bps as needed by operator.

- FLEXion™ an advanced voice paging protocol
  - Motorola's Portable Answering Machine - can receive and store voice messages,
  - digitally compresses voice messages
  - system is aware of the general location of the recipient's messaging unit, therefore sends the message from the closest paging transmitter
- ReFLEX™ a two-way messaging protocol
  - Motorola's Advanced Messaging Group has demonstrated the use of a ReFLEX two-way pager to access Hyper Text Markup Language (HTML) content.

160 FLEX technology-based systems in commercial operation in 36 countries, representing 93% of the world's paging subscriber base - http://www.nasco.com.sa/products/motorola/pager_flex.html

1. As of February 2002, Motorola transferred all their paging subscriber device product lines to Multitone Electronics plc, Basingstoke, UK http://www.multitone.com/

Sleeping for power savings

A major aspect of the link level paging protocols is to enable the pager to spend most of its time **sleeping**.

It does this by **knowing when to listen for its address** and in the case of Motorola if as the address is being received more bits fail to match than the error correction could possibly correct, then it goes to sleep immediately.

Some paging receivers don’t even wake up the decoder unless the page may be for this device (thus the different parts of the page may be awakened separately).

Mobile Telephone Systems Timeline (the first two generations: analog + digital)

Year	Standard	System	Technology	Primary markets
1981	NMT 450	Nordic Mobile Telephone	Analogue	Europe, Middle East
1983	AMPS	Advanced Mobile Phone System	Analogue	North and South America
1985	TACS	Total Access Communication System	Analogue	Europe and China
1986	NMT 900	Nordic Mobile Telephony	Analogue	Europe, Middle East
1991	GSM	Global System for Mobile communication	Digital	World-wide
1991	TDMA(D-AMPS)	Time Division Multiple Access	Digital	North and South America
1993	CdmaOne(IS95)	Code division multiple access	Digital	North America, Korea
1992	GSM 1800	Global System For Mobile Communication	Digital	Europe
1994	PDC	Personal Digital Cellular	Digital	Japan
1995	PCS 1900	Personal Communication Services	Digital	North America

References and Further Reading

See the summary in section 2.5 (and in each chapter) of [1] for more pointers to additional reading. Take careful note that some of the things which the authors have covered in chapter 2 are *simply their proposals and not (yet) implemented*; but their ideas are worth understanding.

Course book

[1] Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, John Wiley & Sons, 2001, ISBN 0-471-39492-0.

Further details concerning physical and link layer wireless communication

[2] David J. Goodman, *Wireless Personal Communication Systems*, Addison-Wesley, 1997, ISBN 0-201-63470-8.

- Great coverage about the link layer details and general architectures of AMPS, IS-41, North American TDMA and CDMA, and GSM. Only very brief coverage of CT2, DECT, PHS, and PACS. This is an extremely well written book.

[3] William C.Y. Lee, *Mobile Cellular Telecommunications: Analog and Digital*

Systems, Second Edition, 1995, ISBN 0-07-038089-9

- all the usual radio topics

[4] Theodore S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd edition, Prentice-Hall, 2002, 736 pages, ISBN: 0-13-042232-0.

[5] Ellen Kayata Wesel, *Wireless Multimedia Communications: Networking Video, Voice, and Data*, Addison-Wesley, 1998, ISBN 0-201-63394-9.

[6] K. Pahlavan and P. Krishnamurthy, *Principles of Wireless Networks*, Prentice Hall PTR, 2002, ISBN 0-13-093003-2.

CDPD

[7] Mark S. Taylor, William Waung, and Moshen Banan, *Internetwork Mobility: The CDPD Approach*, Prentice-Hall, Upper Saddle River, NJ, 1997. ISBN 0-13-209693-5.

LEO

[8] Christopher Redding, “Overview of LEO Overview of LEO Satellite Systems”, Institute for Telecommunication Sciences National

Telecommunications and Information Administration, Boulder, CO - lecture slides from 1999 International Symposium on Advanced Radio Technologies: http://www.its.bldrdoc.gov/meetings/art/art99/slides99/red/red_s.pdf

Fixed Broadband wireless

[9] IEEE 802.16c™, "Air Interface for Fixed Broadband Wireless Access Systems - Detailed System Profiles for 10-66 GHz", http://standards.ieee.org/announcements/80216capp.html

User profiles

[10] Sudeep Kumar Palat, "Replication of User Mobility Profiles for Location Management in Mobile Networks", Norwegian University of Science and Technology, Dr. Ing. Dissertation, Dept. of Telematics, 12 Jan. 1998.

Mobile IP

[11] C. Perkins, IP Mobility Support, IETF RFC 2002, October 1996.

[12] C. Perkins, Ed., "IP Mobility Support for IPv4", RFC 3344, Aug. 2002, note: this obsoletes RFC 3220 and RFC2002.

[13] D. B. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6”, Internet draft, draft-ietf-mobileip-ipv6-21.txt, February 26, 2003, work in progress.

http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-21.txt

Fast handoff

[14] Karim El Malki (Editor), Pat R. Calhoun, Tom Hiller, James Kempf, Peter J. McCann, Ajoy Singh, Hesham Soliman, and Sebastian Thalanany, “Low Latency Handoffs in Mobile IPv4”, Internet draft, draft-ietf-mobileip-lowlatency-handoffs-v4-04.txt, June 2002, work in progress.

http://www.ietf.org/internet-drafts/draft-ietf-mobileip-lowlatency-handoffs-v4-04.txt

Micromobility: Cellular IP, HAWAII, Hierarchical Mobile IP

[15] *http://comet.ctr.columbia.edu/micromobility/*

[16] E. Gustafsson, A. Jonsson, and C. Perkins, Mobile IPv4 Regional Registration, Internet draft, draft-ietf-mobileip-reg-tunnel-07.txt, October 2002, work in progress.

http://www.ietf.org/internet-drafts/draft-ietf-mobileip-reg-tunnel-07.txt

Comparison of IP Mobility protocols

[17] P. Reinbold and O. Bonaventure. A Comparison of IP Mobility Protocol. Technical Report Infonet-TR-2001-07, University of Namur, Infonet Group, June 2001.
http://www.infonet.fundp.ac.be/doc/tr/Infonet-TR-2001-07.html

TeleMIP

[18] Subir Das, et al. TeleMIP: Telecommunication-Enhanced Mobile IP Architecture for Fast Intradomain Mobility. *IEEE Personal Communications*, 7(4):50--58, August 2000.

Intersystem Handoff

[19] *Janise McNair*, Ian F. Akyildiz, and Michael D. Bender, “An Inter-System Handoff Technique for the IMT-2000 System”, Proceedings of IEEE INFOCOM Conference, March 2000, pp.208-216.

KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

2. Network Signaling and CDPD

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Last modified: 2003.03.13:11:56

Lecture 2 (Chapters 5-8)

Network Signaling

Interconnection between a PCS Network (PCN) and a PSTN for:

- mobility management - tracking the location of mobile users
- call control - setting up the call path between a mobile users and the other call party
- interconnection interfaces - the interconnections themselves
- message routing - information exchange

Mobile Identification Number (MIN) -- the main means of identifying a MS

Universal Personal Telecommunication (UPT) number - a number associated with a mobile **subscriber.**

Transaction Capabilities Application Part (TCAP)

For exchanging information which is **not** circuit related.

More than 50 TCAP operations in IS-41 just for:

- inter-MSC handoff
- automatic roaming
- operation, administration, and maintenance (OAM)

A TCAP message has two parts: **transaction** and **component**

transaction	**QueryWithPermission, Response, ConversationWithPermssion**, and **Unidirectional** (pass info in **one** direction)
component	**INVOKE, RETURN RESULT (Last), RETURN ERROR,** or **REJECT**

Each TCAP transaction has a **timeout** associated with it and uses connection*less* transport.

TCAP message flow for a MS registration

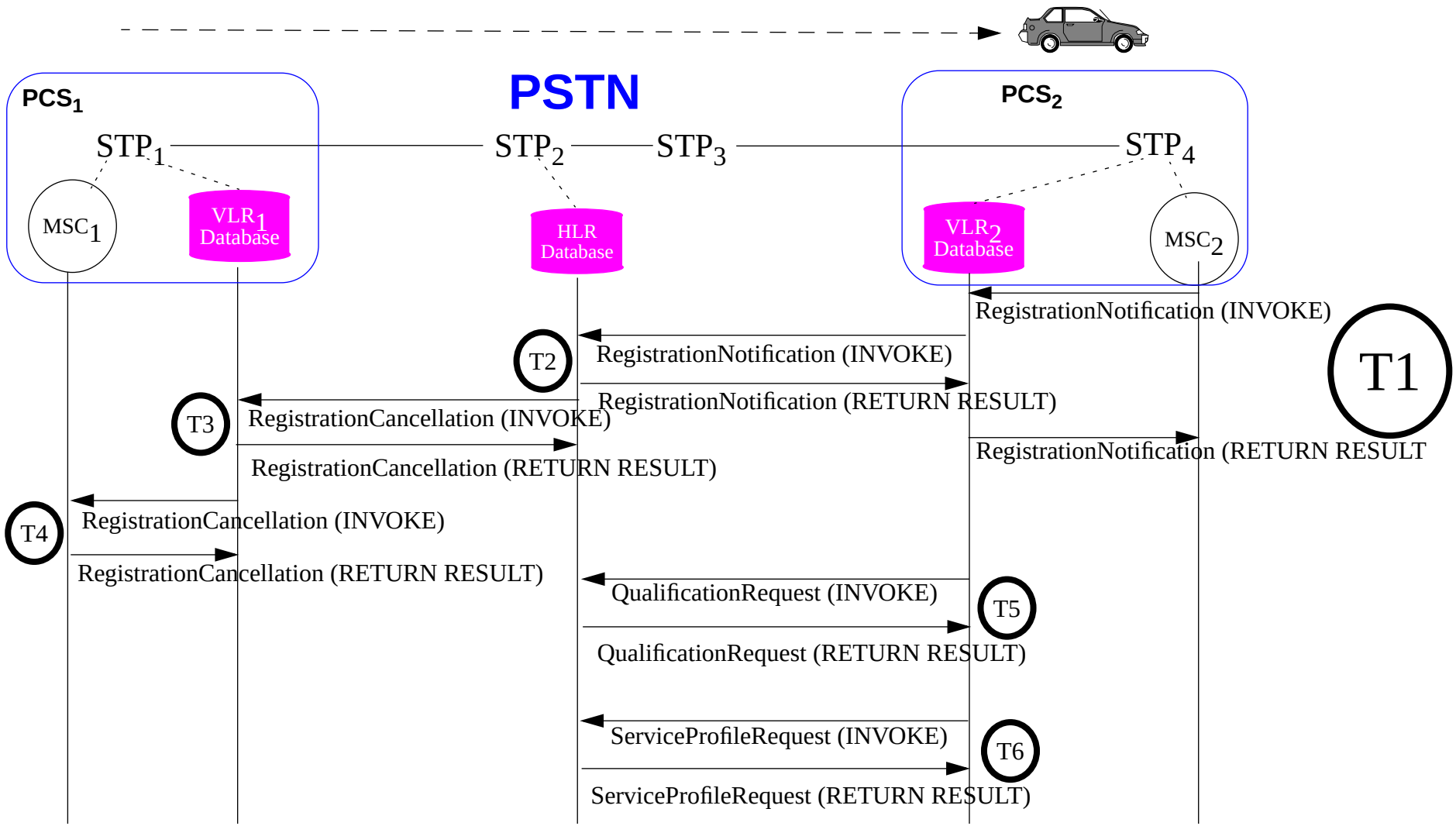


Figure 15: Mobile roams from PCS_1 to PCS_2

Transaction 2 (T2) - additional details

Signal Transfer Point$_3$ (STP$_3$) does a table lookup, i.e., **Global Title Translation** (GTT) of the MIN to identify the HLR's address, then the TCAP message is forwarded from STP$_3$ to STP$_2$ where the HLR is.

GTT is needed because **non-geographic** numbering is assumed {we will return to this later; See "Database lookups" on page 225.}.

Automatic Code Gapping (ACG)

- Can use **Automatic Code Gapping** (ACG) to reduce the rate at which a network entity such as a MSC sends service request messages to a service control function.
- ACG can be applied automatically when an overload occurs or applied manually for system management.
- ACG can be applied to query messages destined for a specific Point Code and Subsystem Number or for an SCCP Global Title.

3rd Generation Partnership Project 2 (3GPP2), Automatic Code Gapping (Stage 1), 3GPP2 S.R0016, Version 1.0.0, Version Date: December 13, 1999

http://www.3gpp2.org/Public_html/specs/S.R0016_v1.pdf

TIA TSB-51: Authentication, Signaling Message Encryption and Voice Privacy

- supports authentication over multiple air interfaces (AMPS,TDMA, & CDMA) -- GSM authentication is excluded, because the GSM authentication process has been defined in the GSM standards
- provides a method of pre-call validation of (MS) that does not require user intervention
- uses Global Challenge procedures at registration, call origination, call termination, and at any time using Unique Challenge procedures
- without-sharing (WS) scheme: “shared secret data” (SSD) known only to Authentication Center (AuC) and MS
- sharing (S) scheme: the SSD or some aspect of it is shared with visited system
- SSD based on Authentication Key (A-Key) - never transmitted over the air
- Also includes procedures for generation and distribution of SSD

MIN and ESN

Mobile Identification Number (MIN) - a North American Numbering Plan (NANP) number which is the phone number of a mobile phone

Electronic Serial Number (ESN) - a 32 bit serial number programmed into the phone at manufacture (top 8 bits identify the manufacturer)

In AMPS the MIN and ESP are transmitted in the clear over the air - so it is easy to listen for them and then program another phone with the same values $\Rightarrow$ **clone**

This lead to hundreds of millions of dollars of fraud $\Rightarrow$ TSB-51

Without-Sharing Scheme

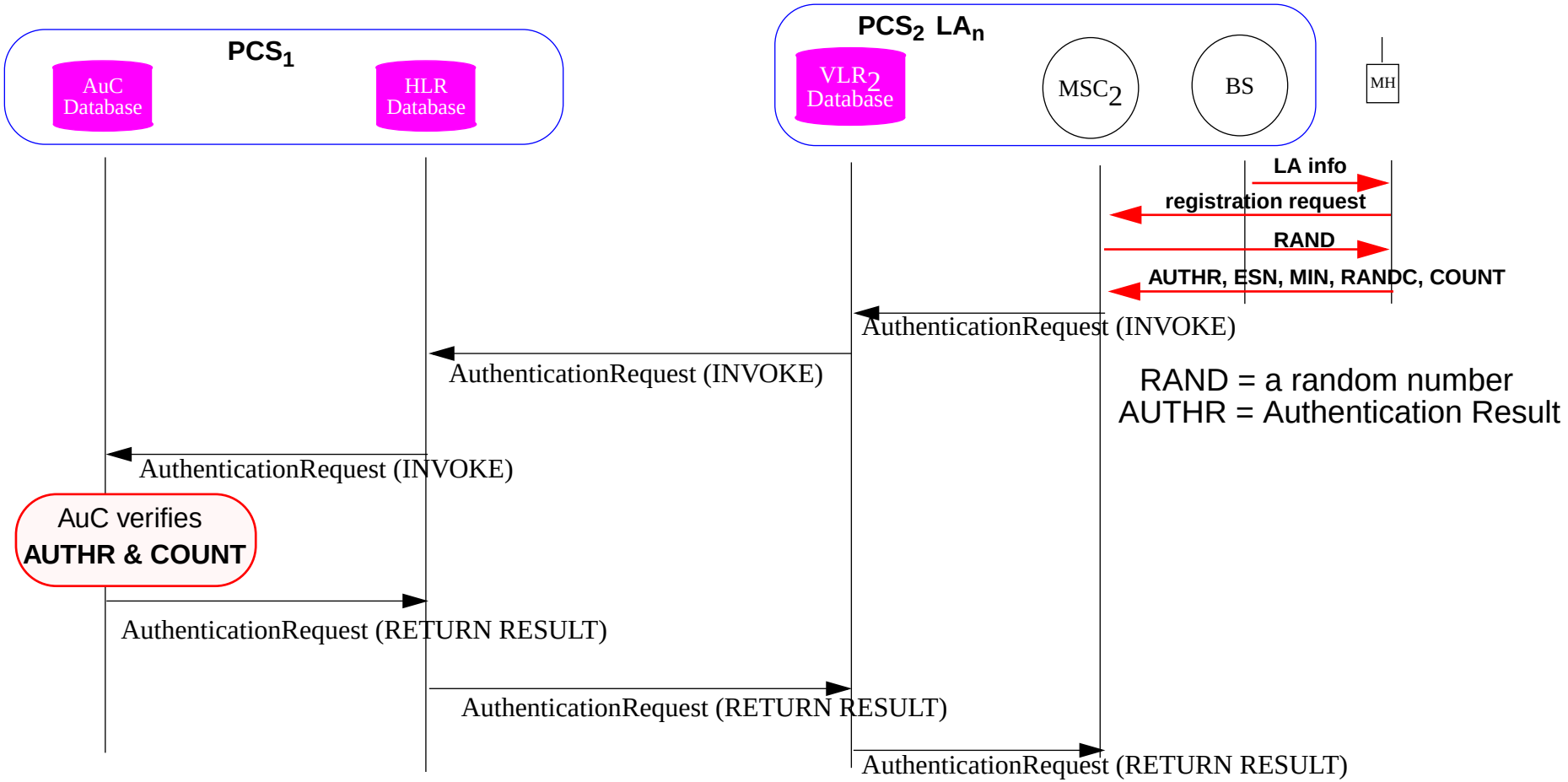


Figure 16: Mobile moves into a new Location Area (LA) at PCS_2

If authentication fails, then the result is RETURN ERROR.

Without-Sharing Call Origination

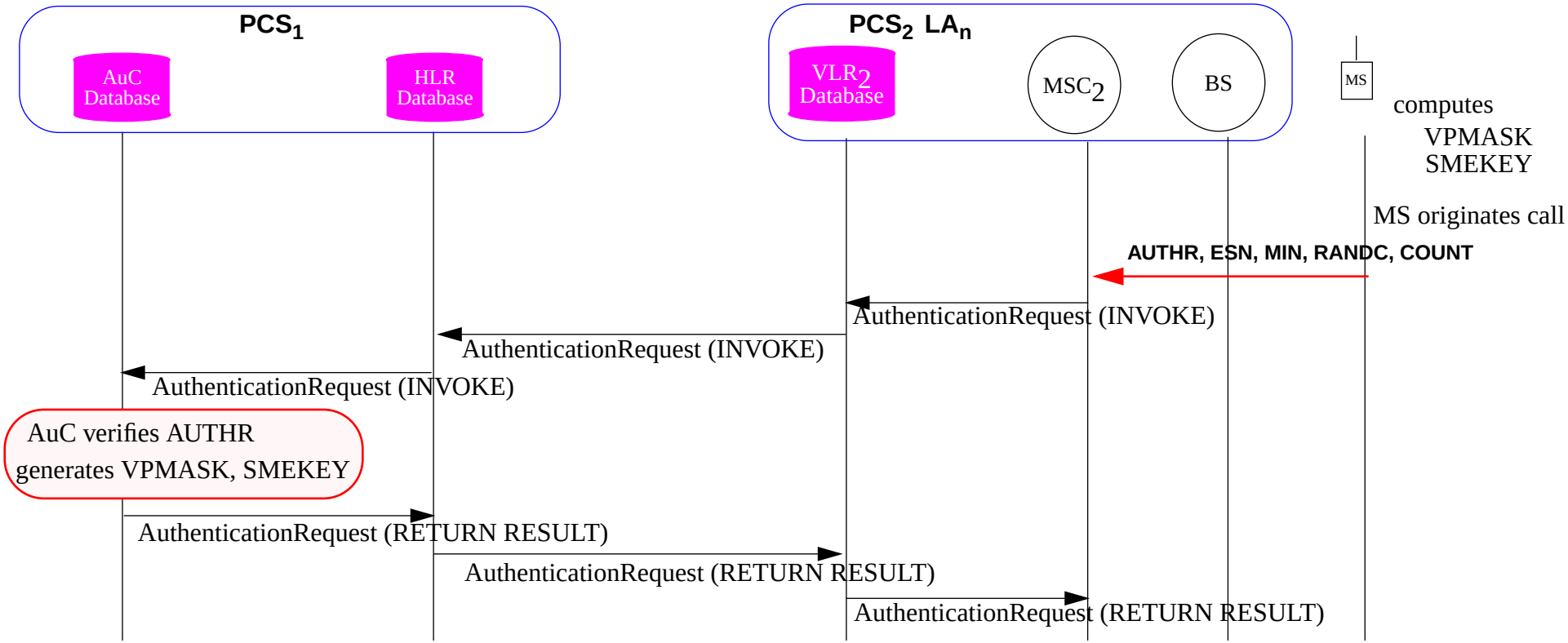


Figure 17: Mobile places a call in PCS_2

Because of SSD the AuC can generate the same Voice Privacy Mask (VPMASK) and Signaling Message Encryption Key (SMEKEY) as the mobile and passes this information to the operator of PSC_2

Sharing Scheme

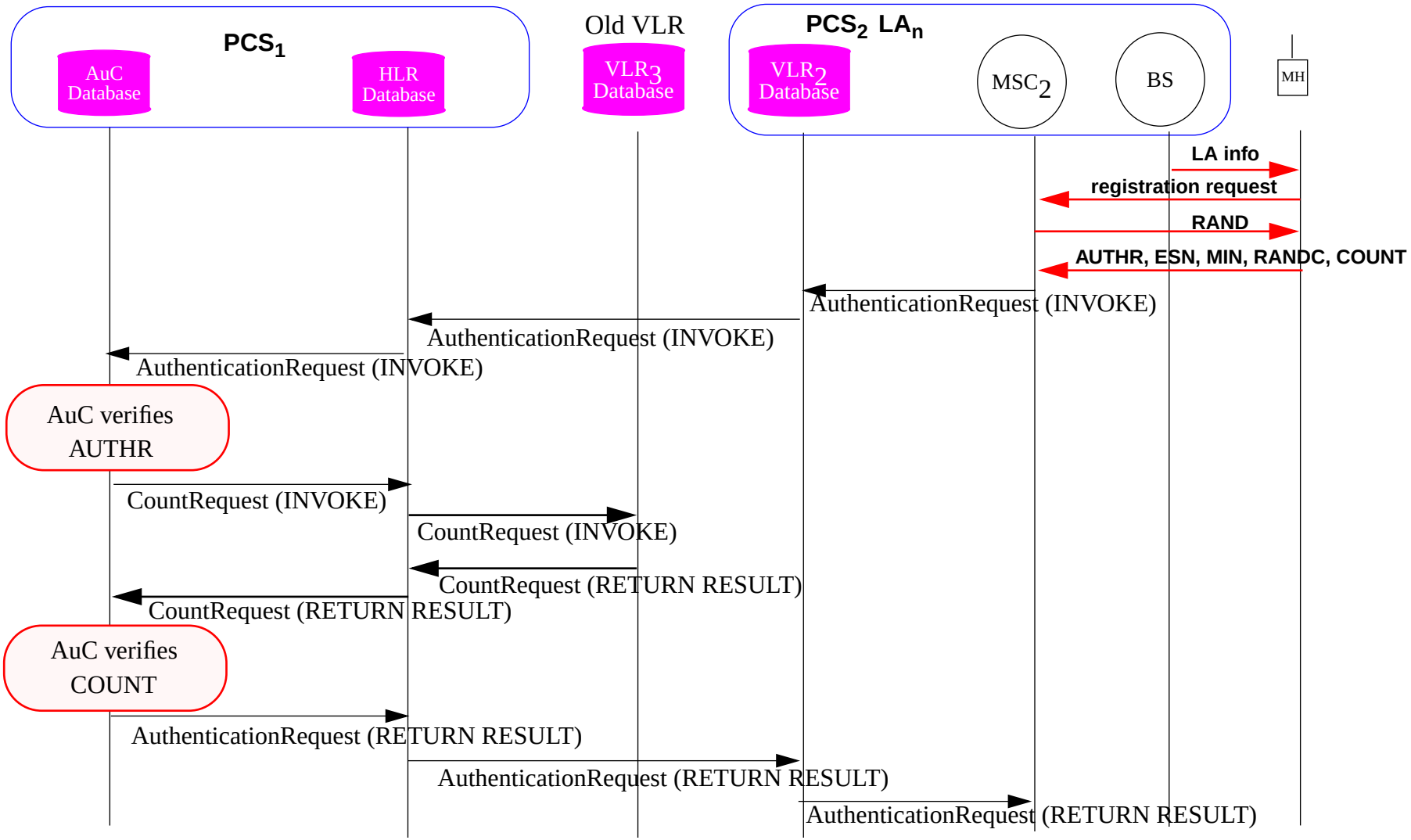


Figure 18: Mobile moves into a new Location Area (LA) at PCS_2 registration using Sharing scheme

Sharing Call Origination

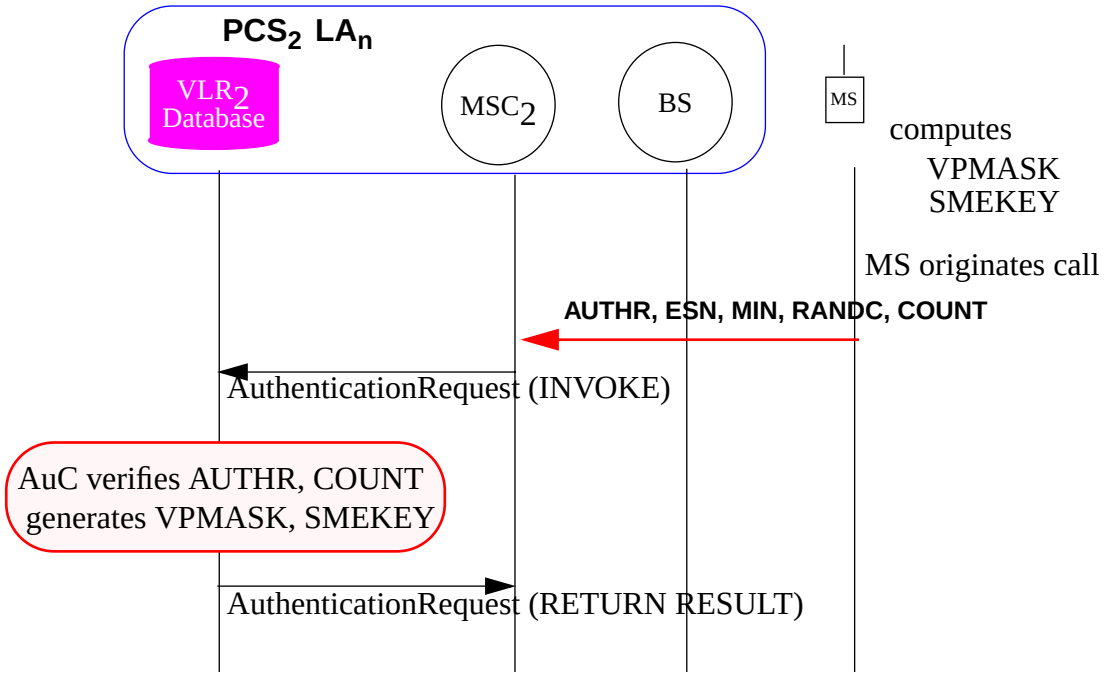


Figure 19: Mobile places a call in PCS_2 using sharing scheme

Note that because the visited system shares the SSD, it no longer has to contact the home PCS's AuC to generate the VPMASK and SMEKEY

When should you use Without-Sharing vs. Sharing

Use Without-Sharing when number of registration operations greater than the number of call origination/termination.

Can use an adaptive algorithm:

- based on statistics move between Without-Sharing and Sharing schemes
- once you make a call, then use Sharing scheme; but if you move without making a call, then revert back to Without-Sharing scheme

Cellular Authentication and Voice Encryption (CAVE) Algorithm

IS-54B - TDMA standard - includes CAVE algorithm

Computes Authentication Result (AUTHR) using SSD, ESN, MIN, a random number (RAND).

RAND is typically updated in the system every 20 minutes and SSD is updated for each mobile every 7 to 10 days [22].

3 of the 4 IS-54 algorithms have been broken:

- David Wagner (then a University of California at Berkeley graduate student, now faculty member) and Bruce Schneier[1] & John Kelsey (both of Counterpane Systems) announced that they had broken the **Cellular Message Encryption Algorithm** (CMEA)[24] which is used to protect the control channel (for example, dialed digits, alphanumeric pages).

1. Author of the popular book *Applied Cryptography.*

- D. Wagner, L. Simpson, E. Dawson, J. Kelsey, W. Millan, and B. Schneier, “Cryptanalysis of ORYX”[25] - shows that the stream cipher used to protect data is breakable with a plain text attack.
- voice privacy depends on a XOR against a generated string - which is generally rather easy to break (as the string is not equal to the message length)

PACS Network Signalling

Personal Access Communications Systems (PACS)

supports:

- basic call control
- roaming
- handoff management

Does **not** use MSCs or HLR/VLR, but uses Advanced Intelligent Network (AIN) protocol with an Access Manager (AM), AIN switch, and AIN **Service Control Point** (SCP).

PACS Architecture

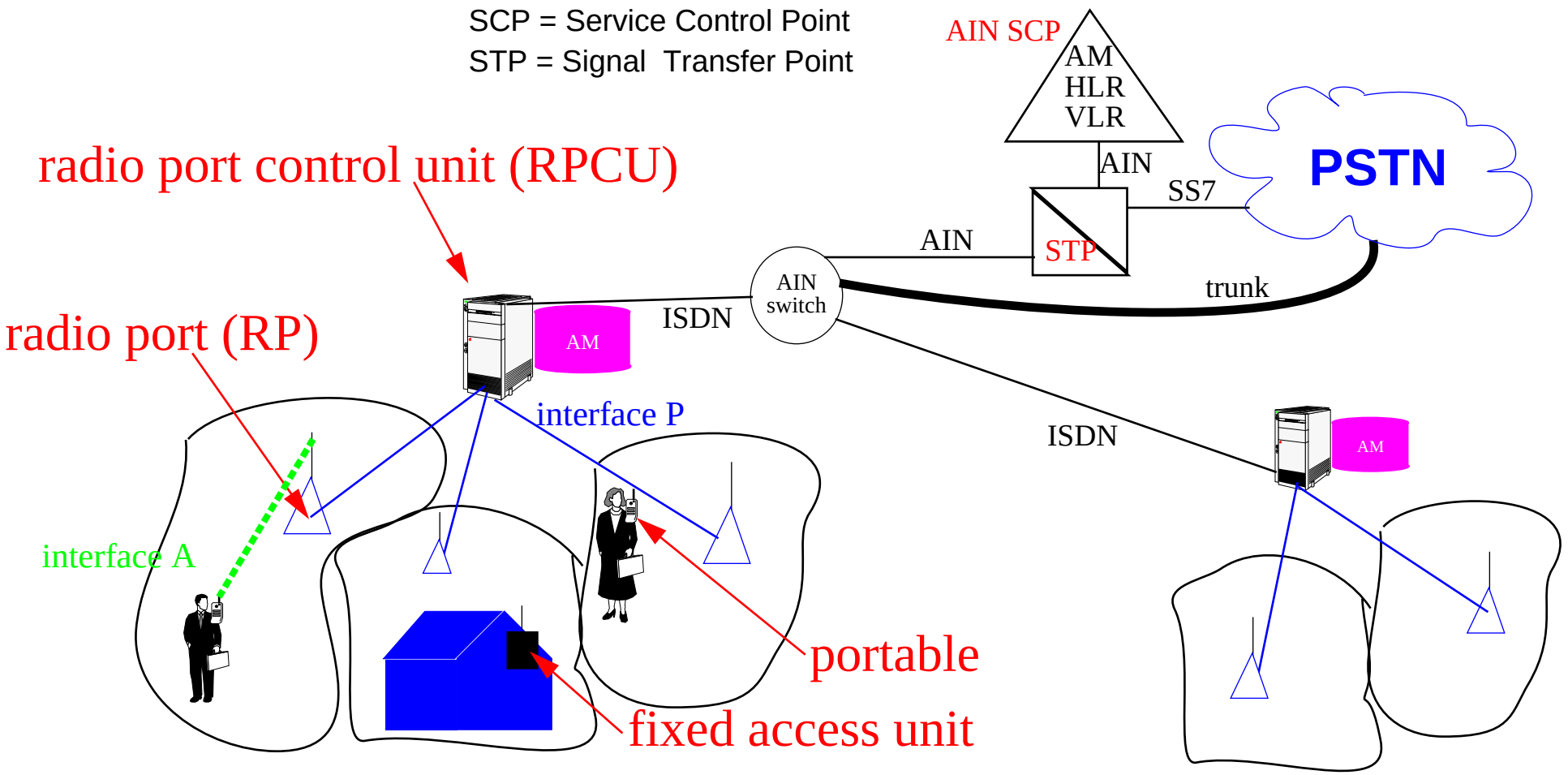


Figure 20: PACS Architecture

Access Manager (AM)

The access manager in the **radio port control unit** (RPCU), it provides:

radio control	managing the RPs, trunk provisioning, RP to RP link transfers
non-radio service control	call control (managing the B channels), switching, routing

The RPCU has to deal with **inter-RPCU** handoff (similar to inter-BSC handoff) and inter-radio port (**inter-RP**) handoff.

Note: an AM is also located in the AIN SCP; the two interact with the ISDN/AIN Switch providing tunneling/de-tunneling (i.e., encapsulation) of the ISDN REGISTER messages over AIN.

Pg. 125 notes that the RPCUs could be connected via an IP network to the VLR, thus by passing the AIN/ISDN Switch (SSP) for all non-call associated (NCA) signalling.

AIN/ISDN Switch

Note: The textbook often refers to this as the AIN Service Switching Point (SSP).

Uses:

- SS7 ISUP to set up trunk and for **inter-system** handoff
- SS7 TCAP to support mobility management and transport AIN messages between switch and SCP; the AIN messages are basically remote procedure calls (RPC) calls to the SCP
- ISDN for:
  - call control {standard ISDN},
  - automatic link transfer (ALT) {**FACILITY** message for **handoff**}, and
  - non-call associated (NCA) signalling {for example, communication between RPCU and VLR for registration and authentication - **REGISTER** message - which is encapsulated in an AIN NCA-Data message}

Also provides:

- Automatic Code Gaping (for traffic load control)
- Automatic Message Accounting (for access charging)

AIN Service Control Point (SCP)

Provides service logic, databases, and operations to support:

- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Access Manager (AM)
- Authentication Center (AuC)

Communicates with:

- the switch via AIN TCAP
- external PCS databases via IS-41 protocol

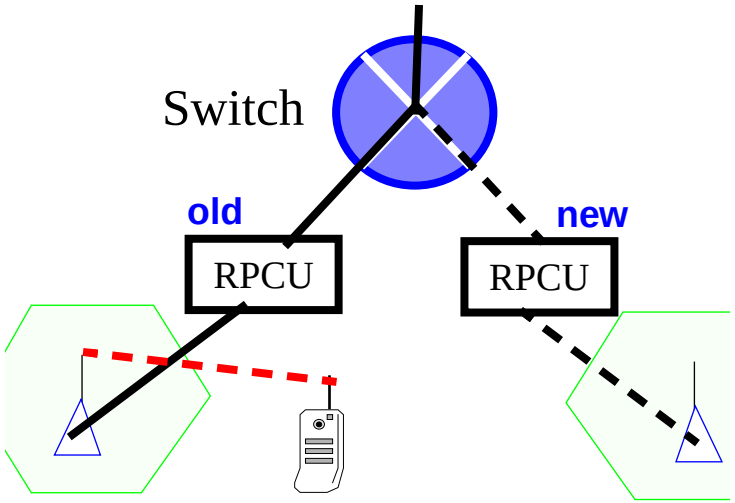
PACS Intersystem Handoff

PACS Intersystem Handoff/automatic link transfer (ALT) follows IS-41 anchor switch approach.

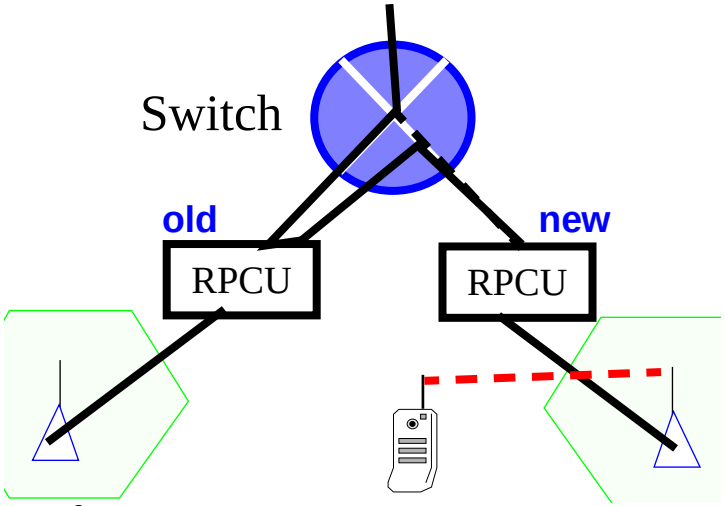
3 alternative inter-RPCU handoff methods

(Switch Loopback, Direct Connection, Three-way Calling Connection):

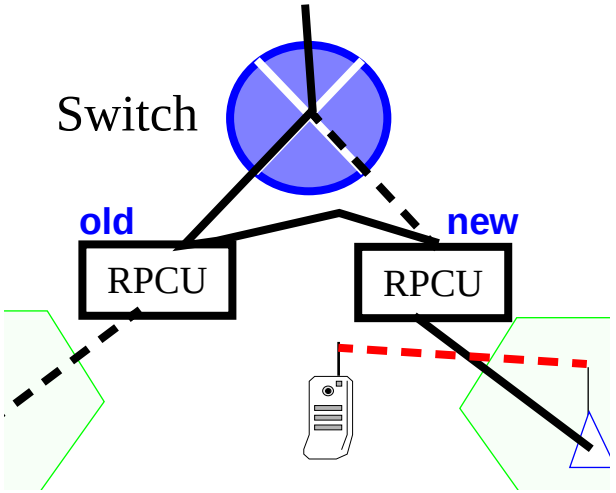
a. Before ALT



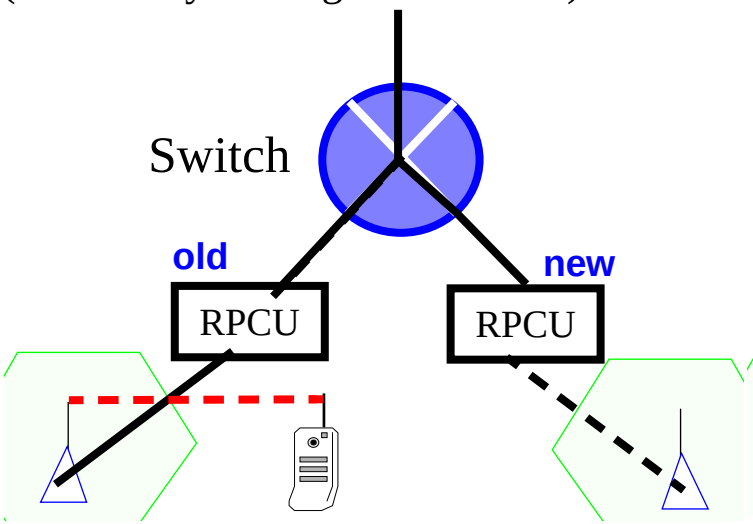
b. After ALT (Switch Loopback)



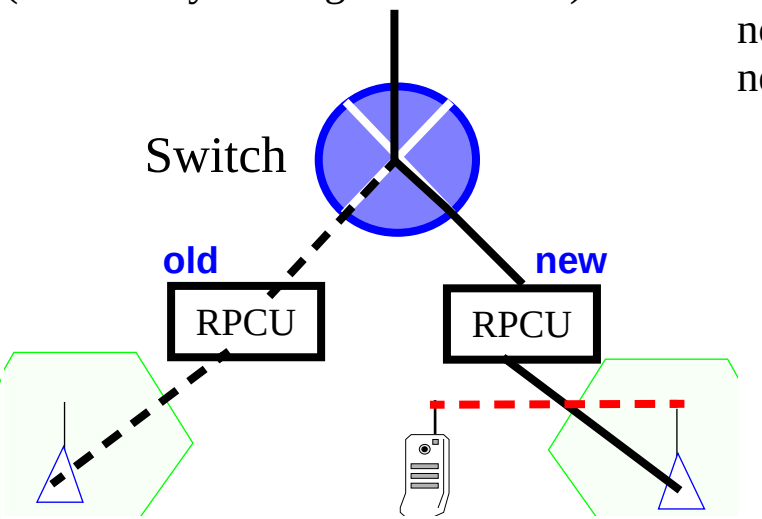
c. After ALT (Direct Connect)



d.During ALT
(Three-Way Calling Connections)



e. After ALT
(Three-Way Calling Connections)



Note: (d) illustrates that the switch is doing bridging, but the traffic is not using any radio capacity in the new cell - until the mobile arrives

CDPD

In 1992, AT&T Wireless Services developed the **cellular digital packet data** (CDPD) protocol, a **data-only** protocol that (re-)uses the AMPS or IS-136 network. Packets (typically ~1.5 kilobytes) use vacant cellular channels - either an assigned channel or between calls.

CDPD **does not** communicate with the underlying network; but **does** utilize knowledge of this network's channel assignment algorithms to predict when channels will be available for CDPD's use.

Mobile Data Base Stations - do **channel sniffing** to find idle channels

It is essentially an implementation of Mobile*IP [28] .. [30].

Motivation for CDPD

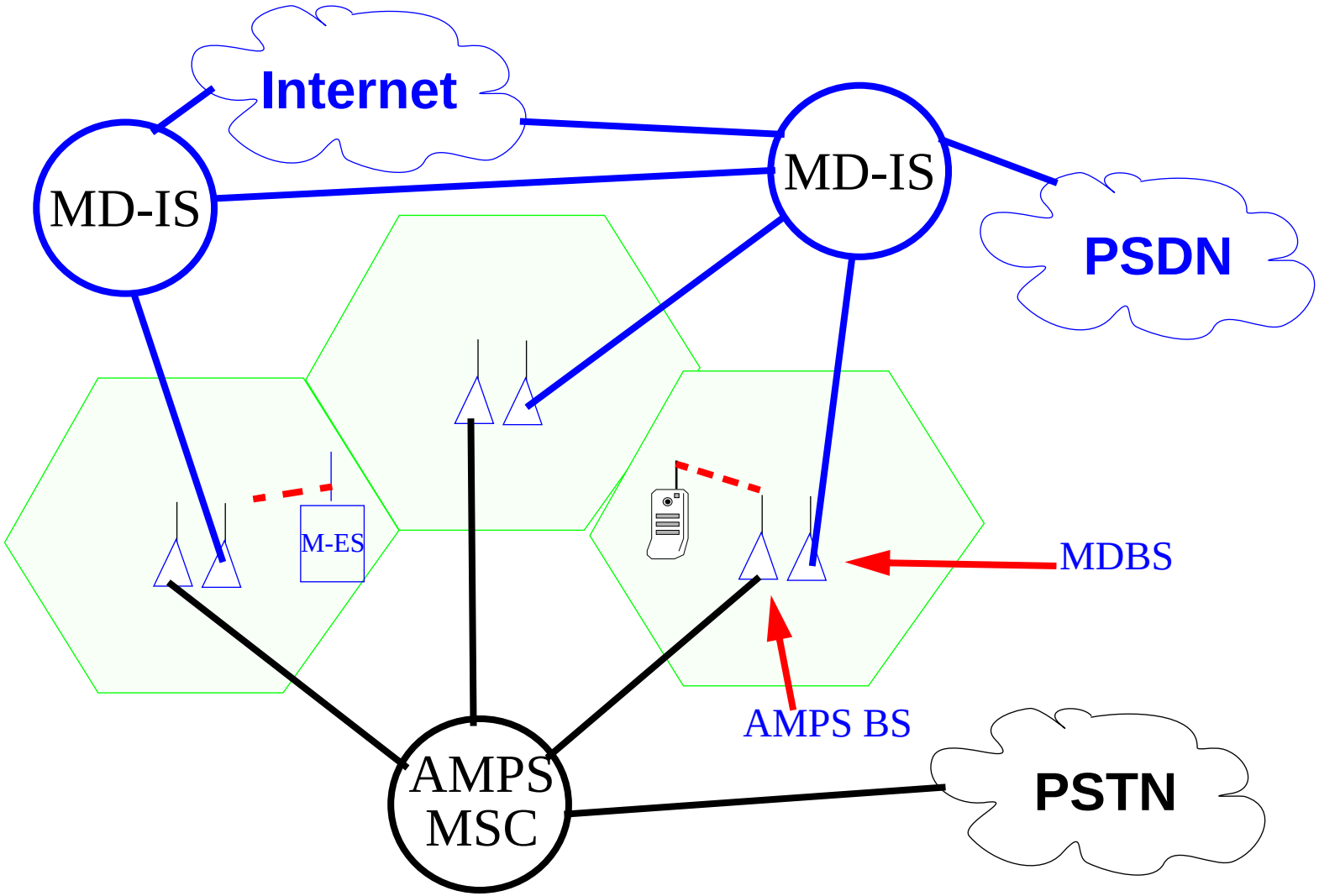
- Most traditional cellular systems (such as AMPS) are unsuited for packet data
  - Long call setup times - many seconds (vs. CDPD with from under 1 to 4 seconds)
  - Modem handshaking required - this modem training can often take more time than the data transfer time!
  - Analog providers already have AMPS frequency allocation
- Re-use AMPS channels to provide data service.
  - Must not interfere with existing analog service (viewed as operator's bread and butter)
  - no new spectrum license needed - but you get to make more money with the spectrum you already have (**IFF** you can share the spectrum wisely)

Goals

- low speed data: Paging, short message, e-mail, …(achieve 10-12kbps)
- broadcast and multicast (for example, for fleet management)
- “always on-line” packet data service
- transparent to existing AMPS service, but shares spectrum with it

CDPD network architecture

Mobile End System (M-ES), **Mobile Data Basestation** (MDBS), **Mobile Data -Intermediate System** (MD-IS)



CDPD Entities

Mobile End System (M-ES)

- Subscriber unit - interfaces with the radio at 19.2 kbps
- **Subscriber Identity Module** (SIM) - used to identify subscriber
- Mobile Application Subsystem - actually provides the functionality (could be a PDA, Laptop, embedded processor, …)

Mobile Data Base Station (MDBS)

- controls the radio: radio channel allocation, channel usage, …
- one modem/transceiver per radio channel pair (up & down link)
- generally co-located with the AMPS basestations (so they can share antenna, site, …)

Mobile Data-Intermediate System (MD-IS)

- frame relay switch + packet router
- buffers packets destined to M-ES it knows about (== with TEI assigned)
- supports user mobility by a mobile location protocol

other entities

Fixed End System (F-ES) - hosts

External F-ESs	traditional non-CDPD host(s)	
Internal F-ESs	hosts **within** the boundaries of the CDPD network; they have access to additional internal network data (usage accounting information, mobile location information, subscriber authentication information, …	
	Accounting Server (AS)	collection and distribution of usage accounting data (each MD-IS periodically sends its usage information to the AS)
	Authentication Server	supports the authentication function in CDPD; may or may not be a part of the MD-IS
	Directory Server	supports directory services within the CDPD network (could support DNS and/or X.500)
	Network Management System	includes configuration management, fault management, performance management and other functions

Limits

- No direct **Mobile End System** (M-ES) to M-ES communication
- radius of a CDPD cell is limited to <10 miles (i.e. < 17km)
- each M-ES can only send two packets back to back - to avoid hogging the channel

Handoffs

Mobile Data Base Station (MDBS) broadcasts a list of **available** channels

When M-ES finds link quality has dropped below a threshold, it checks the channels from the MDBSs that it can hear; if there is a better channel it initiates a link transfer - by switching to the new channel and registering with the new MDBS

MD-IS maintains a **registration directory**

- contains a list of **Temporary Equipment Identifiers** (TEI)
- associated with each TEI is a element **in**activity timer (T203)
- associated with each radio channel stream is a TEI notification timer (T204) - when this timer goes off MD-IS broadcasts a list of TEI's with data buffered for them {mobiles with nothing to send can *sleep* until the next TEI notification frame}
- when a mobile wakes up and hears that there is data for it, it sends a **Receiver Ready** (RR) frame

Connectionless Network Services (CLNS)

CDPD supports both:

- ISO connectionless network protocol
- IP

Roaming Management

Each M-ES has a unique **Network Equipment Identifier** (NEI) which is associated with a home MD-IS (**Mobile Home serving Function** (MHF) {analogous to a Mobile IP **Home Agent**}.

Home MD-IS keeps **location directory** of the MD-IS currently serving each of its mobiles (note that the routing is to the current MD-IS, **not** to the M-ES itself)

Each MD-IS keeps a registration directory listing currently visiting mobile (**Mobile Serving Function** (MSF)) {analogous to a Mobile IP **Foreign Agent**}

When a M-ES moves, the home MD-IS *explicitly* cancels the registration at the former MD-IS.

Packet routing is handled just as in Mobile IP.

Multicast

CDPD has explicit provisions for Multicast and enables mobiles to register for a multicast NEI - this must include a **Group Member Identifier** (GMID) which is unique with in the group

Details at: *http://www.leapforum.org/published/internetworkMobility/split/node75.html*

CDPD Modems

	Price	
Sierra Wireless AirCard® 300	$479	http://www.sierrawireless.com/
Novatel Merlin™ CDPD Minstrel S™ and Minstrel V™	$299	http://www.novatelwireless.com/

CDPD usage

- Very popular for vending machines
- Public safety agencies, Law enforcement, …
  - “because police officers rarely roam outside their well-defined geographic patrol areas”[1]
- Handheld/laptop IP access

Price Plans: was from $14.95 per month for 250 kilobytes to $39.95 monthly for unlimited usage with a two-year commitment

Of course if you are vending machine you don’t buy an unlimited plan, but perhaps if you are vending machine operator you do.

Operators and coverage maps

http://www.novatelwireless.com/support/CDPD%20Tech.html

1. *http://www.proberesearch.com/alerts/2002/wlsdata.htm*

CDPD phaseout

By 2002 GPRS (see page 194) has displaced CDPD. With >85% of US subscribers using digital phones ⇒ the AMPS analog networks have decreasing importance and US FCC will allow carriers to phase out their analog networks.

In March 2002, Verizon Wireless announced rate plans for the service based on data transmission volume as part of their rollout of next-generation wireless networks. CDMA 1X (code division multiple access) Express Network pricing:

- $35 a Month for 10 MB
- $55 per month for 20 MB, and
- fees available for up to 150 MB of data
- $99 a month for unlimited service
- data transmission speeds of up to 144 kilobits per second (kbps), with an average transmission rate of 40 to 69 kbps.

Sprint PCS and others have similar services.

Ricochet[1]

Aerie Networks bought the network assets of Metricom at bankruptcy sale. Currently service exists in Denver and San Diego. (Previously 17 market areas)

The 128kbps network uses a microcellular-packet-switching, FHSS (Frequency Hopping Spread Spectrum) technology, and is designed for forwarding IP packets.

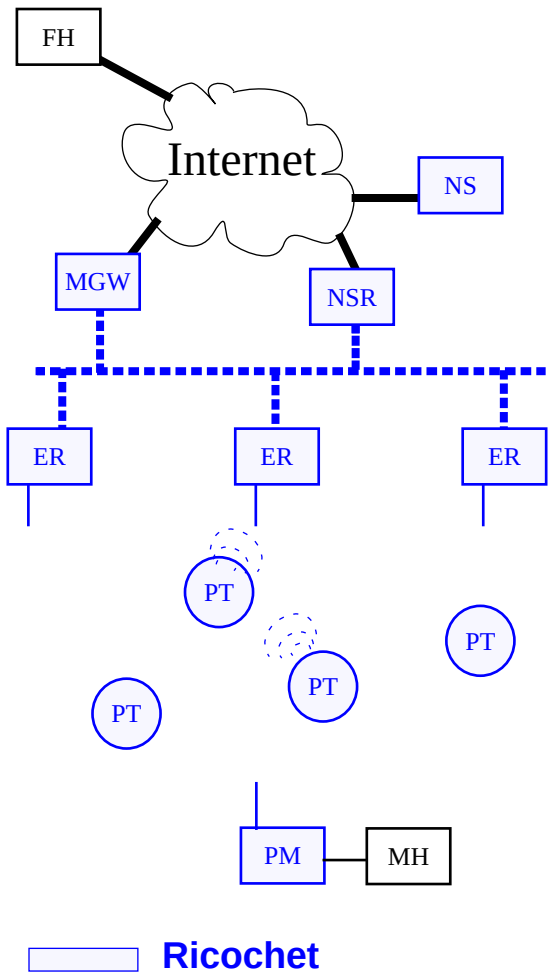
- Transceivers are deployed in a mesh topology, generally on top of streetlights (for power and low cost space!)
- Designed to be self-configuring and do load-balancing (including routing traffic around congested transceivers)
- $44.95 a month for unlimited use
- authentication first using modem's serial number and then via user account and password
- Mean RTT 2450 ms, std. deviation 1500 ms; UDP peak 50-58 kbps

Developed in 1985 for remote meter reading, 1994: 28.8 kbps, 2000:128 kbps

1. *http://www.ricochet.com/*

Ricochet System Architecture

Portable Modems (PM)	Connects the mobile host to the Ricochet network; acts like modem with an extended Hayes AT command set
Pole Top Radios (PT)	Route packets over a wireless link towards or from the nearest wired access point; routing is performed geographically, i.e., based on the latitude and longitude of the pole top radios (PTs) with respect to the final destination.
Ethernet Radios (ER)	Bridges between the wireless and wired portion of the network
Metricom Gateway (MGW)	Maps between IP addresses and Ricochet identifiers and encapsulates packets within Metricom-specific headers and routes the packets to the correct ER. For packets originating from a mobile, decapsulates and forwards the packets on the wired IP network.
Name Server Router (NSR)	Serves as a router to the system name server.
Name Server (NS)	Validate the subscription, based on the PM identification number, and validates service requests.



Further reading

TIA

[20] TIA public documents
ftp://ftp.tiaonline.org/TR-45/TR45AHAG/Public/

TSB-51

[21] Cellular Telecommunications & Internet Association (CTIA) World of Wireless Communication, *http://www.wow-com.com/*

[22] Jey Veerasamy, Cellular Authentication, University of Texas at Dallas, *http://www.utdallas.edu/~veerasam/cs6385/authentication.ppt*

[23] Yi-Bing Lin, Seshadri Mohan, Nelson Sollenberger, and Howard Sherry, "Adaptive Algorithms for Reducing PCS Network Authentication Traffic", IEEE Transactions on Vehicular Technology, 46(3):588-596, 1997. *http://liny.csie.nctu.edu.tw/ieee-tvt94c.ps*

[24] David Wagner, Bruce Schneier, and John Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm", Crypto'97, 1997.

http://www.counterpane.com/cmea.pdf

[25] D. Wagner, L. Simpson, E. Dawson, J. Kelsey, W. Millan, and B. Schneier, "Cryptanalysis of ORYX", SAC'98, http://www.cs.berkeley.edu/~daw/papers/oryx-sac98.ps

[26] David Wagner http://http.cs.berkeley.edu/~daw/

[27] CAVE algorithm ftp://ftp.ox.ac.uk/pub/crypto/misc/CAVE.tar.gz

Mobile*IP

[28] J. Ioannidis and G. Q. Maguire Jr., The Design and Implementation of a Mobile Internetworking Architecture. eds. Dejan S. Milojicic, Frederick Douglis, and Richard G. Wheeler, Mobility Processes, Computers, and Agents, Addison-Wesley Pub Co., ACM Press Series, February 1999, 365-377. {Reprint of J. Ioannidis and G. Q. Maguire Jr., The Design and Implementation of a Mobile Internetworking Architecture.USENIX Winter 1993 Technical Conference, pages 491-502. USENIX Association, January, 1993.}

[29] John Ioannidis, Dan Duchamp, and G.Q. Maguire Jr. IP-based Protocols for Mobile Internetworking. *SIGCOMM'91 Conference: Communications Architectures and Protocols*, pages 235-245. Association for Computing Machinery, September, 1991.

[30] John Ioannidis, *Protocols for Mobile Internetworking*, Doctoral Dissertation, Department of Computer Science, Columbia University, 1993.

CDPD

[31] Mark S. Taylor, William Waung, Mohsen Banan, *Internetwork Mobility: The CDPD Approach*, Pearson Education, Inc., June 11, 1996
http://www.leapforum.org/published/internetworkMobility/split/main.html

- Note that this is an on-line version of the entire 300 page book!

[32] A. Salkintzis, “Packet Data over Cellular Networks: The CDPD Approach”, *IEEE Communication Magazine*, vol. 37, no. 6, June 1999, pp. 152-159.

[33] Sun Jong Kwon, Yun Won Chung, and Dan Keun Sung, “Performance Analysis of CDPD Sleep Mode for Power Conservation in Mobile End Systems”, IEICE Trans. on Communications, VOL. E84B, no. 10, Oct. 2001

[34] Y. Frankel, A. Herzberg, P. A. Karger, H. Krawczyk, C. A. Kunzinger, and M. Yung. Security issues in a CDPD wireless network. IEEE Personal Communications. Volume 2, Number 4, August 1995. pp. 16-27. For a short summary of this paper see:
http://swig.stanford.edu/pub/summaries/wireless/security_cdpd.html

Ricochet

[35] Elan Amir and Hari Balakrishnan, “An Evaluation of the Metricom Ricochet Wireless Network”, CS 294-7 Class Project,
http://www.lariat.org/Berkeley/node2.html

[36] Elan Amir and Hari Balakrishnan, “Performance of the Metricom Ricochet Wireless Network”, Summer 1996 Daedalus Retreat, June 1996,
http://daedalus.cs.berkeley.edu/talks/retreat.6.96/Metricom.pdf

KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

3. GSM, GPRS, SMS, International Roaming, OAM

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Last modified: 2003.03.13:11:56

Lecture 3

- GSM (Chapters 9,10, and11), GPRS (Ch. 18), SMS (Ch. 12), International Roaming (Ch. 13), Operation/Administration/Maintenance (Ch. 14)

Global System for Mobile Communications (GSM)

- designed to be a **digital** (**wide area**) **wireless network**
- driven by european telecom manufacturers, operators, and standardization committees
- very widely used around the world

GSM Requirements

- Service portability
  - mobile should be able to be used in any of the **participating** countries with international roaming and standardized numbering & dialing (but possibly at different rates!)
  - usable for both wireline services and for mobile service
  - usable when: walking, driving, boating, … (upto 250 km/h)
- Quality of service and Security
  - quality at least as good a previous analog systems
  - capable of offering encryption (in some countries this is **off** by default)
- Good radio frequency utilization
  - high spectrum efficiency
  - co-existence with earlier systems in the same bands
- Modern network
  - follows ITU recommendations - to allow efficient interoperation with ISDN networks
  - supports voice and low rate data
  - standardized mobility and switching support
  - standardized **interfaces** between the subsystems - to allow a mix-and-match system
- System optimized to limit cost of mobiles (and to a lesser extent to limit the cost of the whole system)
  - GSM required higher complexity mobiles than earlier analog systems
  - subscriber cost is less than or equal to the then existing analog systems

GSM Architecture

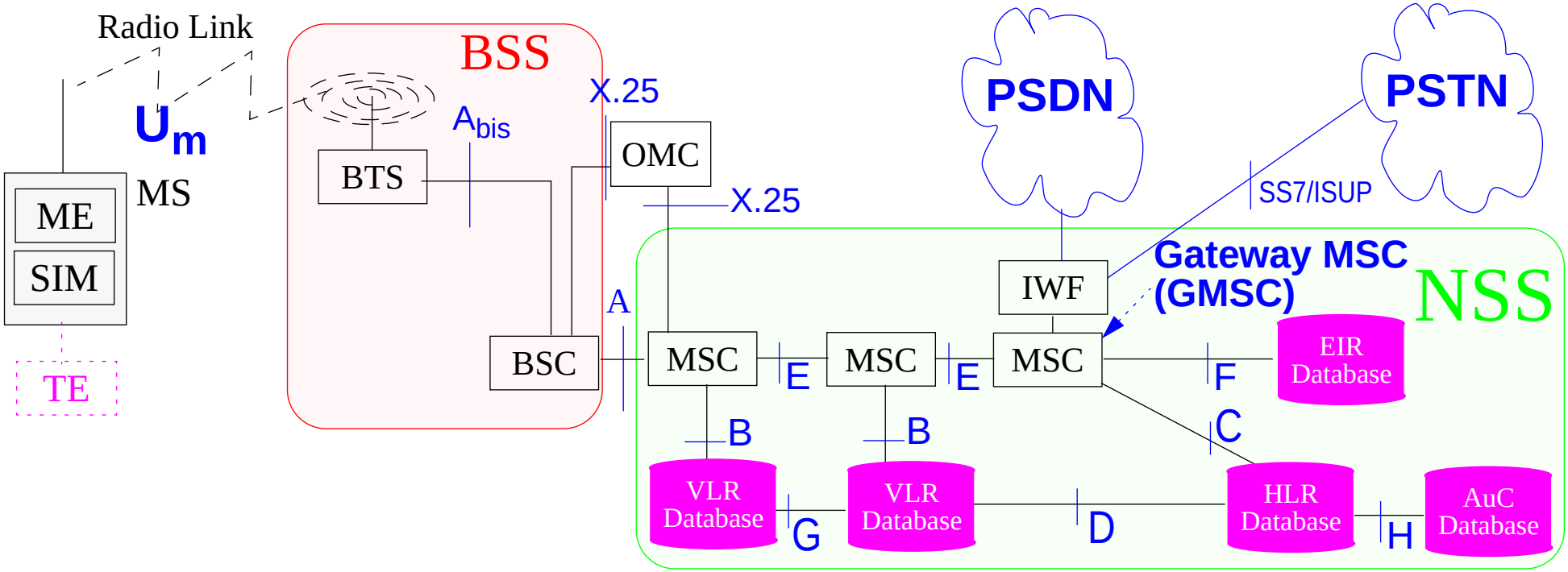


Figure 21: GSM Architecture

MS	Mobile Station
BSS	base station system
NSS	network and switching subsystem

Foundation

- Hybrid frequency-division/time-division multiple access
  - FDMA - division by frequency of the (maximum) 25 MHz allocated bandwidth into 124 carrier frequencies spaced 200 kHz apart.
    - One or more carrier frequencies assigned to each base station
  - Each carrier frequency divided in time, using TDMA
  - Fundamental unit of time in this TDMA scheme is a burst period approx. 0.577 ms long
  - Eight burst periods are grouped into a TDMA frame (approx. 4.615 ms) = basic unit for the definition of logical channels
  - A physical channel is one burst period per TDMA frame
  - Slow frequency hopping at upto 217 times per second
    - hopping algorithm is broadcast on the broadcast control channel
    - helps alleviate multipath fading
    - co-channel interference is effectively randomized
    - Note: broadcast and common control channels are not subject to frequency hopping and are **always** transmitted on the same frequency
- Infrastructure based on Signalling System 7 (SS7)

GSM contributions

- Location-based mobility management
- Mobile assisted handover
- Temporary Mobile Subscriber ID (TMSI)

Distinctive features of GSM

- Cooperative development by many actors from many countries
- preserved open interfaces between the subsystems (especially between infrastructure elements -- particularly between base stations and switches ⇒ lead to an open market for these subsystems)
- specified a large number of interfaces!
- Phased release - since they could not make all the innovations in time for their targeted 1991 introduction
  - Phase 1 GSM spec. - 100 sections and 5,320 pages!
    - telephony (full rate speech) - with some added features
    - emergency calls
    - data transmission at 2.4/4.8/9.6 kbps (transparent {the error correction done by a forward error correction (FEC) mechanism}/non-transparent {information is repeated when it has not been correctly received})
    - short message service (SMS)
  - Phase 2
    - non-voice services (Advice of charge, Calling line identification, Call waiting, Call hold, Conference calling, Closed user groups) and enriched telephony (half-rate speech)
    - High-speed circuit-switched data (HSCSD)

- Phase 2+
  - Multiple service profiles
  - Private numbering plans
  - Access to Centrex services
  - Internetworking with GSM 1800, GSM 1900, Digital Enhanced Cordless Telecom (DECT)
- Phase 2.5
  - GPRS: Global packet radio system
- Enhanced data rates for GSM (EDGE)

Mobile Station (MS)

- Subscriber Identity Module (SIM)
- Mobile Equipment (ME)
- Mobile Terminal (MT)

Subscriber Identity Module (SIM)

- small form factor - which can be removable and can be moved from one terminal to another (latest card connectors: >5,000 cycles)
  - smart card (generally too large for handsets!)
  - plug-in SIM (the processor and contact from a smart card)
- **user** authenticated via a **Personal Identity Number** (PIN)
- if PIN entered incorrectly, N times, then phone is locked for all but emergency calls, until you enter a **PIN unblocking key** (PUK)
- contains subscriber information:
  - some which is fixed by operator (may include preferred network provider(s))
  - some which is changeable by the user (list of short numbers, phone list, SMS messages, …)
- can be updated via:
  - keyboard or attached terminal equipment or **over the air** (OTA) via SMS message sent by operator/application/… built using SIM Toolkit
- often the SIM is owned by the operator
- profiles - operator/subscription info; SIMs are required to be able to hold at least two profiles
- contains **International Mobile Subscriber Identity** (IMSI)

Mobile Equipment (ME)

“the phone” itself - radio and radio interface, display, keyboard, etc.

performs: radio transmission and reception, authentication, handover, encoding and channel encoding.

note: ME without a SIM can **only** make emergency (112) calls

Radios operate in one or more of the following bands:

System	Uplink (mobile station to base station) (MHz)	Downlink (base station to mobile station) (MHz)	Comments
GSM900	890..915	935..960	the original frequency band
GSM1800	1710..1785	1805..1880	also known as DCS1800
GSM1900	1850..1910	1930..1990	also known as PCS 900

ME identified by **International Mobile Equipment Identity** (IMEI)

Power saving and interference reduction

- To reduce the MS's power consumption and minimize interference on the air interface, during pauses in speech the MS does not transmit - this is called: **Discontinuous transmission** (DTX)
  - "Comfort noise" is artificially generated locally by the MS
- **Discontinuous reception** (DRX)-mobile listens to the paging channel, but only needs to wake up for its sub-channel of the paging channel
- To minimize co-channel interference and to conserve power, both the mobiles and the base transceiver stations operate at the lowest power level that will maintain an acceptable signal quality
  - Power levels can be stepped up or down in steps of 2 dBm from the peak power for the class down to a minimum of 13 dBm (20 milliwatts for MS)
  - only one step at a time and each step takes 60ms
  - there are 16 power levels (i.e., 30 db of range)
  - terminal is typically only transmitting in one time slot (i.e., 1/8 of the time - so its radiated power is on average 8db lower than the set power level)
  - Both mobile station and BTS continually measure the signal strength or signal quality (based on the **bit error ratio**), and pass the information to the base station controller (BSC) which actually manages the power levels.

Classmark

32 bit quantity indicating properties of a mobile station

- revision level
- RF power capability

Figure 22: Power classes

Class	GSM900	DCS1800	
1	20 W	1 W	vehicle mounted systems
2	8 W[a]	0.25 W	vehicle mounted systems
3	5 W		
4	2 W[b]		portable terminals
5	0.8 W		

a. 1W average if using a single time slot per frame

b. 250mW average if using a single time slot per frame

- (available) encryption procedures
- frequency capabilities (i.e., which bands)
- if the device is SMS capable

User ID ≠ Device ID

IMEI	**International Mobile Equipment Identity**	15 digits
IMSI	**International Mobile Subscriber Identity**	15 digits
TMSI	**Temporary Mobile Subscriber Identity**	32 **bits**

An important distinction in GSM is that due to the SIM card the user (or at least IMSI) can be identified separately from the device (MS).

TMSI is assigned by the VLR to a visiting subscriber

IMEI consists of:

- Type Approval Code (TAC)
- Final Assembly Code (FAC) to identify the final assembly plant
- Serial number - allocated to the manufacturers.

Mobile Terminal (MT)

Generally a PDA, PC, …

Interface: serial (DTE-DCE) cable, PCMCIA, IrDA, Bluetooth, …

Some of the extended Hayes AT command set:

AT Command	Description	AT Command	Description
+CNMI	New message indication to TE	+CMT	SMS Message Received
+CBM	New Cell-Broadcast Message (CBM)	+CNMA	New Message ACKnowledgement to ME/TE
+CMGC	Send Command	+CPMS	Preferred Message Storage
+CMGD	Delete Message	+CSCA	Service Center Address
+CMGL	List Message	+CSCB	Select Broadcast Message Type
+CMGR	Read Message	+CSDH	Show Text Mode Parameters
+CMCS	Send Message	+CSMP	Set Text Mode Parameters
+CMGW	Write Message to Memory	+CRES	Restore Setting

Base Station System (BSS)

- one or more base transceiver station (BTS) and
- base station controller (BSC)

Base transceiver station (BTS)

Performs: channel coding/decoding and encryption/decryption

BTS includes: radio transmitters and receivers, antennas, the interface to the PCM facility (i.e., backhaul for the voice and control to the BSC), …

About 1/2 the processing is associated with transcoding PCM encoded speech channel to/from GSM coding

Base station controller (BSC)

BTSs are connected to a BSC which manages the radio resources

- call maintenance using the received signal strength sent by mobile stations normally every 480 ms
- initiate handovers to other cells,
- change BTS transmitter power, …

Task breakdown:

call activities	~20-25%
paging and SMS	~10-15%
mobility management	~20-25%
hardware checking/network triggered events	~15-20%

BSCs engineered for about 80% utilization, if overloaded, shed load by: (1) rejecting location updates, (2) rejecting MS originating calls, and (3) ignoring handoffs

Network and Switching Subsystem (NSS)

- MSCs
  - Gateway MSC (GMSC) has interconnections to other networks
- Databases
- Gateways

Databases

Home Location Register (HLR)	database for management of mobile subscribers, stores the international mobile subscriber identity (IMSI), mobile station ISDN number (MSISDN) and current visitor location register (VLR) address keeps track of the services associated with each MS an HLR may be used by multiple MSCs
Visitor Location Register (VLR)	caches some information from the HLR as necessary for call control and service provisioning for each mobile currently located in the geographical area controlled by this VLR connected to one MSC and is often integrated into the MSC
Authentication Center (AuC)	a protected database which has a copy of the secret key stored in each subscriber's SIM card this secret is used for authentication and encryption over the radio channel normally located close to HLR
Equipment Identity Register (EIR)	contains a list of all valid mobile station equipment within the network, where each mobile station is identified by its international mobile equipment identity (IMEI) - split into 3 databases: • White list: all known, good IMEIs • Black list: bad or stolen handsets • Grey list: handsets/IMEIs that are uncertain

Equipment Identity Register (EIR)

Optional in a GSM network, i.e., **not** required

EIR block (bars) calls from a particular MS, **not** from a subscriber.

Sometimes the AuC and EIR are combined.

Operation Sub-System (OSS)

- Operation and Maintenance Center
- Service management
  - subscription management for registering new subscriptions, modifying and removing subscriptions, as well as billing information
  - billing
  - fraud detection
  - …

Operation and Maintenance Center (OMC)

Manages the GSM functional blocks: MSC, BSC (and indirectly the BTSs)

Task: to maintain satisfactory operation of the GSM network

Based on observing system load, blocking rates, handovers, …

Activities:

- Network Management System (NMS)
  - modify network configuration
- equipment maintenance aiming at detecting, locating, and correcting faults

GSM Interfaces (just some of them!)

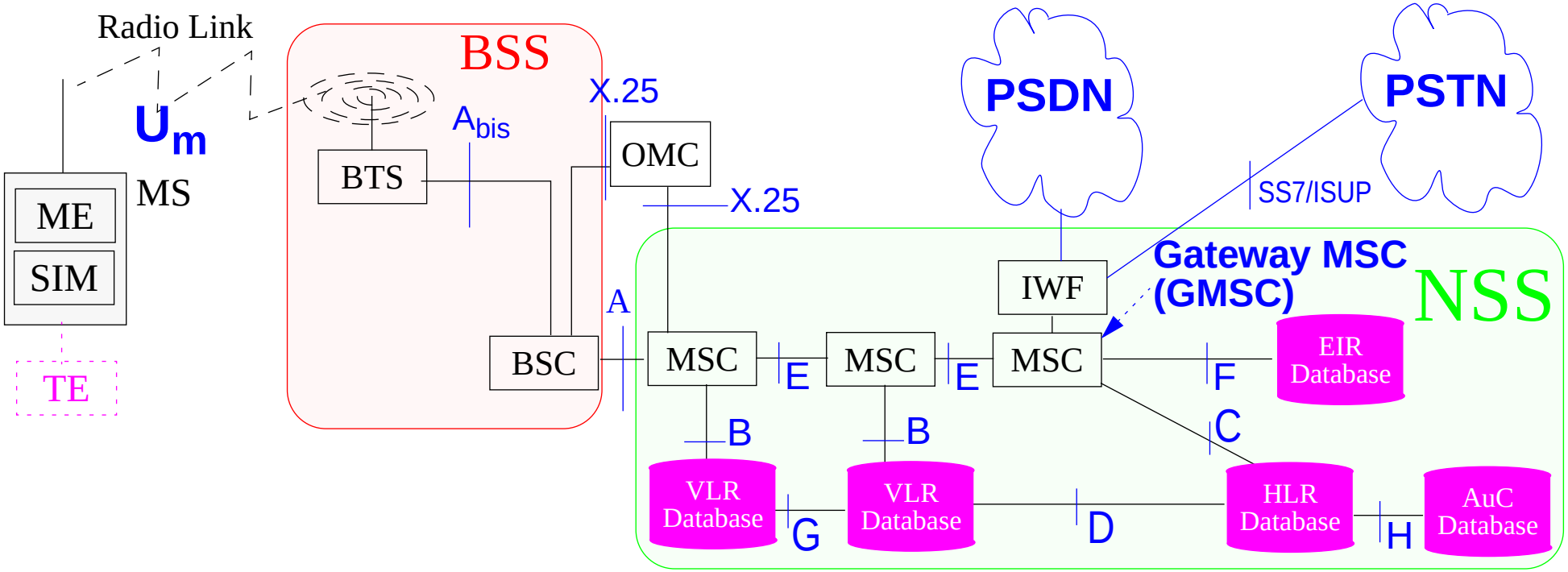
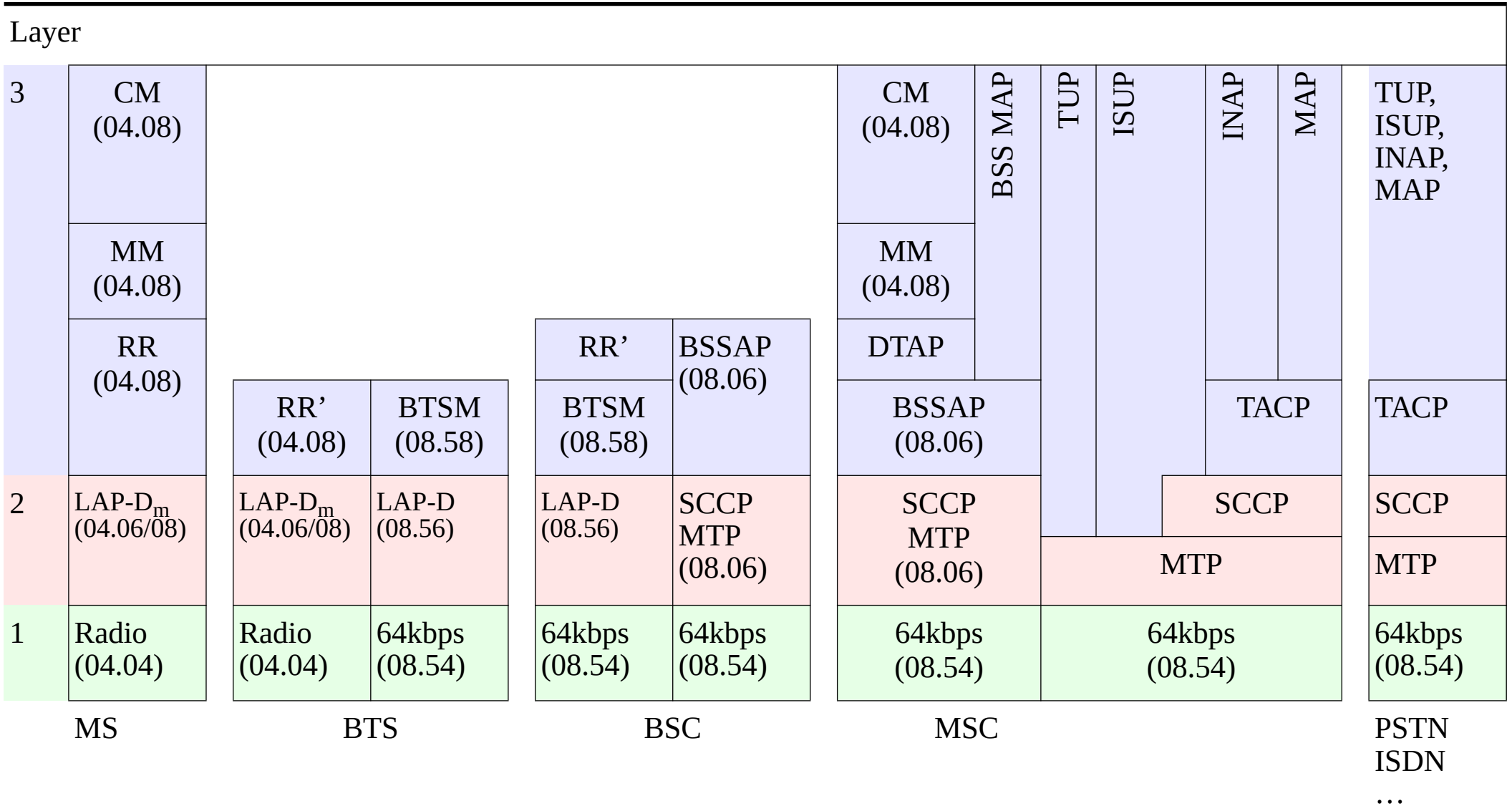


Figure 23: GSM Architecture

Interface	Description	Interface	Description
U_m	Radio link between MS and BTS	D	between HLR and VLR (MAP/TCAP)
A_{bis}	between BTS and BSC, PCM 2 Mbps, G. 703	E	between two MSCs (MAP/TCAP + ISUP/TUP)
A	between BSC and MSC, PCM 2 Mbps, G. 703	F	between MSC and EIR (MAP/TCAP)
B	between MSC and VLR (use MAP/TCAP protocols)	G	between VLRs (MAP/TCAP)
C	between MSC and HLR (MAP/TCAP)	H	between HLR and AuC



Numbers in parentheses indicate the relevant ETSI-GSM recommendations.

GSM Layers

- Layer 1: Physical layer
  - physical transmission
  - channel quality measurements
  - GSM Rec. 04.04, PCM 30 or ISDN links are used (GSM Rec. 08.54 on Abis interface and 08.04 on A to F interfaces)
- Layer 2: Data link layer
  - Multiplexing of layer 2 connections on control/signaling channels
  - Error detection (based on HDLC)
  - Flow control
  - Transmission quality assurance
  - Routing
- Layer 3: Network layer
  - Connection management (air interface)
  - Management of location data
  - Subscriber identification
  - Management of added services (SMS, call forwarding, conference calls, etc.)

GSM Air interface

- Layer 1 (GSM Rec. 04.04): Um interface
- Layer 2 (GSM Rec. 04.05/06): LAP-D_m protocol (similar to ISDN LAP-D):
  - connectionless transfer of point-to-point and point-to-multipoint signaling channels
  - Setup and tear-down of layer 2 connections of point-to-point signaling channels
  - connection-oriented transfer with in order delivery, error detection and error correction
- Layer 3 (GSM Rec. 04.07/08) with sublayers for control signaling channel functions (BCH, CCCH and DCCH):
  - Radio resource management (RR): to establish and release stable connection between mobile stations (MS) and an MSC for the duration of a call and to maintain connection despite user movements - functions of MSC:
    - cell selection
    - handover
    - allocation and tear-down of point-to-point channels
    - monitoring and forwarding of radio connections
    - enabling encryption
    - change transmission mode
  - Mobility management (MM) handles the control functions required for mobility:
    - authentication
    - assignment of TMSI,

  - management of subscriber location
- Connection management (CM) - set up, maintain and tear down calls connections:
  - Call control (CC): Manages call connections,
  - Supplementary service support (SS): Handles special services,
  - Short message service support (SMS): Transfers brief text messages

Neither the BTS nor the BSC interpret CM and MM messages, these messages are exchanged between the MSC or the MS using the direct transfer application part (DTAP) protocol on the A interface.

Radio Resource Management (RR) messages are mapped to or from the base station system application part (BSSAP) for exchange with the MSC:

- Transmission mode (change) management
- Cipher mode management
- Discontinuous transmission mode management
- Handover execution
- Call re-establishment
- RR-session release
- Load management
- SACCH procedures
  - radio transmission control (power & timing, downlink), (measurements, uplink)
  - general information
- Frequency redefinition
  - General information broadcasting (BCCH)
  - cell selection information
  - information for idle mode functions
  - information needed for access
  - cell identity

A_{bis} interface

Dividing line between the BSC function and the BTS

BSC and BTS can be connected using leased lines, radio links, metropolitan area networks (MANs), LANs {see UC Berkeley's ICEBERG}, …

Two channel types exist between the BSC and BTS:

- Traffic channels (TCH): configured in 8, 16 and 64 kbps formats - for transporting user data
- Signaling channels: configured in 16, 32, 56 and 64 kbps formats - for signaling purposes between the BTS and BSC

Each transceiver (transmitter + receiver) generally requires a signaling channel on the A_{bis} interface, data is sent as **Transcoder Rate Adapter Unit** (TRAU)[1] frames (for a 16 kbps traffic channel (TCH), 13.6 kbps are used for user data and 2.4 kbps for inband signaling, timing, and synchronization)

1. It is not defined where TRAU is placed, i.e., it could be part of BTS, BSC, or MSC.

A_{bis} protocols

- Layer 1 (GSM Rec. 08.54)
  - 2.048 Mbps (ITU-T: E1) or 1.544 Mbps (ANSI: T1) PCM facility
  - with 64/32/16 kbps signaling channels and 16 kbps traffic channels (4 per timeslot)
- Layer 2 (GSM Rec. 08.56)
  - LAP-D protocol used for data messaging between the BTS and BSC
  - **Service Access Point Identifier** (SAPI) refers to the link identifier transmitted in the LAPD protocol (inherited from ISDN)
- Layer 3 (GSM Rec. 08.58/04.08)
  - BTS management (BTSM) via three logical signaling connections identified by Service Access Point Identifier (SAPI):
    - SAPI 0 is used by all messages coming from or going to the radio interface
    - SAPI 62 provides O&M message transport between the BTS and BSC
    - SAPI 63 is used for dynamic management of TEIs as well as for layer 2 management functions.

A Interface

Defines interface between the BSC and MSC

TCHs are converted from 64 kbps to 16 kbps in the transcoder equipment, two cases based on where the transcoder equipment (TCE, i.e., TRAU) is located:

at BSC or BTS	traffic channel (TCH) occupies a complete 64 kbps timeslot in the 2 Mbps or 1.544 Mbps PCM link (layer 1, GSM Rec. 08.04)
at MSC	the TCHs are 16 kbps on the A interface

At least 2 time slots on the PCM link are needed for control and signaling purposes.

A interface protocols

Signaling protocol (layer 2+3) between BSC and MSC based on the SS7 standard and is transmitted along with the user data within the PCM facility. Normally timeslot 16 (TS16) of the 64 kbps frame is used.

The following protocols are employed:

- Layer 1 (GSM Rec. 08.04) either 2.048 Mbps (ITU-T: E1) or 1.544 Mbps (ANSI: T1) PCM link
- Layer 2 (GSM Rec. 08.06) SS7-based protocols
  - Message transfer part (MTP) protocol - transmission security between the BCS and MSC
  - Signaling connection control part (SCCP) protocol
  - SCCP connection can be initiated by a mobile station (MS) or an MSC
  - An SCCP connection can involve the following protocols:
  - From the MS:
    - MM: CM service request
    - RR: Paging response
    - MM: Location updating request
    - MM: CM re-establishment request
  - From the MSC:
    - Initiation of an “external handover” (BSSMAP: handover request).
  - MSC manages the SCCP connections

- Layer 3 (GSM Rec. 08.08)
  - Base station system application part (BSSAP) protocol
  - On MSC end:
    - Base station management application part (BSSMAP) protocol - counterpart to the RR protocol on the air interface
    - Direct transfer application part (DTAP) protocol transmits CC and MM messages transmitted transparently through the BTS and BSC

GSM Audio

- Speech coding - 20ms (i.e., 160) samples (8kHz @13 bits) are buffered then coded
- Error protection (codec specific)
- Error detection (CRC)
- Bad Frame Handling (substitution)
- Voice Activity Detection / Discontinuous Transmission (VAD/DTX)

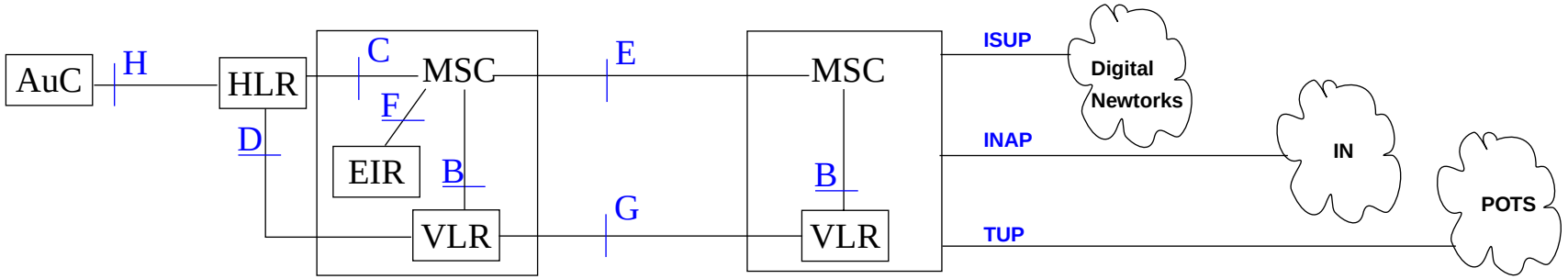
Manufacturer specific audio features:

- noise cancelling
- spectrum equalization
- echo cancellation

CODECs

Full rate (FR)	13 kbps , Regular pulse excitation - long term prediction (RPE-LTP)
Half rate (HR)	5.65 kbps VSELP
Enhanced full rate (EFR)	12.2 kbps ACELP
Adaptive Multi Rate (AMR)	ACELP, 12.2, 10.2, 7.95, 7.4, 6.7, 5.9, 5.15, 4.75 kbps
AMR wideband codec	(under standardization)

MSC interfaces and protocols



- MAP (Mobile Application Part) (GSM Rec. 09.02)
  - controls queries to the different databases in the mobile radio network (HLR, VLR, EIR, …)
  - responsibilities include access and location management, MSC-MSC handover, security functions, O&M, SMS, and supplementary services.
- TCAP (Transaction Capabilities Application Part)
  - provides universal calls & functions for handling requests to distributed appl. processes
- ISUP (ISDN User Part)
  - controls interworking (e.g. call setup/tear-down) between Public Land Mobile Networks (PLMNs) and other networks, and provides the same basic functionality as TUP
- INAP (Intelligent Network Application Part)
  - implements intelligent supplementary services (e.g. free call, time-dependent routing)
- TUP (Telephone User Part)
  - implements interworking between PLMNs and other networks
  - used to provide international connections and is being replaced by ISUP

GSM Logical Channels

Traffic channels		Full-rate (TCH/F) @ 22.8 kbps Half-rate (TCH/H) @ 11.4 kbps	Two way
Signaling channels	Broadcast channels	Frequency correction (FCCH)	base-to-mobile
		Synchronization (SCH)	
		Broadcast control (BCCH)	
	Common control channels	Paging (PCH)	
		Access Grant (AGCH)	
		Random access (RACH)	mobile-to-base
	Dedicated control channels	Stand-alone dedicated control channel (SDCCH)	two-way
		Slow associated control (SACCH)	
		Fast associated control (FACCH)	

Traffic channel (TCH)

Multiframe - group of 26 TDMA frames (120 ms long)

- 24 are used for traffic (voice or user data)
- 1 is used for the slow associated control channel (SACCH)
- 1 is currently unused

TCHs for the uplink and downlink are separated in time by 3 burst periods

- mobile station does not have to transmit and receive simultaneously
- simplifies the electronic circuitry; avoids antenna duplex filters
- reducing complexity helps to cut power consumption

Broadcast channels (BCH)

Carry only **downlink** information - mainly for synchronization and frequency correction.

However, it is the only channel capable of point-to-multipoint communications in which short messages are simultaneously transmitted to several mobiles.

- Broadcast control channel (BCCH)
  - General information, cell-specific; e.g. local area code (LAC), network operator, access parameters, list of neighboring cells, etc. A MS receives signals via the BCCH from many BTSs within the same network and/or different networks
  - tells MS what their initial power level should be
- Frequency correction channel (FCCH)
  - correction of MS frequencies
  - transmission of frequency standard to MS
  - also used for synchronization of an acquisition by providing the boundaries between timeslots and position of the first time slot of a TDMA frame
- Synchronization channel (SCH)
  - frame synchronization (TDMA frame number) and identification of base station
  - reception of one SCH burst provides a MS with all the information needed to synchronize with a given BTS

Common control channels (CCCH)

Uplink and downlink channels between the MS card and the BTS.

Convey information from the network to MSs and provide access to the network.

- Paging channel (PCH)
  - Downlink only
  - MS is informed (by the BTS) of incoming calls via the PCH.
- Access grant channel (AGCH)
  - Downlink only
  - BTS allocates a TCH or SDCCH to the MS, thus allowing the MS access to the network.
- Random access channel (RACH)
  - Uplink only
  - allows MS to request an SDCCH in response to a page or due to a call
  - MS chooses a random time to send on this channel (note: potential collisions with RACH transmissions from other MSs)

PCH and AGCH are transmitted in one channel called the paging and access grant channel (PAGCH) - they are separated in time.

Dedicated control channels (DCCH)

Responsible for roaming, handovers, encryption, etc.

- Stand-alone dedicated control channel (SDCCH)
  - communications channel between MS and the BTS
  - signaling during call setup -- before a traffic channel (TCH) is allocated
  - It takes ~480ms to transmit a message via SDDCH
- Slow associated control channel (SACCH)
  - always allocated to a TCH or SDCCH
  - used for “non-urgent” procedures: radio measurement data (e.g. field strengths) {information is used for handover decisions}, power control (downlink only), timing advance[1], …
  - 260bps channel - enough for reporting on the current cell and upto 6 neighbors about twice per second (if there is no other traffic for this channel)
  - note that the MS is told what frequencies to monitor (BTSs have a color code assigned to them so the that the MS can report on multiple BTSs which are using the same frequency)
- Fast associated control channel (FACCH)
  - similar to the SDCCH, but used in parallel to operation of the TCH
  - if the data rate of the FACCH is insufficient, “borrowing mode” is used (i.e., additional bandwidth borrowed from the TCH), this happens for messages associated with call establishment authentication of the subscriber, handover decisions, …
  - It takes ~40ms to transmit a message via FACCH

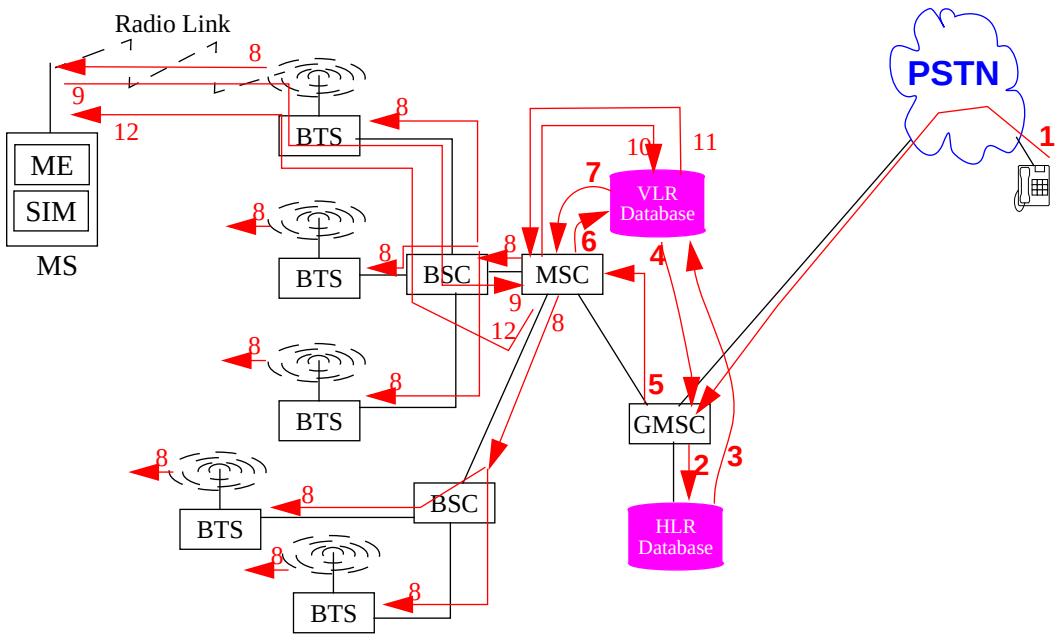
1. Transmission and reception of bursts at the base station must be synchronized, thus the MS must compensate for the propagation delays by advancing its transmission 0 .. 233 ms which is enough to handle cells of radius up to 35 km.

GSM Timing

A **very elaborate** timing structure ranging from 1/4 of a bit (900ns) to an encryption hyperframe (3 hours 28 minutes and 53.76s)!

Unit	Time
bit	3.69us
slot	156.25 bits (577 us)
frame	8 slots (4.615 ms)
traffic multiframe	26 frames (120 ms) or control multiframe 51 frames (235.4 ms)
superframe	51 traffic multiframes or 26 control multiframes (6.12 s)
hyperframe	2048 superframes (3 hours 28 minutes and 53.76s)

Incoming Call



1. incoming call is passed from the fixed network to the gateway MSC (GMSC)
2. based on the IMSI numbers of the called party, HLR is determined
3. HLR checks for the existence of the called number, then the relevant VLR is requested to provide a mobile station roaming number (MSRN)
4. reply transmitted back to the GMSC
5. connection is switched through to the responsible MSC
6. VLR is queried for the location range and reach ability status of the mobile subscriber
7. if the MS is marked reachable, then a radio call is enabled
8. radio call is executed in all radio zones assigned to the VLR
9. reply from the MS in its current radio cell
10. when mobile subscriber telephone responds to the page, then complete all necessary security procedures
11. if this is successful, the VLR indicates to the MSC that call **can** be completed
12. call can be completed

Figure 24: Call from fixed network to MS - we don't know which cell the mobile is in, only its rough location

Mobility Management (MM)

GSM network keeps track of which mobile telephones are powered on and active in the network.

The network keeps track of the last known location of the MS in the VLR and HLR.

Radio sites connected to the MSC are divided into "**location areas**" (LAs), thus when a call comes for an MS, the network looks for the MS in the last known location area.

Each BTS is assigned (by the operator) a 40 bit ID - called a **location area identity** (LAI), with three parts:

- mobile country code
- mobile network code
- location area code

Security

Use of TMSI rather than IMSI - reduces the need to send IMSI over the air (thus simply listening to the radio link it is harder to identify a given user).

Two major aspects of security: Authentication and Encryption

A3	Authentication algorithm
A5	Ciphering algorithm
A8	Ciphering key computation
K_i	secret encryption key - operator determines length, but it can be upto 128 bits
K_c	cypher key, computed based on K_i

Cipher mode management

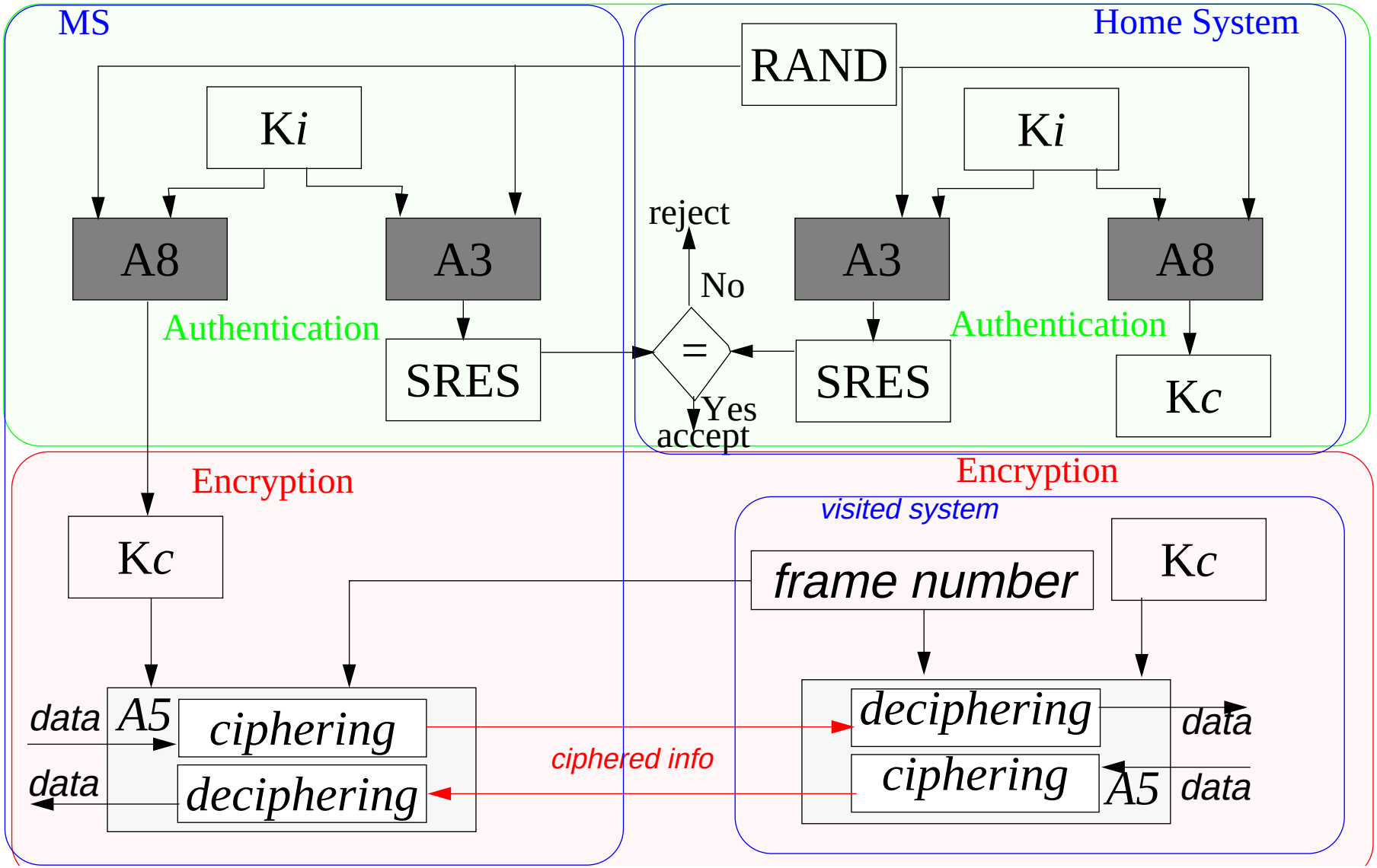
Connection always starts in non-ciphered mode, because ciphering requires a user specific key and the network has to know the identity of the subscriber before it can be used!

Authentication

User authentication normally takes place when the MS is turned on (user must key in a PIN code on the handset in order to activate the hardware before this automatic procedure can start).

Authentication occurs with each incoming call and outgoing call. This is based on checking that “Ki” (secret encryption key) stored in the AuC matches the “Ki” stored in SIM card of the MS.

Authentication and Encryption



GSM data rates

The following table of data rates is from page 39 of [41]

Connection Type[a]	Two-way delay
TCH/F9.6 T	330 ms
TCH/F9.6 NT	> 330 ms
TCH/F4.8 T	330 ms
TCH/F2.4 T	200 ms
TCH/H4.8 T	600 ms
TCH/H4.8 NT	> 600 ms
TCH/H2.4 T	600 ms

a. T = Transparent, NT = Non-transparent

System engineering

The operator must choose how many of each element (MSC, BSC, BTS, …) to order, what capacity each must have, where to install them, …. However, since traffic does not remain constant installing enough capacity for long term traffic is *not* cost effective ⇒system engineering is an on-going activity

Note: goal of cellular planning is to choose the cell sites and cell parameters (frequency allocation, capacity, power, etc.) to provide economically continuous coverage and support the required traffic density (not an easy task)

Table of parameters, from page 101 of [41]

Area	Parameters	
Cell planning	frequencies beacon frequencies hopping sequences power control parameters	handover parameters cell selection parameters Base Station Identity Code (BSIC)
Dimensioning	# of common channels # of traffic channels	location areas periodic location updating
Load control	overload control parameters	

GSM Network Optimization

Based on network performance & utilization, subscriber behavior, and (QoS)

Test methods:

- **Traffic analysis**: the signaling channels in the PCM frame are monitored and analyzed on the Abis and A interfaces
- **Bit error ratio test** (BERT): bit error measurement at the PCM level and the GSM-specific level (TRAU frame)
  - PCM bit error ratio (BER) is used to verify the quality of lines leased from fixed network operators
  - By evaluating the control bits in the TRAU, a bit error probability can be determined (uplink) during actual communications (in-service) {No easy measurement of the downlink BER}
  - More accurate radio link BER measurement (out-of-service) measurement in which the 260 data bits in the TRAU frame are checked using a pseudo-random bit sequence (PRBS)
- **Alarm monitoring** - checking PCM links for layer 1 alarms
- **Network quality test**: lots of measurements - including:
  - island problems, detection of coverage holes, interference, network load regarding signaling and traffic, handover failures, Receive level (RXLEV) surveillance, bit error ratio of a BTS (RXQUAL), multipath interference and propagation delays, frequency interference (due to nearby frequency reuse), call completion/disconnect rate, indications of system overload.

Optimal Cell Planning

Some of the parameters which have to be decided [44]:

- Selecting Site location
- Antenna parameters
  - Tilt, Azimuth, Height, Antenna type
- **Site parameters**
  - **Transmitter power/Dedicated channel power level/Common channel power level**
- **Service parameters**
  - **Power per service**
  - **Enable/disable handover per service**
- **Network parameters**
  - **Handover**
    - **Neighbor lists/Hysteresis/Timers**
  - **Power control policy**
- **Resource management**

Note: first two are sets of parameters are fixed ($\Rightarrow$ a physical change in the site), while the others can be changed under software control.

Features

Call Waiting (CW)	{network-based feature} users with a call in progress receive an audible beep to alert them that there is an incoming call for their MS The incoming call can be: • **accepted** {the original call is put on hold}, • **sent to voice mail**, or • **rejected** {in this case the caller will receive a busy signal}
Call Hold (CH)	allows the MS to “park” an “in progress call”, to make additional calls or to receive incoming calls
Call Forwarding (CF)	{network-based feature} allows calls to be sent to other numbers under conditions defined by the user Conditions can be either unconditional or dependent on certain criteria (no answer, busy, not reachable)
Calling Line ID	caller’s network to delivers the calling line ID (telephone no.) to the GSM network; GSM telephone displays the originating telephone number
…	

GSM Phase 2+

- **High Speed Circuit Switched Data** (HSCSD)
- **General Packet Radio Service** (GPRS)

High Speed Circuit Switched Data (HSCSD)

Idea is simple	use several time slots out of each TDMA frame for one data connection
Reality	this is taxing for the RF power systems

In the basic GSM model transmit/receive (TX/RX) activities, the terminal can be implemented using **one** frequency synthesizer (even though it takes some time for the synthesizer to change from one frequency to another) - because of the offset of 3 slots between transmit and receiver.

If you only use 2 slots, you just need a synthesizer that changes faster, but at 3 slots you potentially need to transmit and receive at the same time.

At eight time slots (i.e., continuous transmission):

- monitoring neighboring base stations would require an independent receiver
- the terminal will be more expensive than one slot terminals
- power consumption will be **much** higher

Multi-slot systems have required changes in: ciphering, frequency hopping, and generally radio resource management functions.

HSCSD depends on:

- **Terminal Adaptation Function** (TAF)
- **Interworking Functions** (IWF)
- enhanced RLP to handle multilink (aka multiple time slot) operation

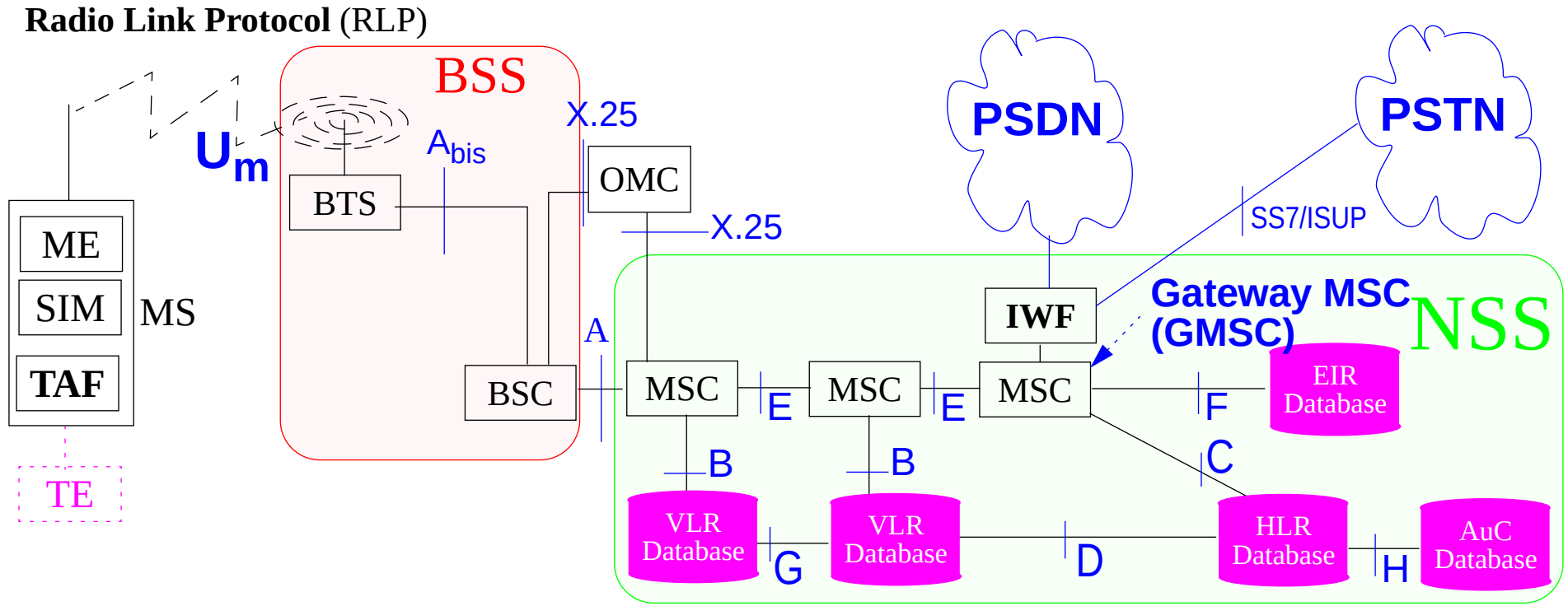


Figure 25: GSM/HSCSD Architecture

Nokia's Card Phone 2.0: HSCSD at upto 43.2 kbps (without data compression)

General Packet Radio Service (GPRS)

GPRS features:

- True packet radio system - sharing network and air interface resources
- Volume based charging
- TCP/IP (Internet & Intranet) interworking, SMS over GPRS, (and X.25 interworking)
- Peak data rate from 9.05 kbps .. 171.2 kbps
- Protocols designed for evolution of radio
  - EDGE - new GSM modulation
  - Migration into 3rd Generation

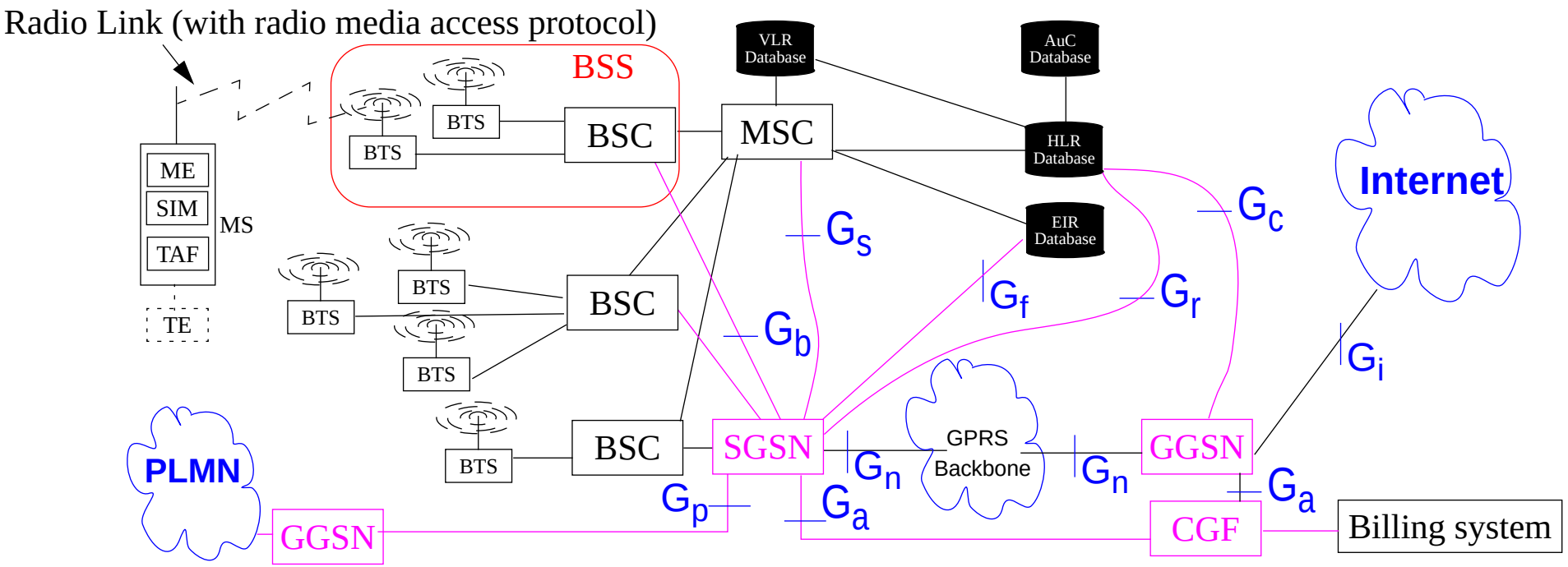
GPRS nodes

GPRS introduces new network elements

- **Serving GPRS Support Node** (SGSN)
  - authentication & authorization, GTP tunneling to GGSN, ciphering & compression, mobility management, session management, interaction with HLR,MSC/VLR, charging & statistics, as well as NMS interfaces.
- **Gateway GPRS Support Node** (GGSN)
- interfacing to external data networks (basically it is a network router) encapsulating data packets in GTP and forwarding them to right SGSN, routing mobile originated packets to right destination, filtering end user traffic, as well as collecting charging and statistical information of data network usage

GPRS is the result of committees trying to “adapt” Mobile IP to GSM systems.

GSM/GPRS Architecture and Interfaces



G_a	Charging data collection interface between a CDR transmitting unit (e.g. a SGSN or a GGSN)	G_i	reference point between GPRS and an external packet data network (G_i = **i**nternet)
G_b	between a SGSN and a BSS (G_b = **b**ase interface)	G_n	between two GSNs within the same PLMN (G_n = **n**ode)
G_c	between a GGSN and a HLR (G_c = **c**ontext)	G_p	between two GSNs in different PLMNs (G_p interface allows support of GPRS network services across areas served by the co-operating GPRS PLMNs.) (G_p = **P**LMN)
G_d	between a SMS-GMSC and a SGSN, and between a SMS-IWMSC and a SGSN (**not shown**)	G_r	between an SGSN and a HLR (G_r = **r**oaming)
G_f	between an SGSN and a EIR (G_f = **f**raud)	G_s	between a SGSN and a MSC/VLR

GPRS Coding Schemes

Four coding schemes (but only CS1 and CS2 are in early systems)

Coding Scheme	CS1	CS2	CS3	CS4
User Data Rate	9.05 kbps	13.4 kbps	15.6 kbps	21.4 kbps
Correction Capability	Highest			None
Worst-link Budget	135 dB	133dB	131 dB	128.5 dB
Maximum Cell Range	450 m	390 m	350 m	290 m
40 bytes (320 bits) of payload see [47], pg. 33	1956 bits	1132 bits	1018 bits	625 bits
1500 bytes (12000 bits)	55787 bits	32490 bits	27218 bits	19345 bits

For comparison with GSM the worst-case link budget is 142.5 dB and the maximum cell range is 730 m.

But the real problem is that GPRS uses *interleaving* to spread the effect of burst errors - but this means that the delay is always high!

Unstructured Supplementary Service Data (USSD)

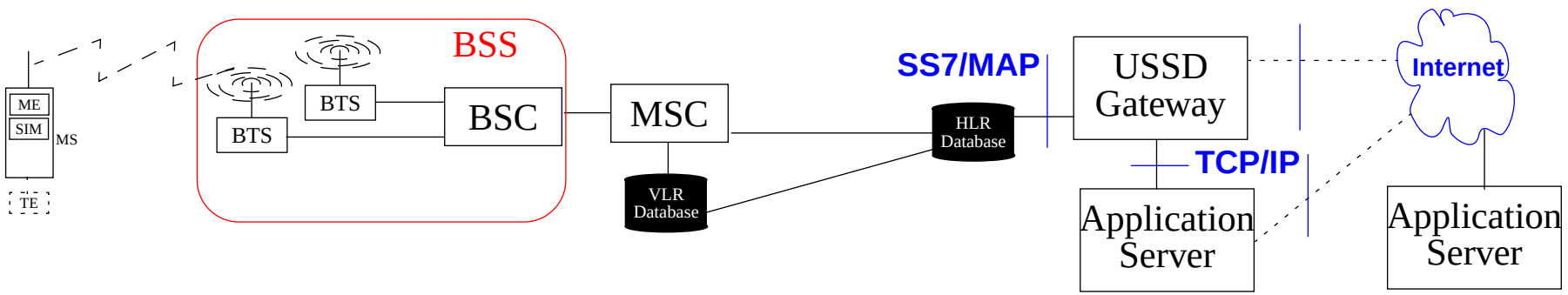
When MS can not recognize text - it simply passes it to the network as USSD.

USSD supports all digits, asterisk (*), and punt/pound (#) keys. In the form:

(* | #) command_code (2-3 digits) {*parameter}* #

total length up to 200 ASCII characters

A USSD server (or gateway) is connected to the user's HLR via MAP and to servers (which actually provide a specific service) via TCP/IP. USSD is thought to be ~7x faster than SMS for two-way transactions (this is because USSD is session oriented as opposed to SMS's store-and-forward behavior).



USSD continued

Examples:

- set-up or cancel of services like call forwarding
- Swisscom's SIm Card Application Platform (SICAP) prepaid roaming platform[1]: users dial in a USSD string that includes the telephone number they want to call (e.g., *101*NUMBER#) this is sent to the SICAP platform at their (home) operator, who then connects them to the desired number by dialling them back!

In addition to passing the USSD message to the external application, the USSD Gateway passes:

- originating subscriber's MSISDN
- number of the HLR which handled the USSD
- originating subscriber's IMSI (optional)
- VLR Number (optional)

Disadvantage: USSD and SMS both use the same control channel

1. Sold as "GSM Card easyRoam"

Short Message Service (SMS)

Short Message Service (SMS) offers connectionless (message) delivery (similar to “two-way-paging”)

If the GSM telephone is not turned on, the message is held for later delivery. To Ensure that each time a message is delivered to an MS, the network expects to receive an acknowledgement from the MS that the message was correctly received.

SMS supports messages up to 140 octets (160 characters of GSM default Alphabet - see GSM 03.38) in length.

SMS concatenation - combines several messages

SMS compression - defined standard for compression of content

With international roaming these messages can be delivered by any GSM network around the world to where the MS currently is.

Two types of messages: **cell broadcast** and **point-to-point service**

SMS message types

User-specific — message is to be display to the user

ME-specific — message is targeted at the mobile terminal itself

- playing a ring tone
- displaying a business card
- changing the default icon
- …

SIM-specific — message is targeted at the SIM card

- change the balance in a pre-paid card

Short Message Service Architecture

SM-SC	Short Message Service Centre
SMS GMSC	SMS Gateway MSC
IWMSC	Interworking MSC
ESME	External Short Message Entities

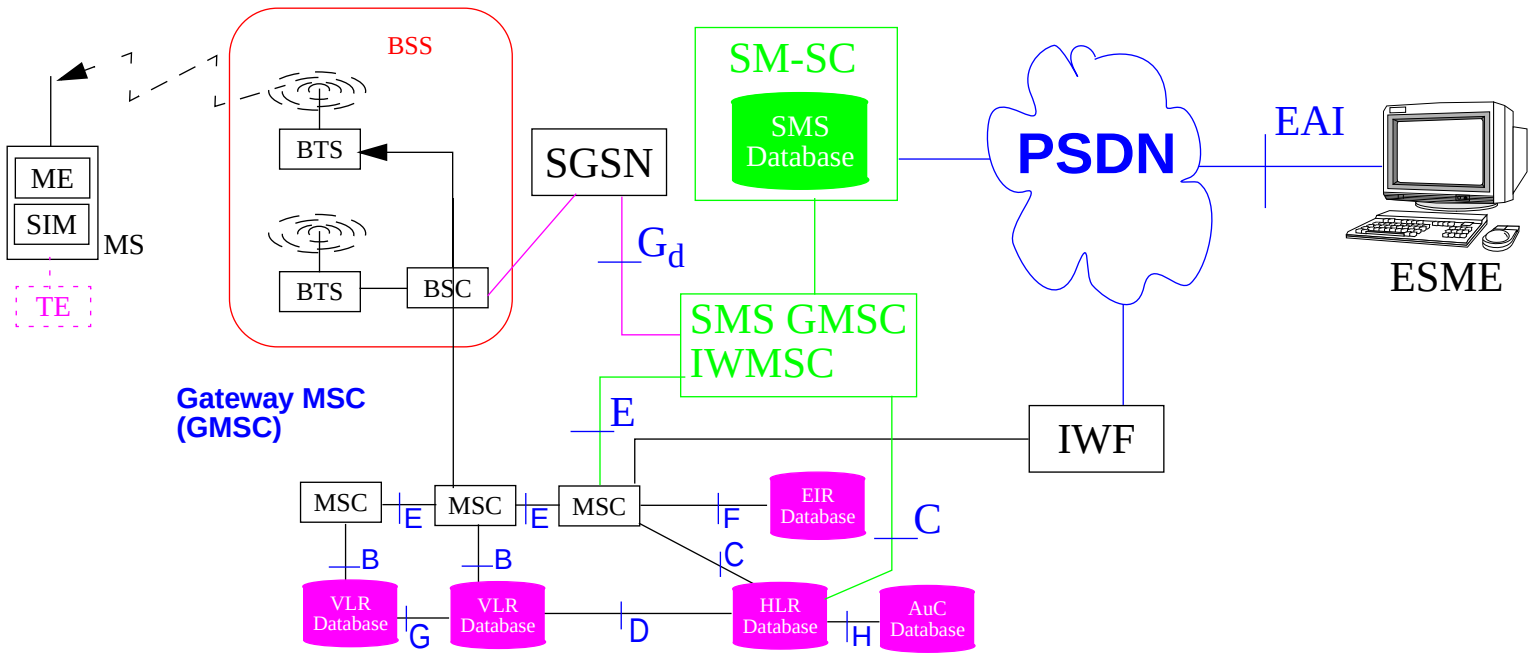


Figure 26: SMS Architecture

SM-SCs

- High reliability
- High availability
  - Logica's Picasso SMS Centre allows new hardware can be added within 60 seconds, with no service outage
- High performance
  - HP's (formerly Compaq's) AlphaServer™ ES45,over 8,000 SMS deliveries per second with CMG Wireless Data Solutions (formerly CMG Telecommunications) SMSC software [52]; note that they have merged with Logica plc forming: LogicaCMG
  - Logica's Picasso SMS Centre supports configurations of 1 to 128 nodes with automatic load sharing
- existing SM-SCs talk TCP/IP as well as other protocols

There exist SMS brokers from whom you can buy SMS capacity in bulk, they receive your messages and then transfer them to operators that they have agreements with.

As each SMS is charged for resulting CDR volumes can be very high, e.g., Mannesmann has peak CDR rates as high as 2,500-3,000 CDRs per second ([55], pg. 13)

Three kinds of SMSs

User-specific	display to a user
ME-specific	ME processes the message when it is received Nokia has special function to play ring tone, display a business card, modify the default icon, …
SIM-specific	SIM processes the message when it is received (for use via SIM toolkit applications)

Entering Short Messages

To improve the speed of entering SMSs (and other text)

- Full keyboards (such as Ericsson's Chat Board)
- Onscreen keyboard (such as Palm's on-screen keyboard)
- Fitaly keyboard - arranges letters based on their frequency and probability transitions in English (see page 43 of [51])
- Predictive text input algorithms
  - Tegic T9 - utilizes numeric keypad and probability to work out probably string (see page 45 of [51])
  - e-acute's Octave keyboard (see pages 46-47 of [36])
- Handwriting recognition
  - Word recognition, such as Psion's CalliGrapher (see pages 47-48 of [36])
  - Character recognition, such as Palm's Graffiti (see pages 48-49 of [36]) and
  - CJKOS - an OS extension for Palm for Chinese, Japanese, and Korean (see page 49 of [36])
- Speech recognition

SMS shorthand

From “Get 2 grips with SMS-speak b4 it’s 2 L8 !” some examples:

afasik	as far as I know	<g>	grin	sc	stay cool
asap	as soon as possible	gr8	great	sol	sooner or later
atw	at the weekend	gsoh	good sense of humour	t+	think positive
awhfy	are we having fun yet?	h2cus	hope to see you soon	t2ul	talk to you later
b4	before	hak	hug and kisses	tuvm	thank you very much
bbfn	bye bye for now	ic	I see	w4u	waiting for you!
bcnu	be see in you	idk	I don’t know	wuwh	wish you were here
brb	be right back	idts	I don’t think so!	X!	Typical woman!
btw	by the way	iow	in other words	Y!	Typical man!
cm	call me	j4f	just for fun		
cu	see you	kc	keep cool		
cul8ter	see you later	khuf	know how you feel		
dk	don’t know	l8r	later		
dur?	do you remember	m8	mate		
e2eg	ear to ear grin	mtfbwu	may the force be with you		
eod	end of discussion	nc	no comment		
F?	Friends?	nwo	no way out		
F2F	Face to Face	o4u	only for you		
fya	for your amusement	O!ic	Oh, I see!		
fyi	for your information	ruok	are you okay?		

External Application Interface (EAI)

In order to enable non-mobile External Short Message Entities (ESME) to interface with an SMSC one of the following protocols (which all run over TCP/IP) is generally used:

Short Message Peer to Peer (SMPP)	open message-transfer protocol to enable SMPP V5.0 specification released 20 February 2003 [54] Initially defined by Logica - now SMSForum
CIMD2	Nokia's Computer Interface to Message Distribution 2 [56]
EMI/UCP	CMG's Universal Computer Protocol [57]

Note:

- this avoids the earlier problem of the interface to the SMSC being closed;
- more and more operators seem to be converging on using SMPP.

Voice Messaging System (VMS)

A value-added service which redirects incoming calls (i.e., forwards them) to a voice mailbox when MS is turned off, low on battery, left unattended (after ringing for xx seconds) or temporarily out of coverage.

A **Voice Message Alert** (VMA) can be send (via SMS) to the MS to let the user know there is a waiting voice message.

Note that you can use SMS's "replace message" facility - to over-write last VMA - thus there will only be one message with the latest status voice messages (for example saying: "You have N voice messages waiting").

Voice Profile for Internet Mail (VPIM)

Voice Profile for Internet Mail (VPIM) Version 2 is currently a Proposed Standard (RFC 2421) Applicability Statement, it is an application of Internet Mail originally intended for sending voice messages between voice messaging systems

http://www.ema.org/vpim

http://www.ietf.org/html.charters/vpim-charter.html

VPIM v3 Specification add extensions: IMAP voice extensions, voice directory profiles, content negotiation details for voice, and partial non-delivery notifications.

Enhanced Message Service (EMS)

Allows basic graphics, icons, and sounds to be incorporated in SMS messages.

Based on concatenating (i.e., linking together a chain of) several SMS messages

Multimedia Messaging Service (MMS)

MMS Centre (MMSC) - a logical extension of an SMS Centre, but must cope with a larger variety of message types; in addition, it can convert message formats to suit the capabilities of the receiving terminal

Four key functional elements:

- MMS Relay - engine which transcodes and delivers messages to mobile subscribers
- MMS Server - provides the store in the store-and-forward architecture
- MMS User Databases - user profiles, subscription data, …
- MMS User Agent - an application server which enables users to view, create, send, edit, delete, and manage their multimedia messages

An MMS presentation can utilize a synchronization language (e.g. **Synchronized Multimedia Integration Language** (SMIL)) for a synchronized presentation.

In addition to store and forward, MMS also supports store and retrieve (via e-mail and web)

SMS over GPRS

Can send SMS over GPRS - thus avoiding the problem of SMS utilizing the GSM control channel

There is the threat of users sending their messages directly via an messaging application or via e-mail -- this could take a lot of revenue away from the operators, see

International Roaming

GSM's roaming feature allows a user to make and receive calls in **any** GSM network and to use the same user-specific services worldwide, but this requires a **roaming agreement between the *individual* operators**.

Good news	With worldwide roaming the MS is accessible via the same phone number everywhere!
Bad news	It could be very expensive - much more expensive than you think!

The basic problem is that when you roam to another network (for example, in another country) - your Mobile Station ISDN number (MSISDN) *still looks like it is in your home network*. {This is one of the more stupid aspects of GSM.}

Worst is if you are in the same (non-home) network as the person you are calling, as this results in two international calls! This is due to tromboning. For four solutions see section 13.2 of [62], pages 242-249.

Enhanced Data Rates for GSM Evolution (EDGE)

- enhanced modulation technique designed to increase network capacity and data rates in GSM networks
- provide data rates up to 384 Kbps.
- EDGE lets operators without a 3G license compete with 3G networks (since the data rates are comparable in the wide area)

GSM/EDGE Radio Access network (GERAN)

The radio interface used in Enhanced Data Rates for GSM Evolution (EDGE)

Maximum data rate: 384 kbps

EGRPS

EGPRS = EDGE -- an extension/enhancement of GPRS including 4 new Data Packet Traffic Channels using 8-PSK modulation and a incremental redundancy mechanism extended to the GMSK based data packet traffic channels.

- Support for simultaneous, multiple radio access bearers with different QoS profiles.
- New bearer classes:

Conversational Class	Voice & video conferencing where small delay is required
Streaming Class	Capable of processing as transfer is taking place, needs somewhat constant delay and throughput
Interactive Class	on-line applications
Background Class	Delay insensitive but requires few errors (may require multiple re-transmissions to hide errors)

Operation/Administration/Maintenance

Operation/Administration/Maintenance (OA&M) follows ITU-T's Telecommunications Management Network (TMN) model, which has several components:

Operations system (OS)	OS uses Operating System Function (OSF) to provide overall management, billing, account, management of mobile equipment, HLR measurement, …
Network Element Functions (NEFs)	provides monitoring and control of Network Elements (NEs): HLR, VLR, AuC, EIR, MSC, BSC, and BTS
Data Communication Network	OS, NEs, and other TMN elements via Data Communication Function (DCF)
Mediation device (MD)	adapts the OS to a specific NE
Q-Adapter (QA)	uses Q-adapter function to adapt non-TMN equipment
Workstation (WS)	OA&M personnel interact with OS via Workstation functions (WSFs)

I personally find this ITU-T speak! But you have to talk the talk to walk the walk!

Further reading

GSM

[37] M. Mouly and MB Paulet, *The GSM System for Mobile Communications*, Mouly and Paulet, 1992

[38] M. Mouly and MB Paulet, Current evolution of the GSM systems, IEEE Personal Communications, vol. 2, no. 5, pp. 9-19, 1995.

[39] David J. Goodman, *Wireless Personal Communications Systems*, Chapter 7, GSM: Pan-European Digital Cellular System, Addison-Wesley, 1997, ISBN 0-201-63470-8

[40] Marc Kahabka, GSM Pocket Guide revised version Vol. 2, Acterna Eningen GmbH, 72795 Eningen u. A., Germany

[41] Petri Jarske, The GSM System, Principles of Digital Mobile Communication Systems, 2001 edition, Technical University Tampere, Finland
http://www.cs.tut.fi/kurssit/83150/DigiCom2001.PDF

[42] Sudeep Kumar Palat, “Replication of User Mobility Profiles for Location Management in Mobile Networks”, Dr. Ing. dissertation, Norwegian University of Science and Technology, Dept. of Telematics, 12 Jan. 1998.

[43] GSM security
http://www.isaac.cs.berkeley.edu/isaac/gsm.html

[44] Ron Abiri, “Migrating to an Advantage: Planning & Optimizing to Maximize Networkf efficiency & ROI”, Schema Ltd., 2002.
http://www.iec.org/events/2002/natlwireless_nov/featured/f1_abiri.pdf

[45] Mobile Application Part (MAP) ETSI R10 ETSI 08/96, CAA 201 45
http://www.ericsson.com/signaling/cards/map_etsi.shtml

GPRS

[46] Jari Hämäläinen, “Design of GSM High Speed Data Services”, Dr. Tech. dissertation ,Tampere University of Technology, Department of Information Technology, 4 October 1996.

[47] Jouni Mikkonen, “Quality of Services in Radio Access Networks”, Dr. Tech.

dissertation,Tampere University of Technology, Department of Information Technology, 19 May 1999.

[48] Don Zelmer, “GPRS, EDGE, & GERAN: Improving the performance of GSM & TDMA Wireless by Packet Capabilities”, Cingular Wireless LLC, SUPERCOMM 2001, Atlanta, Georgia, Wednesday, June 6, 2001

http://www.atis.org/atis/Pictures/Supercomm01/Presentationfolder/T1P1zelmer3Gtemplate2.PDF

USSD

[49] GSM 02.90: USSD Stage 1 -- only one way communication

[50] GSM 03.90: USSD Stage 2 -- allows two way communication

SMS and Multimedia Messaging Service (MMS)

[51] Jochen Burkhardt, Dr. Horst Henn, Stefan Hepper, Klaus Rintdoff, and Thomas Schäck, *Pervasive Computing: Technology and Architecture of Mobile Internet Applications*, Addison-Wesley, 2002, ISBN 0-201-72215-1

[52] CMG ANNOUNCES THIRD-GENERATION HIGH-PERFORMANCE SMS CENTRE: AlphaServer-based SMSC clocks unrivalled 8,000

sustained deliveries per second, Nieuwegein, the Netherlands, Feb. 19th 200, *http://h18000.www1.hp.com/products/software/in7/art4.html*

[53] Logica's Picasso SMS Centre

[54] SMS Forum - *http://smsforum.net/*

[55] Glyn Lloyd , Phill Davies, and Andrew Beswick, "Short Messaging Service Centres (SMSCs) Uncovered: More Than Just Text!", Lehman Brothers, November 2000, Pub Codes: 01/07/43/2035, *http://www.airslide.com/pdf/lehman.pdf*

[56] Nokia's Computer Interface to Message Distribution *http://www.forum.nokia.com/main/1,35452,1_2_9_10,00.html*

[57] Short Message Service Centre 4.0, EMI - UCP Interface Specification, Document Version: 4.2, May 2001, *http://www.cmg-wireless.com/wds/downloads/EMI_UCP_Specification_40.pdf*

[58] Palowireless's SMS, EMS and MMS tutorials, (accessed 2003.03.12)

http://www.palowireless.com/sms/tutorials.asp

[59] Gustav Söderström, “Virtual networks in the cellular domain”, M. Sc. Thesis, KTH/IMIT, January 2003 - ftp://ftp.it.kth.se/Reports/DEGREE-PROJECT-REPORTS/030211-Gustav_Soderstrom.pdf

[60] Logica, “The essential guide to Multimedia Messaging”, (accessed 2003.03.12) *http://www.logica.com/pdf/telecom/Mmsguide.pdf*

[61] *http://www.3gpp.org/ftp/specs/2002-03/Rel-4/23_series/23140-460.zip*

International Roaming

[62] Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, Chapter 13, psages 239-250 in [1].

Operation/Administration/Maintenance

[63] Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, **Chapter 14**, pp. 252-263 in [1].

KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

4. Number portability, VoIP, Prepaid

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Last modified: 2003.03.13:11:56

Lecture 4

- Number portability (Ch. 15), VoIP (Ch. 16), Prepaid (Ch. 17)

Database lookups

Local Number Portability (LNP)

Local Number Portability is required by the Telecommunications Act of 1996 and a July 1996 order of the Federal Communications Commission (FCC) - similar requirements in Sweden and elsewhere.

LNP (as defined by the FCC): “the ability of users of telecommunications services to retain, at the same location, existing telecommunications numbers without impairment of quality, reliability, or convenience when switching from one telecommunications carrier to another.”

LNP implies efficient call-routing must **not be based** on a **physical** location, but rather a **logical routing scheme** for how and where to route a call.

Verizon’s cost recovery for providing LNP amounts to US$13.80/line over a 5 year period! In Denmark, donor operator charges the recipient operator a fee of DKK 72 (~9.6 EURO) excl. VAT (~9.6 EURO) for the coverage of one-time administrative costs related to the porting of a single subscriber number.

Three kinds of Local Number Portability

- **Service Provider Portability**: subscriber can move to an new provider without a change in number (current requirement)
- **Location** (or **Geographic**) **Portability** (GNP): subscriber can move to a new location/geographic area (future requirement)
- **Service Portability**: if the service (mix) which the subscriber has is not available in their new local exchange, then connect them to where the services are available (future requirement)

Mobile Number Portability (MNP)

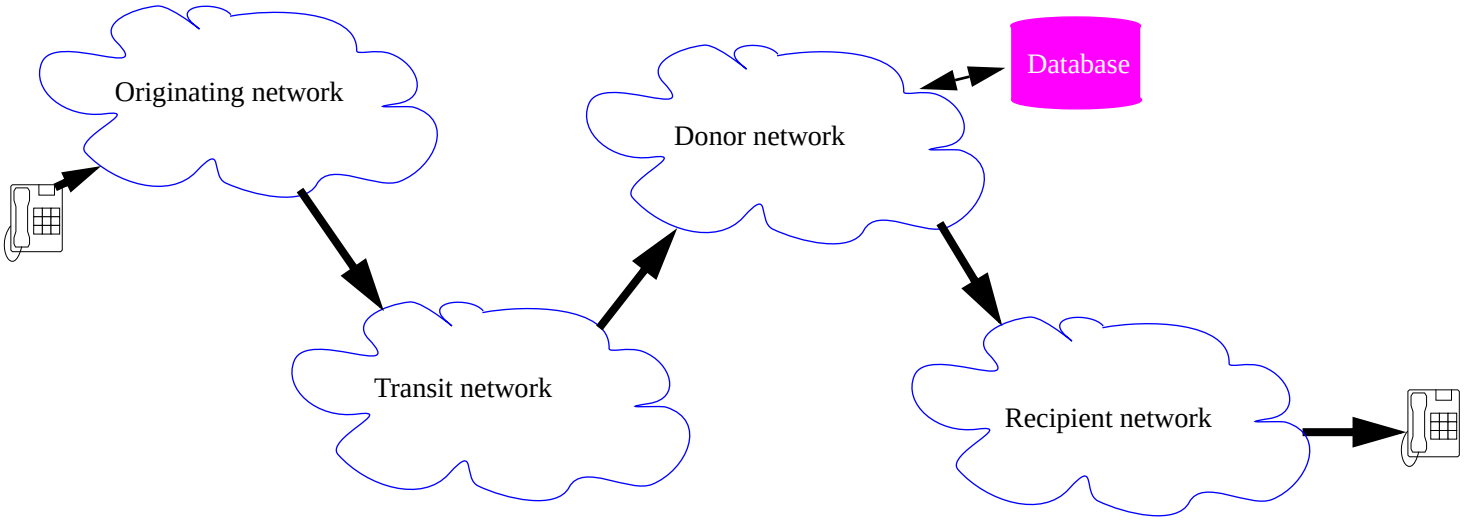
requirement that any mobile (e.g., GSM) subscriber be able to move to a new **operator** or **service provider** and keep the same number (MSISDN)

Non-geographic number portability (NGNP)

numbers (typically) associated with a service rather than a geographic destination, e.g., freephone, low rate calling numbers, premium rate numbers; requires that the service provider can be changed without a change of number; these all require DB lookup

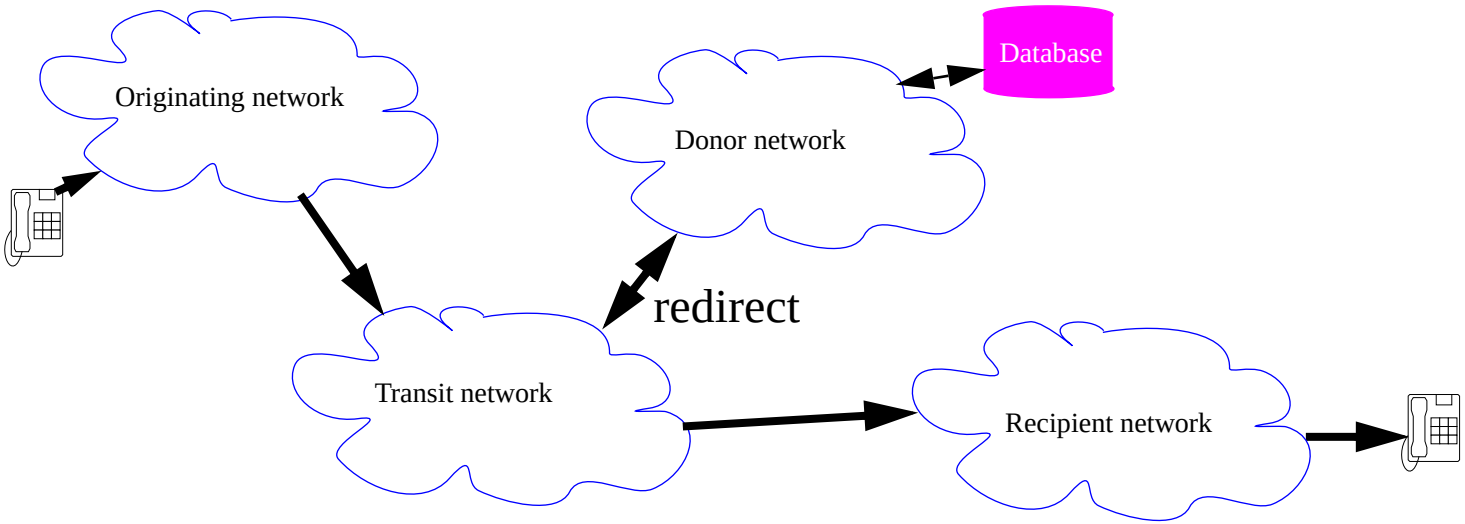
Call forwarding at donor end

Donor = service provider whom the number is initially associate with



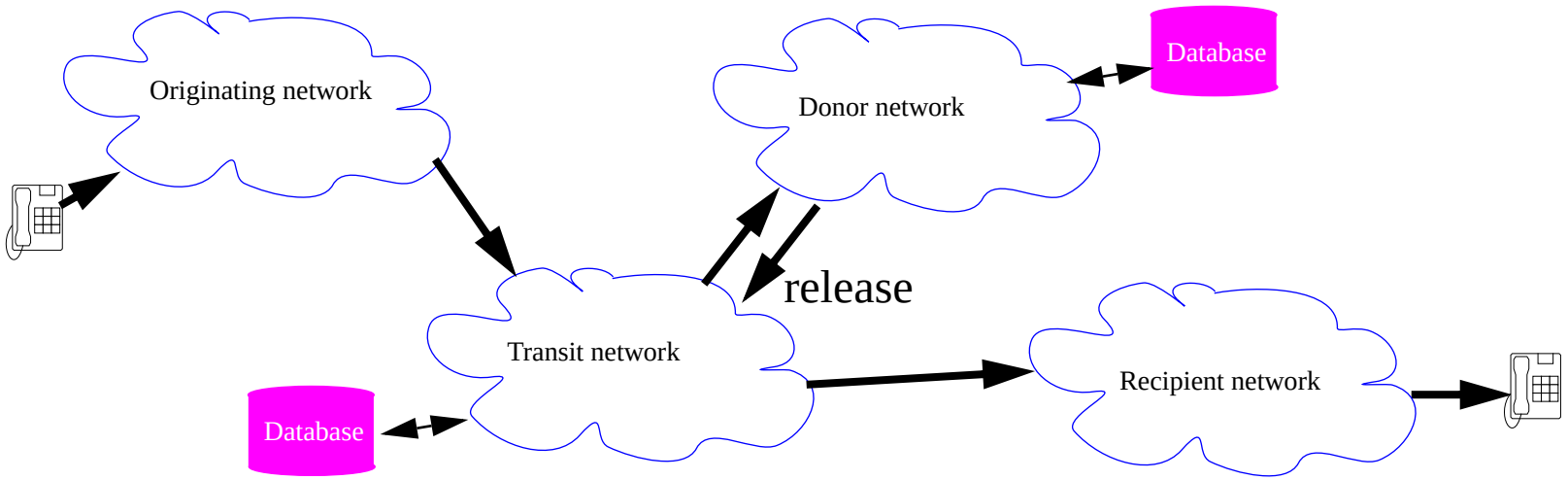
- inefficient in terms of call setup delays and usage of transmission capacity
- can not easily cope with numbers ported more than once, and
- the donor network continues to control first and subsequent portings.

Drop back forwarding



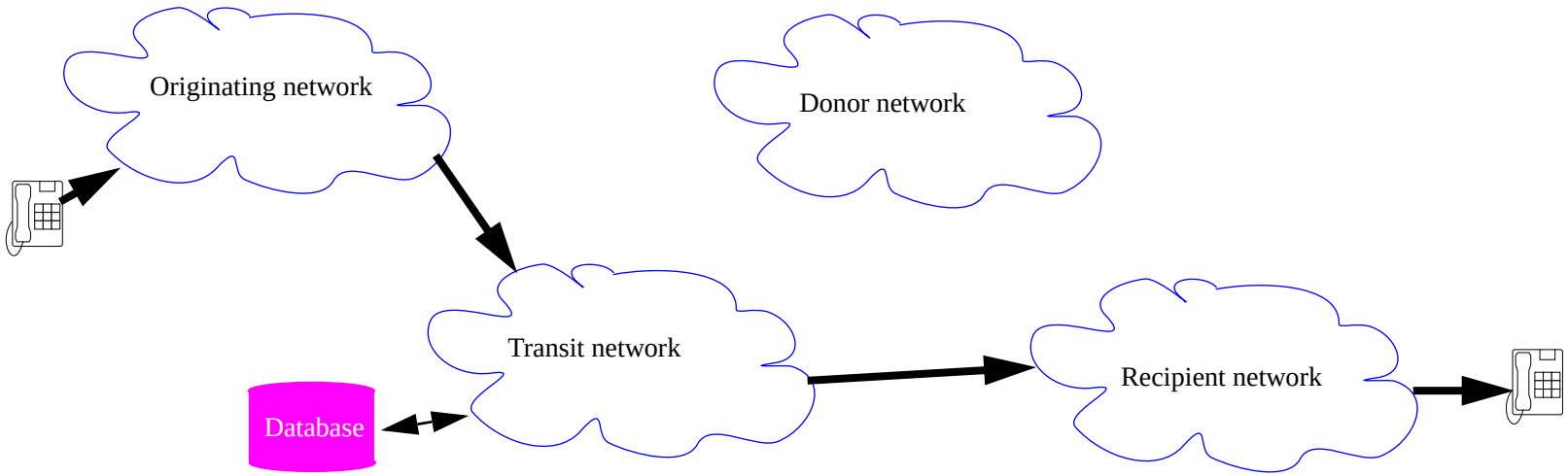
- transit network gets a **redirect** from the donor network, it may be able to pass this all the way back to the originating network (i.e., dropping back through each of the networks to the originating network)
- makes better use of transmission capacity and can handle multiple portings
- the donor network continues to control first and subsequent portings.

Query on release (QoR) solutions



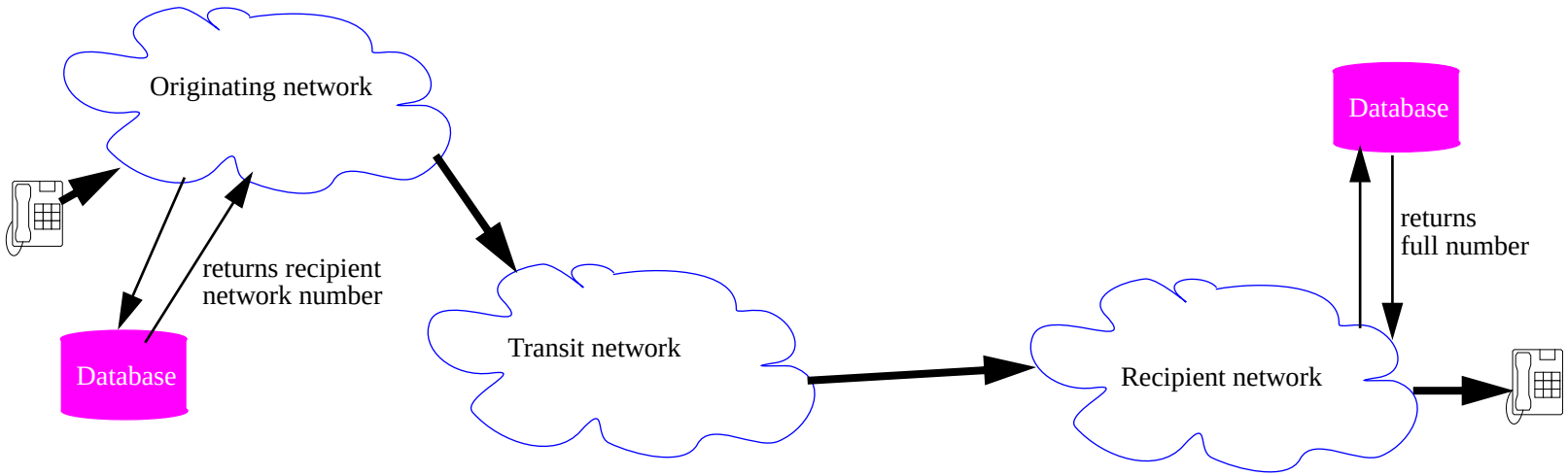
- Donor network realizes the number has been ported out and sends an **ISUP release** or it might not know anything about this number (i.e., not it its DB any longer) ⇒ releases the call
- Release causes an intermediate point to query a portability database and to redirect the call.
- If the forward signalling indicates that preceding networks have QoR capability, then the release goes all the way to the originating network, which does the DB lookup and reroutes the call to recipient network.

Look up type solutions



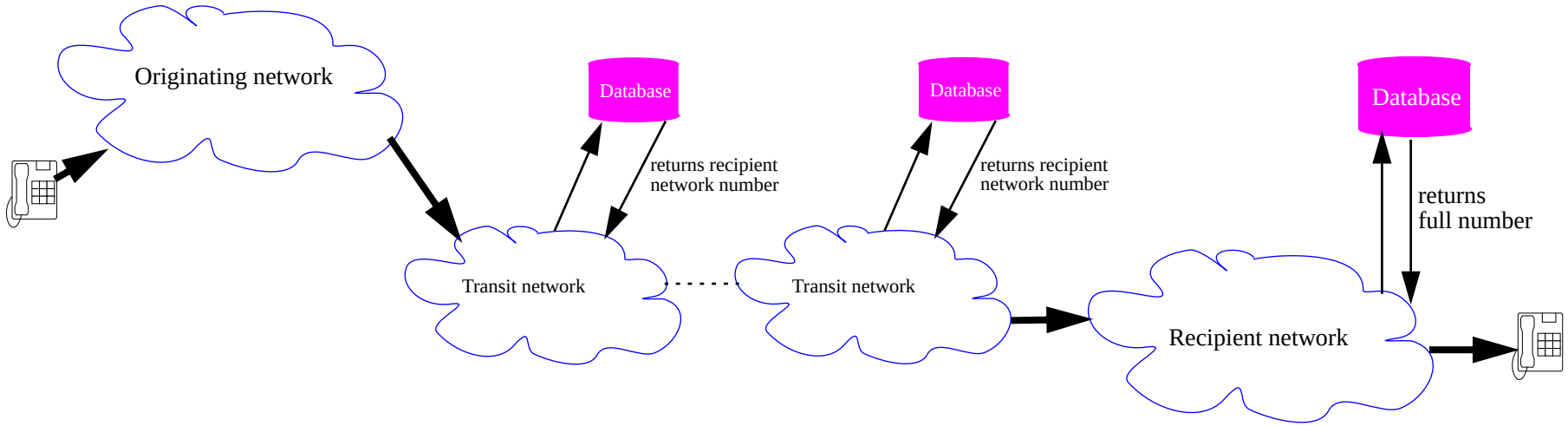
- portability database is checked for **all** calls, if the number has been ported, the new number is obtained and the call rerouted (done at first **first exchange** in a network that can access a **portability database**)
- solution is often implemented in North America via modified Signalling Transfer Points (STPs) which can check and translate ported numbers by modifying call setup information
- the donor network now has **no** role, multiple portings easy; but requires lookup of **all** numbers

Two stage solutions



- Originating network simply learns the recipient network's number (called a **Logical Routing Number** (LRN), in North America this is a unique 10 digit number for the exchange)
- Recipient network does a second lookup to determine where to deliver the call within their network
- increases the privacy (since the originating network does not learn about the recipient network numbering)

All call/all network solutions



- each network does a lookup, but simply learns the “next” network’s number
- final recipient network does a second lookup to determine where to deliver the call within their network
- increases the privacy -- since all networks along the path only learn about the “next” network

Who knows the mappings?

Who knows the mappings?

For North America the **Number Portability Administration Center** (NPAC) has **all** the mappings and passes then to the operator's **Local Service Management System** (LSMS).

See also Neustar Number Pool Administration *http://www.nationalpooling.com/*

Swedish Number Portability Administrative Centre AB (SNPAC) officially appointed as the single operator of the Swedish **Central Reference Database [68]**; interaction follows ITS standard SS 63 63 91 [69].

see also regional numbering plan administrators:

- North American Numbering Plan (NANP) *http://www.nanpa.com/* (also performed by NeuStar Inc.)
- …

Nummerportabilitet i Sverige

- Europaparlamentets och rådets direktiv 98/61/EG om nummerportabilitet
- Sverige ändringar i telelagen (1993:597) 1 juli 1999
- Post- och telestyrelsen (PTS) om nummerportabilitet (PTSFS 1999:3 och PTSFS 2000:6).
- PTS beslut 15 augusti 2001 (ärende nr. 01-19102):

Swedish Number Portability Administrative Centre AB (SNPAC)

Peter Myndes Backe 12

118 46 Stockholm

(organisationsnr. 556595-2925)

http://www.pts.se/dokument/getFile.asp?FileID=2384

PTS recommended **All Call Query** (ACQ) as the preferred routing method for Swedish telecommunications networks [67]

EU Document 398L0061

[13.20.60 - Information technology, telecommunications and data-processing]

[13.10.30.20 - Research sectors]

Instruments amended:

397L0033 (Modification)

398L0061: Directive 98/61/EC of the European Parliament and of the Council of 24 September 1998 amending Directive 97/33/EC with regard to operator number portability and carrier pre-selection

Official Journal L 268 , 03/10/1998 p. 0037 - 0038

http://europa.eu.int/cgi-bin/eur-lex/udl.pl?REQUEST=Seek-Deliver&LANGUAGE=en&SERVICE=eurlex&COLLECTION=oj&DOCID=1998l268p00370038

Nortel Networks' Universal NP Master (UNMP)

A complete end-to-end **number portability** (NP) solution provides:

- **Number Portability Database** (NPDB) and **Number Portability Global Title Translation** (NPGTT) functionality as a single network element
- **Local Service Management System** (LSMS) for the management of the ported subscriber records
- support: AIN/IN and IS41 protocols for wireline and wireless porting services
- up to 11-digit GTTs for wireless number porting
- up to five million ported number records.
- Ported number service support includes Calling Name, CLASS, Inter-switch Voice Messaging, Line Information Database, Short Message Service, and PCS Call Delivery services.
- 5,000 queries per second, with planned expansion to 20,000 queries per second.

Lookup engines

Aeroflex UTMC (*http://www.utmc.com/ecard*) LNP-Engine (cPCI or PCI board):

- Stores up to 160 million 16-digit phone number pairs
- Supports 100k lookups/sec. and 10K updates/second

Based upon two Content Addressable Memory Engines:

- custom 100 MHz chip
- lookup in as little as 100 nanoseconds
- partitions memory into upto 8,192 tables, from 256 to 30 million records
- programmable key widths (per table): from 1 to 32 bytes
- programmable association widths (per table) up to 8 megabytes
- performs exact matches, as well hierarchal, longest-prefix, and proximity matches
- pipelined operation with separate I/O FIFOs
- bulk table load, unload, and count functions
- handles table overflows

Voice over IP (VoIP)

Integrating VoIP with mobile telephony

TIPHON

ETSI's Telecommunication and Internet Protocol Harmonization over Network (TIPHON) - *http://www.etsi.org/frameset/home.htm?/tiphonweb/*

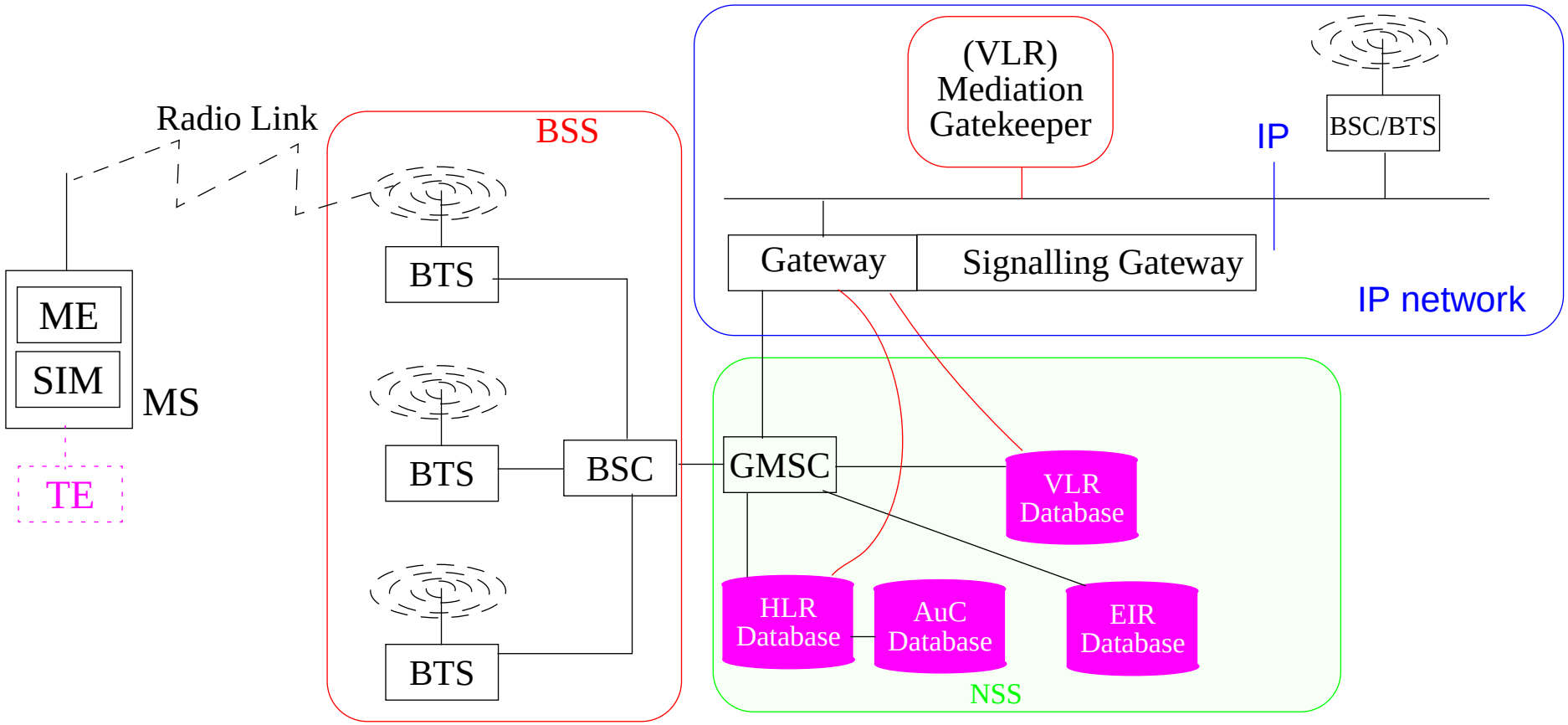


Figure 27: TIPHON Architecture

Ericsson's GSM on the Net

Olle Granberg, "GSM on the Net", Ericsson Review No. 04, 1998[1]

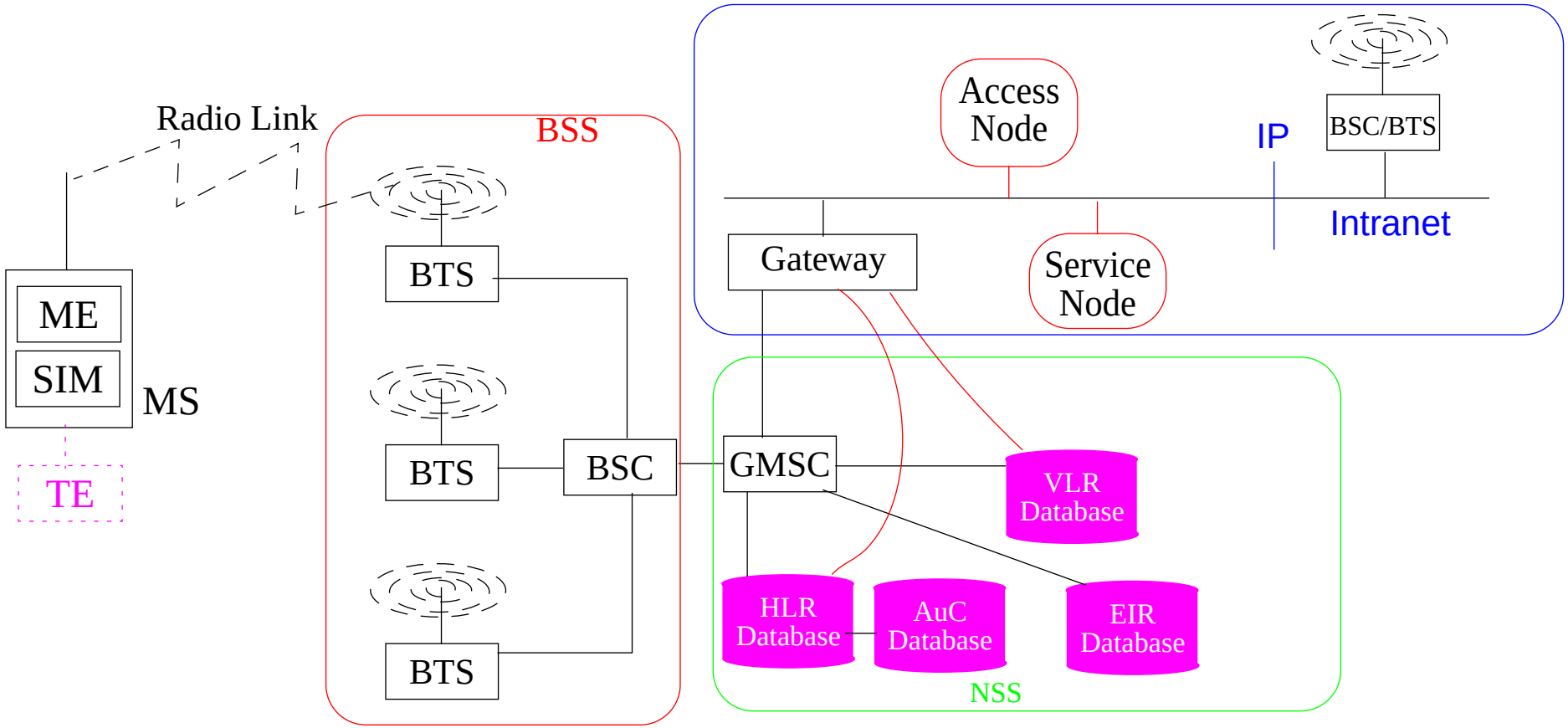


Figure 28: Ericsson's GSM on the Net Architecture

1. http://www.ericsson.com/about/publications/review/1998_04/files/1998046.pdf

iGSM

Proposed by Yi-Bing Lin and Imrich Chlamtac in section 16.2([1], pp. 290-293).

This architecture is really a joining of H.323 with a gateway to GSM.

Prepaid

Customer pays **before** using service.

Advantages:

- operator has the money - all up front (**no risk** and they can even earn interest on it)
- operator **saves**: no need for: credit checking, invoices, collections, …
- customer: no need for credit worthiness, no need for a contract, immediate service, anonymous service is possible
- since for many cultures and countries there is no tradition or infrastructure for post-paid service - business is strictly cash up front -- prepaid fits well with the expectation of these customers
- prepaid value can be installed in devices (such as toys, jewelry, …)
- many customers will never use up all their balance - it will simply be abandon -- much to the delight of the operator {It is “like printing money”!}

GSM Prepaid

Prepaid credit is either kept in the SIM card or in the network.

When the balance is zero, customer can only receive calls. {this may be limited by the operator}

To refill:

- customer buys a refill/top-up card with a secret code
- dials a freephone number to an Interactive Voice Response server
- enters MSISDN number of their phone + secret code
- system verifies secret code (so code can only be used once), then refills the account

Difference between Mobile and Fixed Prepaid

Mobile servers needs:

- more complex billing system due to more complex **tariffs** (which can be location dependant!)
- more complex billing system due to more complex **taxation** (which can be location dependant!)
- real-time usage metering - which has to cut off service when balance is zero (there is a trade off between accuracy and cost of implementation - if the operator is willing to take some loss, the implementation can relax the real-time constraints)
- increased complexity of customer care: warning customer to refill in a timely fashion (maintaining a credit balance - maintains cash at the operator!)

Four alternatives for Mobile Prepaid

- **Wireless Intelligent Network** (WIN)
- Service Node
- Hot Billing
- Handset-Based

Wireless Intelligent Network (WIN)

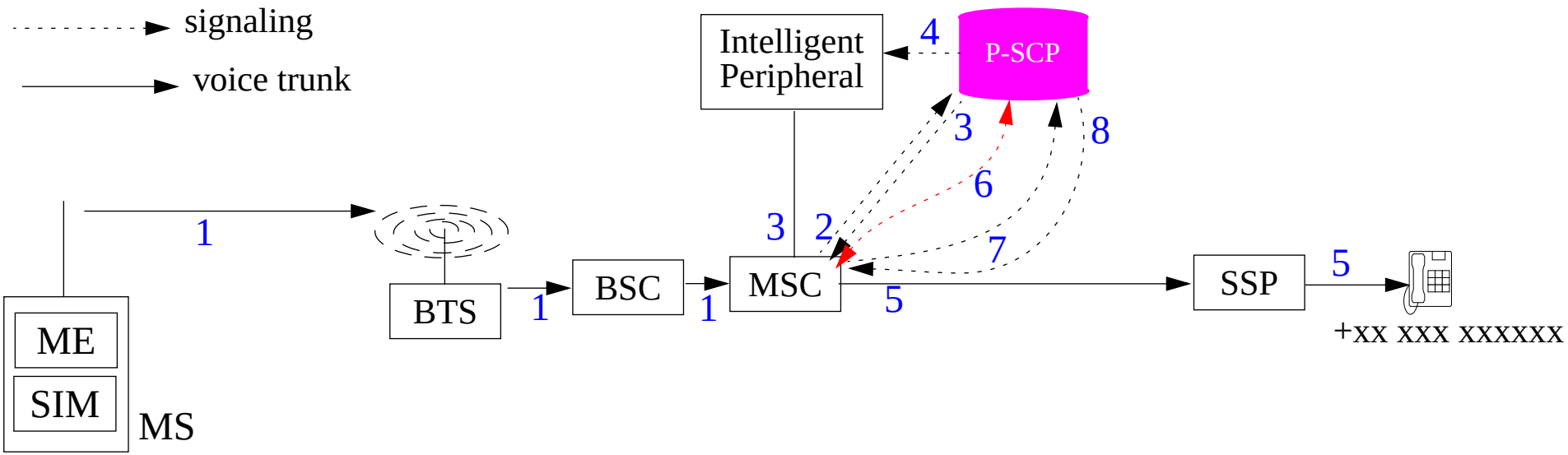


Figure 29: WIN Prepaid call origination

1. Prepaid mobile customer calls +xx xxx xxxxxx
2. MSC gets WIN call setup trigger, call setup suspended, message sent to Prepaid Service Control Point (P-SCP)
3. P-SCP instructs MSC to set up ISDN (voice) link to intelligent peripheral
4. P-SCP instructs intelligent peripheral to provide **account status notification** (balance, charging rate, …) for this call
5. P-SCP starts countdown timer & instructs MSC to resume call processing -- which connects the call
6. Call terminates: either (a) countdown timer expires (P-SCP instructs MSC to terminate call) or (b) call completes
7. MSC gets WIN call release trigger, sends disconnect message to P-SCP indicating duration of call
8. P-SCP rates the call (computes charges) and debits the prepaid balance, sends current balance and cost of call to MSC

Calling party pays vs. Called party pays

Calling party pays style billing - Europe, Taiwan

Called party pays style billing - US (where mobile subscriber pays for ***both*** incoming and outgoing calls)

WIN Call termination when called party pays

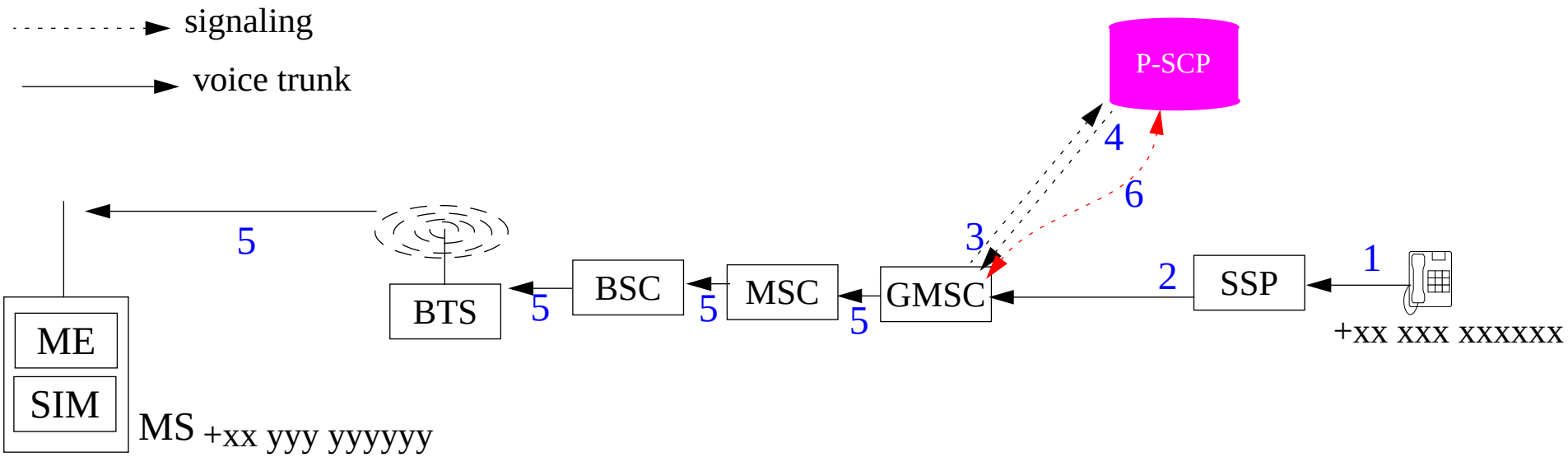


Figure 30: WIN Prepaid call termination

1. Caller dials prepaid mobile customer +xx yyy yyyyyy
2. Call forwarded to gateway GMSC
3. GMSC get a WIN call setup trigger, suspends call processing, sends message to P-SCP
4. P-SCP determines if mobile is allowed to receive this call, if so instructs GMSC to resume call setup procedure
5. GMSC connects the call
6. P-SCP monitors called party's balance and can terminate the call if there is no credit (just as per call origination case)

Service Node

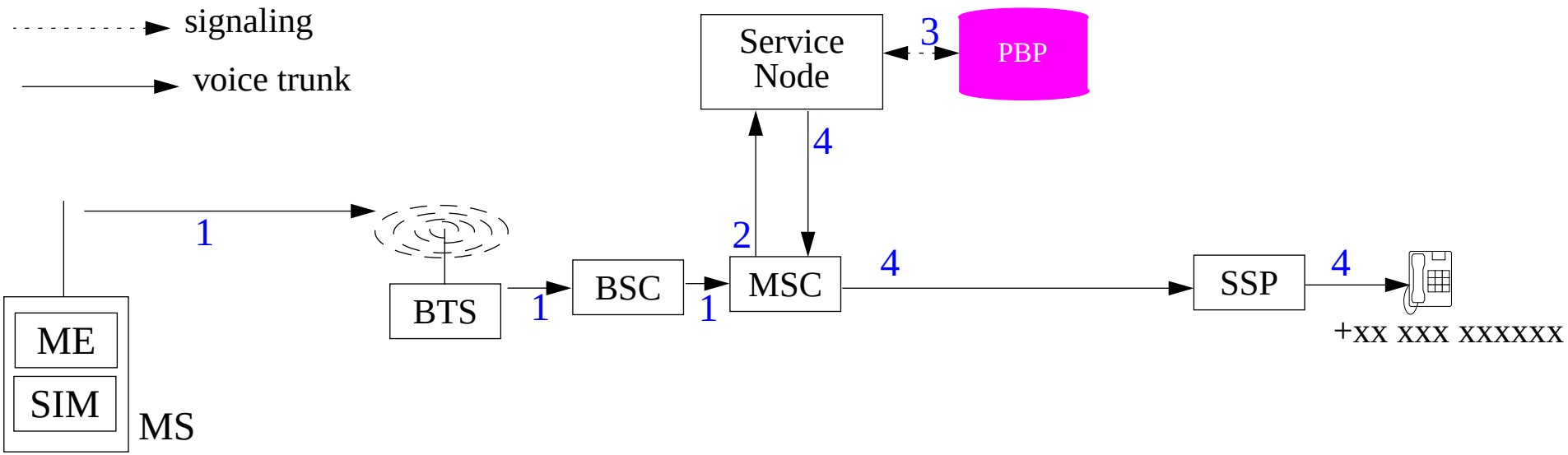


Figure 31: Service Node Prepaid call origination

1. Prepaid mobile dials called party (+xx xxx xxxxxx)
2. MSC detects this is a prepaid customer and sets up trunk to service node
3. Service node consults Prepared Billing Platform (PBP) to determine if the call should be allowed
4. If so, then a 2nd trunk is setup from the service node via the MSC to the called party

Note: at the cost of the 2nd trunk (and two ports of MSC), this is a very easy service to build - since the MSC does not actually know about the prepaid service - only that it is to connect calls from these customers to the service node.

Hot Billing

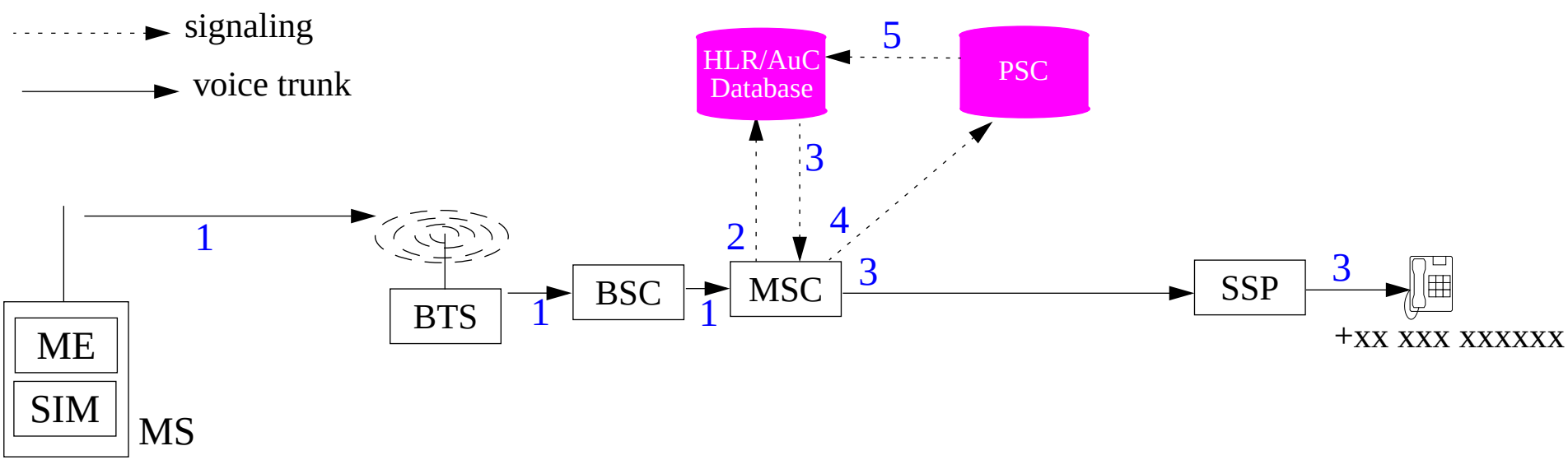


Figure 32: Hotbilling Prepaid call origination

1. Prepaid mobile dials called party (+xx xxx xxxxxx) and sends their own IMSI
2. Based on IMSI, MSC asks HLR/AuC if this is a valid service request
3. If verified, HLR/AuC sends customer data and a prepaid tag to MSC, MSC connects call
4. When call terminates, a Call Detail Record (CDR) is sent to the Prepaid Service Center (PSC)
5. PSC debits the account, if the account is out of funds it notified the HLR/AuC to suspend service!

With hot billing the operator is taking a risk (of the cost of the call exceeding the balance), but it is a "**one-call exposure**" and reduces the complexity of the system.

“**one-call exposure**” in depth

Since the operator may have no idea of who this customer is, they have no way of collecting on the “bad debt”, thus they try to avoid it:

- Use large values for the initial payment and refill/top-up - thus the account has quite a ways to go before it is depleted (i.e., no low value prepayments)
- prohibit call forwarding to prepaid accounts (since otherwise you could simultaneously forward lots of calls through a given prepaid account at one time and “one-call” suddenly becomes “N-calls”!)
- increase the interval at which CDRs are sent for processing {but this costs in increased load on the PSC} -- in fact the trend is towards the opposite, send bunches of CDRs are one time rather than in “real-time” as calls end {this decreases load on PSC, but increases bad debt exposure} -- in the end it is a business decision of risk/reward

Handset-Based

Uses GSM Phase 2, Advice of Charge (AoC):

- Advice of Charge Charging (AoCC) ⇐ this is how you debit the balance in the SIM card
- Advice of Charge Information (AoCI)

Builds upon sever SIM data fields:

- accumulated call meter (ACM)
- accumulated call meter maximum (ACM*)
- price per unit and currency table (PUCT)

Prepaid service center (PSC) uses SMS messages to execute program in the handset, these applications are controlled by the SIM Toolkit.

Different sized SIM cards may be needed if large tariff rate tables or complex rating schemes are to be used.

ACM and ACM* are generally user accessible (via PIN2), but for prepaid cards this access is disabled (either at time of manufacture or via an SMS message when users subscribes to prepaid service).

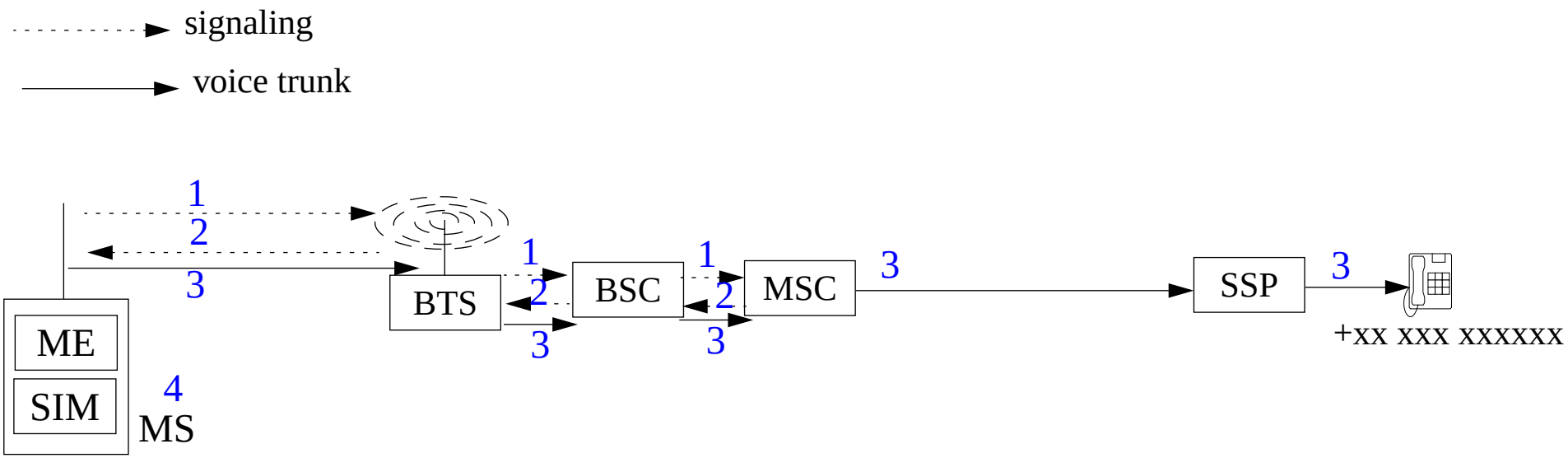


Figure 33: Handset-Based Prepaid call origination

1. Prepaid mobile dials called party (+xx xxx xxxxxx)
2. Based on rate plan (+ destination, time/date), MSC sends AoC e-parameters (including ACM and ACM*) to mobile
3. If mobile support AoCC, it acks receipt of e-parameters; if MSC gets this ack, call is connected, otherwise call is denied
4. During call MS uses AoC e-parameters for tariff info; locally decrements credit by incrementing ACM. When ACM reaches ACM*, MS terminates call and informs MSC of call release

Combined Handset-based + Hot Billing

For fraud reduction, Handset-based approach can be combined with the Hot billing approach - thus if PSC thinks there is no credit but SIM claims credit, the PSC can inform operator to: terminate service and/or trigger fraud investigation.

Unfortunately, the disagreement might be legitimate due to poor synchronization (of charging information) between PSC and MS.

Roaming and Prepaid

Lots of problems:

- can’t easily use special MSISDN numbers as this would:
  - prevent operator number portability
  - service portability is not allowed, since you could not change to post paid without changing MSISDN
  - could use IMSI, but this might require software change at visited system
- prepaid charging might not be performed at visited system (because it uses a different prepaid scheme than home system)
  - therefore route the call via the home system - letting it implement the prepaid debiting
  - but this requires a trunk to the home system ($\Rightarrow$ higher charge for a specific prepaid call than a postpaid call) -- this may be too expensive for international roaming
- scalability problems with service node approach (since you use up two MSC ports per call)
- AoC traffic is not encrypted - so the handset can just tamper with or ignore debit commands! $\Rightarrow$ manufactures working on SIM encryption
- handset-based approach may lock operator to a SIM supplier
- some of the schemes have a high setup cost

Further reading

Number portability

[64] Tango Telecom,"Number Portability: a white paper", Tango Telecom, wpnp01-18/02/00

[65] Barry Bishop, "LNP, Pooling and IVR: What are the impacts to Public Safety Organizations and Law Enforcement?", Lockheed Martin, *http://www.numberpool.org/law_911_registration/apco.ppt*

[66] North American Number Portability Administration Center (NPAC) (*http://www.npac.com*)

[67] Olle Röding, "NUMBER PORTABILITY IN SWEDEN: A project summary", YABSA Informatik AB, Saltsjöbaden, Sweden - *http://www.hif.hu/menu6/m6_3/pdf_p/13w5%20yabsa.pdf* , the author was responsible for

- "Principal design and specification of the Central Reference Database for number portability in Sweden"
- "Development & definition of business model and operational model for SNPAC AB", …

[68] Swedish Number Portability Administrative Centre AB
http://www.snpac.se/

[69] Number portability in Sweden: Administrative process for number portability, including the administrative interface and the central reference database (Nummerportabilitet i Sverige Administrativa rutiner för nummerportabilitet inkluderande administrativa gränssnitt och central referensdatabas), Swedish Standard SS 63 63 91, 2000-03-14,
http://www.its.se/ITS/ss6363x/SS636391-ed2.pdf

[70] Number Portability in Sweden - Network solutions for Service Provider Portability for public digital mobile telephony services, Swedish Standard SS 63 63 92, 2000-03-14,
http://www.its.se/ITS/ss6363x/SS636392-ed1.pdf

VoIP

[71] G. Q. Maguire Jr., “2G1305: Internetworking”, Lecture notes, Period 3, 2002
http://www.it.kth.se/edu/gru/Internet/Coursepage-Spring-2002.html

[72] G. Q. Maguire Jr., “2G5564 Practical Voice Over IP (VoIP): SIP and related protocols”, Lecture notes, Period 3, 2003
http://vvv.it.kth.se/edu/Ph.D/2G5564/VOIP-Coursepage-Spring-2003.html

Prepaid

[73] Gemplus, “Smart Card in Wireless Services”, {perhaps a bit biased since they are one of the leading vendors of smart cards}

KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

5. WAP, Heterogeneous PCS, 3G

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Last modified: 2003.03.13:11:56

Lecture 5

- WAP (Ch. 19), Heterogeneous PCS (Ch. 20), 3G (Ch. 21)

Wireless Application Protocol (WAP)

Goal: a set of communication protocol standards to make accessing online services from a mobile phone simple

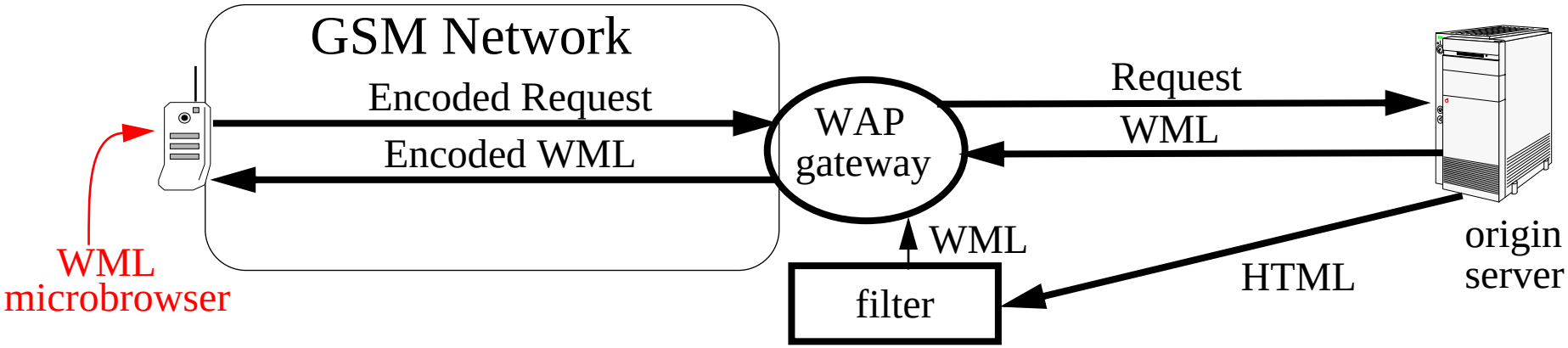
> "The motivation for developing WAP was to extend Internet technologies to wireless networks, bearers and devices."[74], page 4.

Initially conceived by four companies: Ericsson, Motorola, Nokia, and Unwired Planet (today called Phone.com)

WAP Forum is an industry association to promote WAP, they are now called "The Open Mobile Alliance Ltd." *http://www.openmobilealliance.org/*

WAP Model

Now called the WAP “Proxy Model” - since WAP gateway acts as a proxy:



The basic (erroneous) thoughts behind WAP were:

- that terminals were “limited” in processing/memory/display,
- that the communication channel was expensive,
- that the operator was “the” natural intermediary in every mobile user’s interaction with any services, and
- that a special protocol stack was necessary to “optimize” for the above.

Push services

In push services **content** is sent to the user without the user requesting it.

WAP (first round) Summary

Massive failure, because:

- tried to introduce a WAP protocol stack
- did not really provide an **end-to-end service** {because they wanted to keep the operator in the middle of all transactions} - the result is that content was in clear text in the WAP gateway
  - the result was significant security problems - especially because the changes that were introduced into the “WAPified” SSL introduced problems
- most operators used SMS to carry the WAP traffic and this was too expensive and had very significant delay problems
- many terminals had problems with their software and each type had its own resolution, size, … - so content had to be prepared for a specific terminal {which increased content development costs - since automatic conversion was not really successful}

WAP 2.0 moves toward being an IP based stack (with HTTP, TLS, and TCP) - although of course they still support their earlier “optimized/wapified” stack. The new model is a direct connection between mobile and HTTP server.

WAP 2.0

Wireless Profiled HTTP (WP-HTTP)	a profile of HTTP for the wireless environment and is fully interoperable with HTTP/1.1. Built on HTTP request/response transaction. Supports message body compression of responses and the establishment of secure tunnels.
Transport Layer Security (TLS)	a wireless profile of the TLS protocol, includes cipher suites, certificate formats, signing algorithms and the use of session resume. Support end-to-end security at the transport level.
Wireless Profiled TCP (WP-TCP)	provides connection-oriented services, optimized for wireless environments and fully interoperable with standard TCP implementations. Builds upon IETF Performance Implications of Link Characteristics (PILC) working group recommendations
Wireless Session Protocol (WSP)	Wireless Transaction Protocol (WTP), Wireless Transport Layer Security (WTLS), Wireless Datagram Protocol (WDP) - as now “Legacy Protocol Layers”[74]

WAP 2.0 new & enhanced services

WAP Push	allows content to be sent or "pushed" to devices by server-based applications via a Push Proxy; real-time applications; provides control over the lifetime of pushed messages, store&forward capabilities at the Push Proxy, control over bearer choice for delivery.
User Agent Profile (UAProf)	provides a mechanism for describing the capabilities of clients and the preferences of users to an application server, based on the Composite Capabilities / Preference Profiles (CC/PP) work of the W3C Wireless Telephony Application (WTA)
External Functionality Interface (EFI)	specifies the interface between WAE and components or entities with embedded applications that execute outside of the defined WAE capabilities (i.e., basically allowing plug-in modules) - thus allowing access to external devices (e.g. smart cards, GPS, digital cameras, sensors, …)
Persistent Storage Interface	a standard set of storage services and interface for organizing, accessing, storing and retrieving data on the wireless device or other connected memory device.
Data Synchronization	adopts SyncML language for the data synchronization (see www.syncml.org)
Multimedia Messaging Service (MMS)	permits delivery of varied types of content
Provisioning	provides clients with information needed to operate on wireless networks; permits network operator to manage the devices on its network using a common set of tools
Pictogram	tiny images, that can be used to quickly convey concepts in a small amount of space

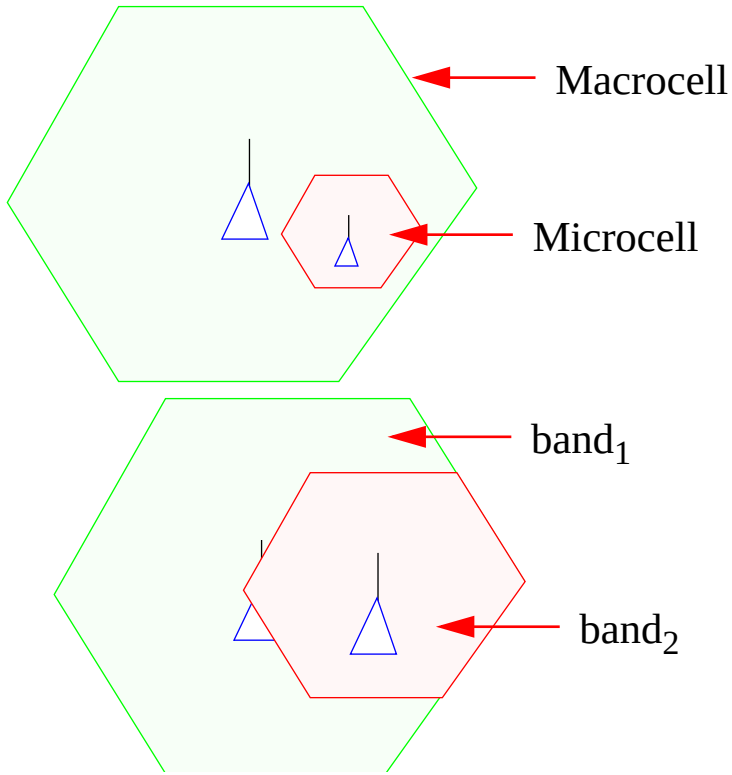
Heterogeneous PCS

Utilize multiple types of radios to get the advantages of each to:

- increase capacity and/or
- increase coverage area and/or
- decrease power consumption and/or
- increase bandwidth and/or
- decrease delay, …

Similar Radio technologies + Same Network technology (SRSN)

with different power levels	different size cells; for example macrocells with microcells for hotspot coverage; microcells “borrow” radio channels from the macrocellular system - so that they use a different channel than the overlapping macrocell
with different frequency bands	multiband system such as: GSM900+GSM1800macrocell since the cells can overlaps arbitrarily they can of course be of different sizes



Different Radio technologies + Same Network technology

Both using IS-41 as network protocol:

- IS-136 + AMPS
- IS-95 +AMPS

Different Radio technologies + Different Network technology

Generally high-tier PCS with low-tier PCS

Examples:

- AMPS +PACS or GSM +PACS
- GSM + DECT

Tier Handoff

Tier Handoff performs handoffs from one system to another.

For the case of SRSN - different power levels, the macro and microcells use the same air interface and the handoffs is as usual.

For the case of SRSN - different bands, just a little harder than usual (because the handset might not be able to listen to more than one frequency at a time).

For the case of DRSN it is harder yet generally requires modification in the handoff of each system, in some cases the handoff might only work in one direction

For the case of DRDN the easiest is to simply set up a new call (perhaps via automatic redial) in the new network.

Registration for SRSN & DRSN

Fairly straight forward since the systems use the same network technology.

Key problem is: Who does the tier selection?

Registration for DRDN

Since the different systems use different registration & authentication and different data may be store in their different HLRs (and VLRs) ⇒ define a new **multitier HLR** to integrate the two.

Implemented via **tier manager**

Single (SR) vs. Multiple registrations (MR) - the former is simpler, the later reduces the registration traffic and decreases the time required for tier handoffs.

Call delivery

SR case	simply query the MHLR to find where to deliver the call
MR case	either select the tier to try based on some heuristic (for example, always try low-tier first or try the system where the MS register most recently) or page first, then try the one where you get a response

User identity (identities) and MSs

Their can be

- a single identity or several identities
  - user can be associated with a single logical “number” or multiple
  - identities can have a primary association with a MS or no
- single or multiple MSs
  - user can use one (multimode MS) or several MSs
  - D>oes the user choose which device to use or does the multitier manager?

A hard problem is what to do when the service (for example, streaming video) only makes sense on a subset of the MSs or PCS systems.

Major forces driving heterogeneous PCS

consolidation/mergers&acquisitions/bankruptcy/… ⇒ new owner may end up owning several different types of systems, examples:

- AT&T acquisition of McCaw's cellular system
- Bell Atlantic merger with NYNEX
- Merger of Vodaphone with AirTouch
- DeutscheTelekom's (T-Mobile) Voicestream Wireless Corp. acquistion of WLAN operations of MobileStar

Third Generation Mobile (3G)

Offering data rates greater than ISDN (144kbps), typically thought to be 384kbps and perhaps upto 2 Mbps when stationary near a base station.

Six types of services:

- Interactive multimedia (video conferencing)
- High speed multimedia (“broadcast” TV)
- Medium speed multimedia (web browsing)
- Circuit switched data (FAX)
- Speech (telephony)
- Messaging (e-mail, SMS, …)

All based on CDMA; Europe’s Universal Mobile Telecommunications System (UMTS) will be Wideband CDMA (W-CDMA, 25 MHz channel bandwidth):

- ETSI agreed to use a combination of wideband code division multiple access (W-CDMA) and time division multiple access (TD/CDMA) on the air interface
- W-CDMA will be used to cover larger areas
- TD/CDMA for local (indoor) applications

Paradigm shifts

- voice-centric ⇒ data centric
  - shift to packet switching
  - problems: QoS, streaming media
- continually evolving terminals and data applications - end users **expect** the same services (and more) from wireless systems as they expect from wireline systems

3rd Generation Partnership Project (3GPP)

Original scope was to produce **globally applicable** Technical Specifications and Technical Reports for a **3rd Generation Mobile System** based on evolved GSM core networks and the radio access technologies that they support ⇒ Universal Terrestrial Radio Access (UTRA)[1], W-CDMA, UMTS (in Europe) and FOMA (in Japan)

Amended to include the 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**)).

See: *http://www.3gpp.org/*

ETSI is the 3GPP Secretariat

1. Both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes.

Third Generation Partnership Project 2 (3GPP2)

A collaborative third generation (3G) telecommunications standards-setting project comprising **North American** and **Asian** interests developing global specifications for **ANSI/TIA/EIA-41** “Cellular Radiotelecommunication Intersystem Operations network evolution to 3G”, and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41.

Focus is cdma2000

See: *http://www.3gpp2.org/*

TIA is the 3GPP2 Secretariat

Mobile Station Application Execution Environment (MExE)

Building on ideas from WAP, UMTS introduces a Mobile Station Application Execution Environment (MExE) to provide a standard environment for the MS to access the internet and intranet services.

MExE Classmark

classifies the MS based on its capabilities (processing, memory, display, …)

MExE classmark 1	based on WAP
MExE classmark 2	based on PersonalJava (supports JavaPhone Power Monitor package)
MExE classmark 3	based on Java 2ME Connected Limited Device Configuration (CLDC) and Mobile Information Device Profile (MIDP) environment - supports Java applications running on resource constrained devices.
MExE classmark 4	based on ECMA's Common Language Infrastructure Compact Profile - supports CLI based applications running on resource constrained devices (CLI designed to be programming language and OS neutral)

Common Language Infrastructure for MExE devices: Classmark 4

Service discovery and management

Browser installed on a MExE device should support MIME type text/vnd.sun.j2me.app-descriptor. Allows user to browse and discover a Java application which can then be downloaded. Capability negotiation information in the request header can determine which application to present.

MID applications (MIDlets) and MIDlet suites are indicated to the user, if the terminal has a display, may be presented as an icon and a tag or as a textual tag

Java Application Description (JAD) file can be downloaded and to determine if the MIDlet is suitable for download and installation

- If it is, then JAR file can be downloaded and installed
- If not, the MExE UE should be able to prompt the user so that the user (they can delete some existing applications if there is not enough space to install the new application)
- If the application chosen already exists on the device, the user should be notified so they can choose to either to download the chosen version or to retain the existing one
- user should be able either to launch the MIDlet immediately or later

CLI MExE Devices

SMExE Classmark 4 devices based on CLI Compact Profile spec.: defines runtime environment and APIs available to a CLI based MExE device such that services (specified in the form of language independent classes and interfaces) can control such a device in a standardized way.

CLI Compact Profile Namespaces

- System
- System.Collections
- System.Globalization
- System.IO
- System.Text
- System.Threading
- System.Runtime.CompilerServices
- System.Reflection
- System.Net
- System.Xml

Application management features for a Classmark 4 application

- Discovery
- Download
- Verification
- Installation
- Execution Start
- Execution Pause
- Execution Resume
- Execution Stop
- Execution Terminate
- Uninstall

Support for network protocols

Protocol	Optionally		
HTTP/1.1	Mandatory	Gopher	Optional
HTTPS	Mandatory	ftp	Optional
SOAP	Mandatory	mailto	Optional
		File	Optional

3G Physical Layer

There has been great fighting over what is the “best” physical and link layer for 3G, due to political, economic, … reasons.

Indications are that there will be several 3G CDMA modes (at least 5 different choices), but there might be some hope for harmonization at the network level (with at least 3 choices: ANSI-41, GSM MAP, and IP)!

Gateway Location Register (GLR)

3GPP introduces a **Gateway Location Register** (GLR) to reduce traffic between VLR and HLR {especially for the case of international roaming}. The GLR is located in the visited network.

While it can clearly reduce signaling costs when the user is not in their home country - the book does not address the question of “Does this really matter?” Since there is an enormous amount of bandwidth available via fibers - does the signaling traffic really matter? Does the GLR reduce the delays for providing service to the user?

3G QoS

Four QoS classes:

conversational	for delay sensitive traffic, with limited transfer delay
streaming	for one-way real-time traffic
interactive	for delay-insensitive traffic such as e-mail, telnet, …
background	for delay-insensitive traffic such as FTP, background bulk transfer of e-mail, …

7 QoS parameters: max/min/guaranteed bit rates, max. packet size, reliability, …

Major problems with how to **map** between the QoS of different systems.

UMTS Subscriber Identity Module (USIM)

3GPP specifications:

TS21.111	USIM and IC card requirements
TS22.112	USIM toolkit interpreter; Stage 1
TS31.111	USIM Application Toolkit (USAT)
TS31.112	USAT Interpreter Architecture Description; Stage 2
TS31.113	USAT interpreter byte codes
TS31.114	USAT interpreter protocol and administration
TS31.115	Secured packet structure for (U)SIM Toolkit applications
TS31.116	Remote APDU Structure for (U)SIM Toolkit applications
TS31.120	UICC-terminal interface; Physical, electrical and logical test specification
TS31.121	UICC-terminal interface; USIM application test specification
TS31.122	USIM conformance test specification
TS31.131	C-language binding for (U)SIM API
TR31.900	SIM/USIM internal and external interworking aspects
TS42.017	Subscriber Identity Module (SIM); Functional characteristics
TS42.019	Subscriber Identity Module Application Programming Interface (SIM API); Stage 1
TS43.019	Subscriber Identity Module Application Programming Interface (SIM API) for Java Card; Stage 2
TS51.011	Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface
TS51.013	Test specification for SIM API for Java card

Wireless Operating System for Handsets

There has been a battle brewing for who will define and dominate the OS market for 3G handsets - which given the expected handset volume could be a very large market.

Candidates:

- Microsoft - WinCE (and its successors)
- Symbian's EPOC OS - built upon Psion's OS - Symbian formed by Nokia, Ericsson, Motorola)
- 3Com's PalmOS
- linux

Mobile Virtual Network Operator (MVNO)

A virtual operator who uses the physical infrastructure of other operators.

Pyramid Research projects a greater than 3x ROI for MVNOs vs. facilities-based UMTS network operator[1].

See: *http://www.pyramidresearch.com/info/rpts/mvno.asp*

Richard Branson's Virgin Mobile signed up 700k customers in their first year![2]

"Freed from a large subscriber base that is necessary to cover network deployment costs, an MVNO can target a more finely segmented market."[3]

Mobile Virtual Network Operators: Oftel inquiry into what MVNOs could offer consumers - *http://www.oftel.gov.uk/publications/1999/competition/mvno0699.htm*

---

1. *http://www.pyramidresearch.com/static_content/feature_articles/010402_feature.asp*
2. *http://www.adventis.com/mvno/main.htm*
3. *http://www.gii.co.jp/english/pr8818_mvno.html*

πG

See: Theo Kanter, “Adaptive Personal Mobile Communication -- Service Architecture and Protocols”, Tekn. Dr. Dissertation, KTH, December 14, 2001

http://ps.verkstad.net/Thesis/Final/theoDissertation.pdf (6271k)

4th generation?

Matthias Unbehaun, “Self-deployed Wireless Access Networks”, Doctoral dissertation, Radio Communication, KTH, 2002.

Further reading

WAP

[74] WAP Forum, “Wireless Application Protocol (WAP) 2.0 Technical White Paper”, www.wapforum.org, January 2002.

Heterogeneous PCS

[75] Ian F. Akyildiz and Wenye Wang, “A Dynamic Location Management Scheme for Next-Generation Multitier PCS Systems”, IEEE Transactions on Wireless Communications, Vol. 1, No. 1, January 2002, pp. 178-189.

3G

[76] Janos A. Csirik, “A guide to 3GPP security documents”, AT&T Research, http://www.research.att.com/~janos/3gpp.html

[77] Gavin Stone, MExE: Mobile Execution Environment White Paper, Ronin Wireless, MExE Forum, Dec. 2000

[78] 3rd Generation Partnership Project (3GPP) - www.3GPP.org

[79] www.3GPP2.org

[80] 3GPP TS 23.057 V4.4.0 (2001-12) 3rd Generation Partnership Project Technical Specification Group Terminals Mobile Station Application Execution Environment (MExE), Functional description, Stage 2 (Release 4) http://www.3gpp.org/ftp/Specs/2001-12/Rel-4/23_series/23057-440.zip

[81] PersonalJava™ Application Environment http://java.sun.com/products/personaljava

[82] JavaPhone™ API http://java.sun.com/products/javaphone

[83] Java 2 Micro Edition http://java.sun.com/j2me

[84] Connected Limited Device Profile (CLDC) http://java.sun.com/products/cldc/

[85] Mobile Information Device Profile (MIDP) http://java.sun.com/products/midp/

[86] ECMA's Common Language Infrastructure (ECMA-335)
http://cedar.intel.com/media/zip/ECMA-335.zip

[87] ECMA's Common Language Infrastructure Technical Report (ECMA-TR-084)
http://cedar.intel.com/media/zip/ECMA-TR-084.zip

[88] Erik Meijer and John Gough, "Technical Overview of the Common Language Runtime",
http://research.microsoft.com/~emeijer/Papers/CLR.pdf

KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

6. Wireless Local Loop (WLL) and Enterprise Networks

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Last modified: 2003.03.13:11:54

Lecture 6

- Wireless Local Loop (WLL) (Ch. 23), Enterprise Networks (Ch. 24)

Wireless Local Loop (WLL)

Providing wireless connections to stationary or near stationary stations within a small service area

Generally targeted at the “last mile” or from a point in the neighborhood to the user

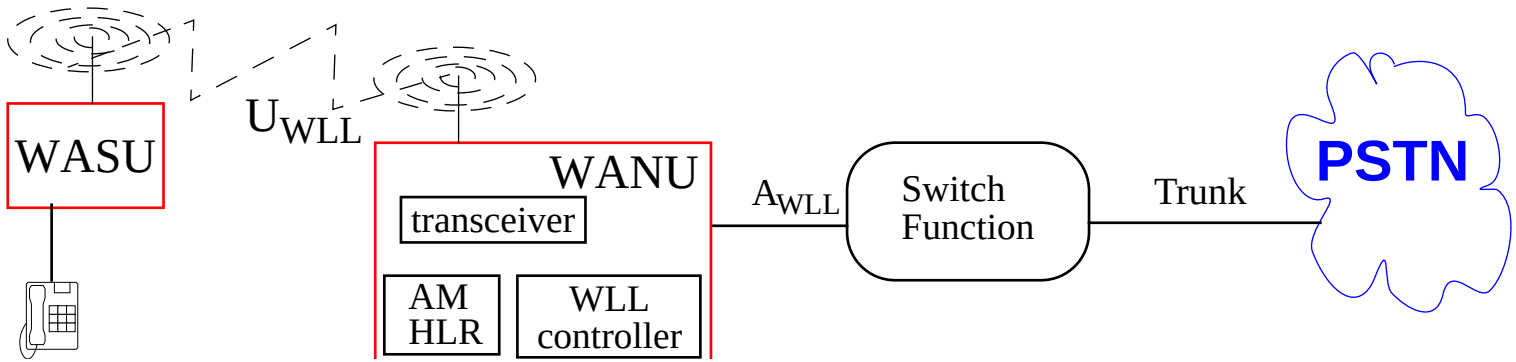
Advantages of Wireless local loop:

- ease of installation
  - reducing digging, reduce poles, ducts/conduits, …
  - quick installation of new links (i.e., rapid provisioning)
  - largely distance insensitive pricing - at least up to some limit
- concentration of resources (especially at the multiplexer to the high bandwidth backbone)

IS-54 architectural reference model for WLL:

WANU = Wireless Access Network Unit

WASU = Wireless Access Subscriber Unit



Deployment issues

- **Spectrum**
  - licensed - limited interference, but requires licensing
  - unlicensed - more interference, but no licensing - generally limited in (maximum and average) power
- **Service Quality**
  - Users expect it is going to be the same as wireline service
  - high reliability
  - low risk of fraud (due to others “hijacking” the link)
- **Network planning**
  - should support very high penetration levels (for example >90%)
  - exploits the fact that users are not moving (or rarely move)
  - antenna height, etc. is generally derived from user density

Very popular in the former “East block” of Europe - since there was no need to install a local loop cable to bring users to the local exchange of the PSTN; enabled very rapid provisioning to very large numbers of subscribers.

WLL Technologies

- **Satellite**
  - a great chance for the satellite operators (Hughes Network Systems, Inmarsat International Circular Orbit (ICO), Iridium, Globestar, Odyssey, American Mobile Satellite Corporation (AMSC), Asia Cellular Satellite (ACeS), Thuraya, …)
  - note that some of these operators (such as Hughes) used terrestrial versions of their system
- **Cellular-based**
  - used in rural and sparse urban settings
- **Low Tier PCS** or **Microcellular** based systems
  - PACS, PHS, DECT, …
- **Fixed Wireless Access** (FWA)
  - some times proprietary point-to-point links
  - increasingly LMDS

Enterprise Networks

Networking within an organization - often campus networking. Traditional voice enterprise networks were based on a PBX, today this often extended by cordless telephony, wired LANs, and WLAN systems.

Enterprise based location systems (such as Ericsson DECT mobility server, which enabled redirecting a DECT call to any Ericsson site from the user's home site).

Olivetti& Oracle Research Labs (now AT&T Research Labs) in Cambridge developed an active badge system which used IR emitting badges (called *active badges*) to locate users with in the building. This enabled delivering a phone call to the nearest fixed line phone, logging who visited who, finding people and equipment, … . Their recent project uses ultrasound for location: *active bat*s.

Theo Kanter and colleagues at Ellemtel showed a system in the mid-1990s which utilized SmartBadges (developed at KTH, HP, and Univ. of Wollongong) to locate users and by providing voice gateways the could direct a user's calls to computers, cordless, or mobile phones as appropriate.

Cordless PBXs

For example, Ericsson's MD110 Communication System (aka "Consono") -- which is a DECT based system - simply attaches DECT base stations to their PBX.

See *http://www.ericsson.com/enterprise/products/md110.shtml/index.shtml*

Telia provides packages where the user can pay:

- per line/month - fixed
- per line/month - DECT (with local mobility support)
- per line/month - DECT (with mobility support over several exchanges)
- per line - DECT (with local or multiple site mobility) - but only outgoing/incoming trunk costs/month
- …

Virtual enterprise networks

By utilizing location based billing, it is possible to offer an enterprise a virtual cellular PBX (ala the Centrex systems for fixed telephony). In such a system the operators negotiates a price for providing coverage to a campus or set of coverage areas - typically for a fixed price for a year (or more).

The operator likes this as they know they have a given amount of income and they know what their fixed costs for installing a base station to cover the relevant areas is. As a side effect they may also be able to handle calls for other users -- and not have to pay for renting antenna and other space!

Remoting the office to where the user is

A rapidly growing area of business utilizes Virtual Private Network technology to extend the corporate network (voice, fax, data, file system, etc.) to where the user is and via what ever communications interconnect that is available.

(See for example: Ericsson's Virtual Office (EVO))

Unified Communications

- Integrated messaging
  - Cellular, cordless, fixed lines - are share the same voice mailbox, potentially with interface to e-mail, …
- Synchronizing calendars, phone books, …
- Synchronizing services across many devices (which may be using different networks)
- Ericsson's **Always Best Connected** (ABC) - to use the best technology for the current setting

KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

7. Bluetooth

Lecture notes of G. Q. Maguire Jr.

Last modified: 2003.03.13:11:54

Lectures 7 & 8

- Bluetooth: Piconets, Scatternets

Bluetooth name comes from Danish king Harald Blåtand (Bluetooth), credited with uniting the Scandinavian people during the 10th century.

The idea was that Bluetooth wireless technology would unite personal computing devices.

Bluetooth™

Bluetooth is a trademark owned by the Bluetooth SIG, Inc., USA.

Bluetooth Special Industry Group (SIG) formed in winter of 1998 by Ericsson, IBM, Intel, Nokia, and Toshiba.

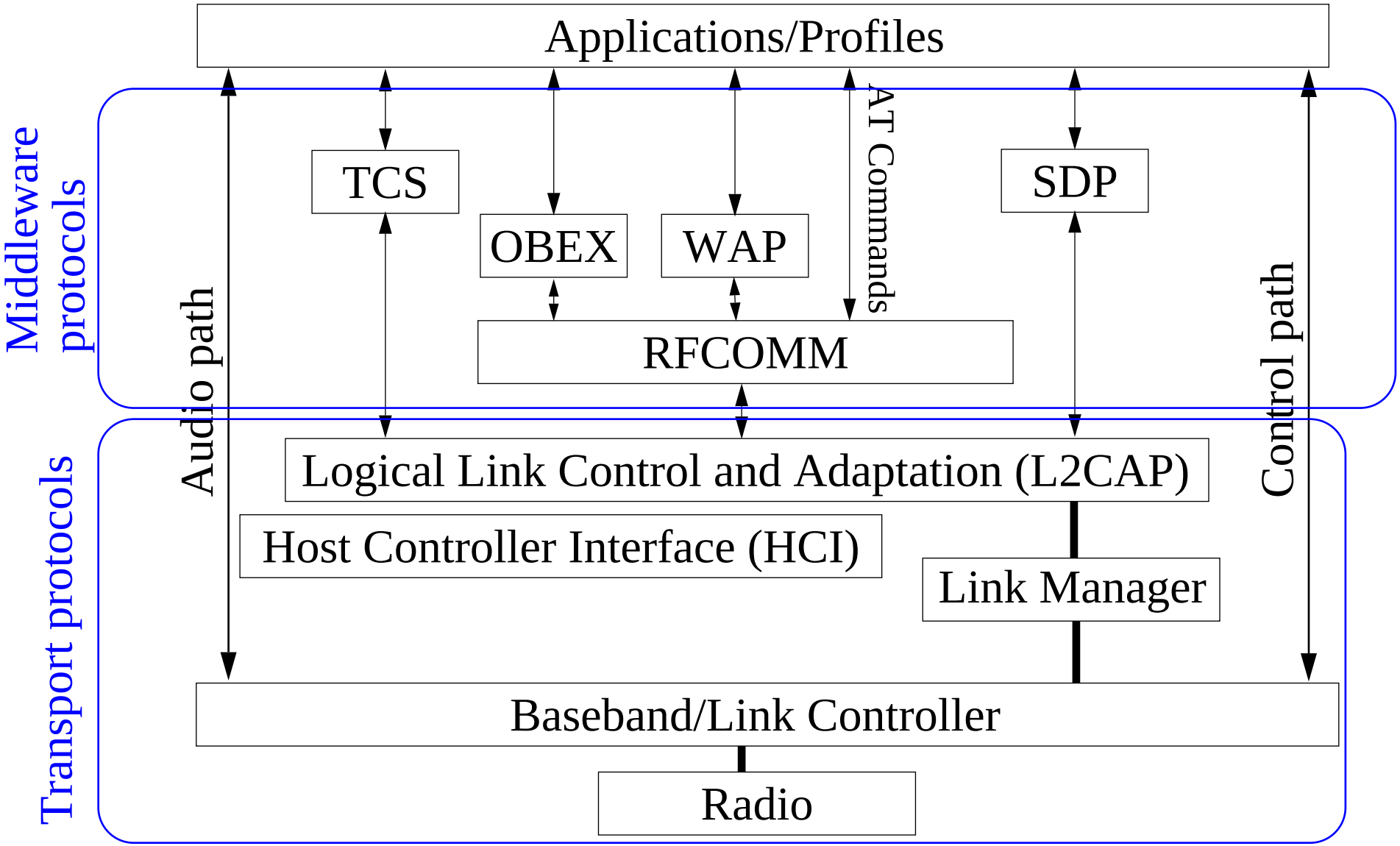
Goals

- low cost
- low power
- primarily a cable replacement (to connect mobile phones to headsets)
  - There are those who believe it can be used as a Wireless Personal Area Network (WPAN), hence it was the basis for IEEE 802.15.

Using:

- short-range radio technology
- ad hoc networking
- dynamic discovery of other Bluetooth devices & the services they offer

Bluetooth protocol stack



Physical Layer

- Uses 2.4 GHz unlicensed Industrial, Scientific, and Medical (ISM) band (globally portions of this band are available)
  - many other systems using the same spectrum
    - interference to other systems
    - interference from other systems
  - 2.400-2.4835 GHz, i.e., 83.5 MHz divided into 79 channels with carrier frequencies f = 2402 +k MHz, k = 0, … , 78; Channel spacing is 1 MHz
  - Gaussian Frequency Shift Keying (GFSK) modulation with one bit per symbol
  -
- uses fast (1600 hops/s) frequency hopping spread spectrum (FHSS)
  - 625 microsecond long time slots
  - one hop per packet, but a packet can be 1 slot, 3 slots, or 5 slots long

Transmit Power

- Low transmit power
- original goal was a 10m radius of operation, but some thought about using Bluetooth for longer ranges ⇒ Transmit Power Classes

Class	Max. output power	Range	Power control
1	100mW (20 dBm)	100m+	mandatory
2	2.5mW (4 dBm)	10m	optional
3	1mW (0 dBm)	1m	optional

- most manufacturers producing Class 3 radios
- power control is to reduce both interference and power consumption

Masters vs. Slaves

Each Bluetooth device is a Master or Slave:

- master initiates exchange of data and the slave responds to the master
- in order to communicate devices must use same sequence of frequency hops, hence slaves synchronize to hop sequence of master
- master assigns an **A**ctive **M**ember **add**ress (AM_ADDR) to the slaves participating in active communications within the piconet

Additional devices may be registered with the master and be invited to become active as necessary -- their state is called "**parked**"

Devices not currently associated with any piconet are in **stand-by mode**.

Frequency Hop Sequence

Each device has a 48 bit IEEE MAC address (called a Bluetooth device address (BD_ADDR)) and a local free-running 28-bit clock that ticks once every 312.5 µs (which corresponds to half the residence time in a frequency when the radio hops at the nominal rate of 1,600 hops/sec.)

Each slave receives master's address and clock, then uses this to calculate frequency hop sequence

Time Division Multiplexing (TDM)

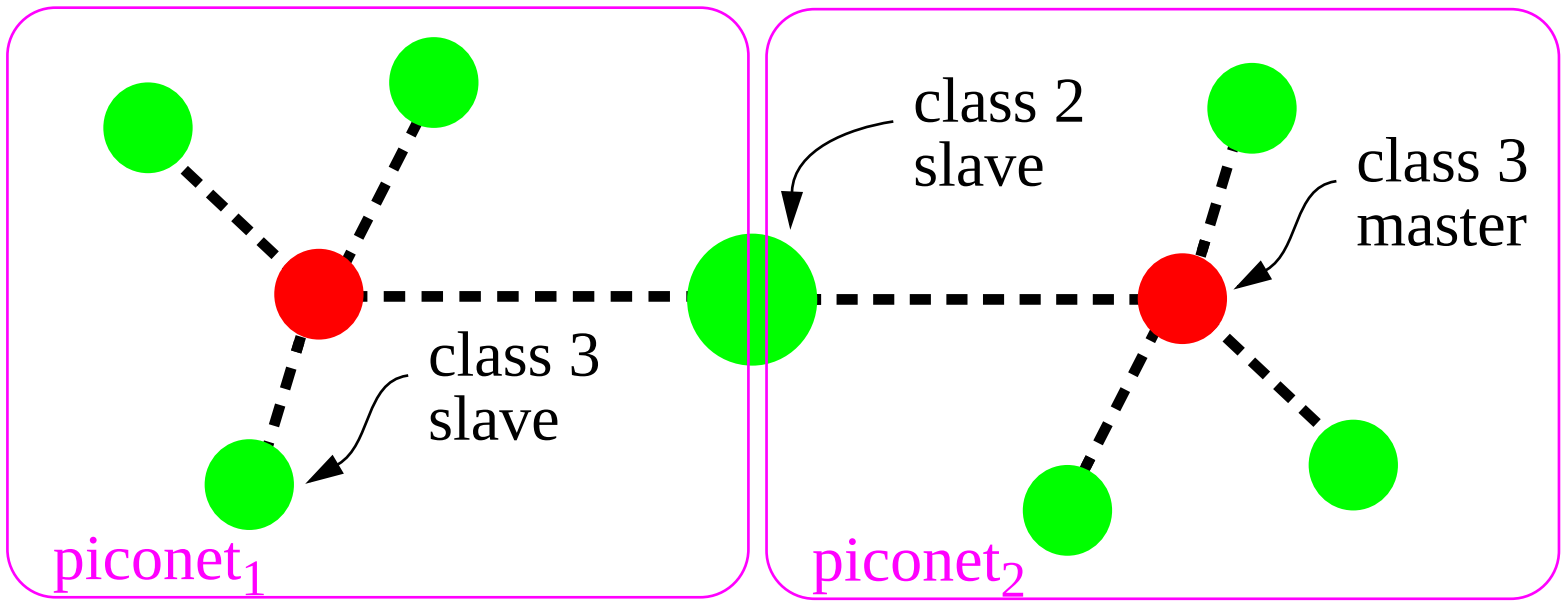
Divide the total bandwidth between Bluetooth devices using a given hop sequence

- Master assigns time slots to slaves
- packets are joined together in transmit and receive pairs; master and slaves alternate in time-division duplex (TDD)

Network Topology

Piconet	subnet of Bluetooth devices, synchronized to the timing and hopping sequence of a master • slaves only communicate with the master • maximum of 7 slaves in a piconet (as there are only 3 address bits!)
Scatternet	multiple Bluetooth piconets joined together by devices that are in more than one piconet • Routing of packets between piconets is not defined)

Scatternet



Scatternets

If a device is present in more than one piconet, it must time-share, spending a few slots in one piconet and a few slots in the other

A device may not be master of two different piconets since all slaves in a piconet are synchronized to the **master's** hop sequence, thus if the slaves were all synchronized with a single master -- they would be part of the **same** piconet!

This means that piconets making up a scatternet do **not** coordinate their frequency hopping ⇒ unsynchronized piconets in an area will randomly collide on the same frequency.

Voice + Data support

As an important application of Bluetooth was a cable replacement between handset and headset and this was developed in a telecom company's development lab ⇒ synchronous voice support was the focus of the link protocol design

- Synchronous Connection Oriented (SCO) links for voice
  - circuit-switched connections - 64 kbps in each direction per voice channel (using their own voice coding or) using reserved slots
  - up to three voice channels active at one time (may be to 1, 2, or 3 slaves)
  - ~78% overhead for data! (this is without FEC)
- Asynchronous Connectionless (ACL) links for data
  - ACL Data Packets: 72-bit access code, 54-bit header, 16-bit Cyclic Redundancy Checksum (CRC), and varying amount of data
  - with largest packet (Data High rate, DH5, packet stretching over five slots) ⇒ maximum data rate of ~650 kbps
  - a best effort delivery service - maintains integrity by using retransmissions and sequence members, as well as forward error correction (FEC) **if** necessary
  - a master can have an ACL link to each of several slaves, but only one per slave
  - Broadcast packets: packets that are not addressed to a specific Slave

Baseband

Baseband controls the radio and is responsible for low level timing, error control, and management of link during a single data packet transfer

Packet types:

- SCO, ACL - carrying payload
- ID packet consists of access code, used during re-connection
- NULL packet consists of access code and header, used for flow control or to pass ARQ
- POLL packet same structure as NULL packet, must be acknowledged
- FHS (Frequency Hop Synchronization)

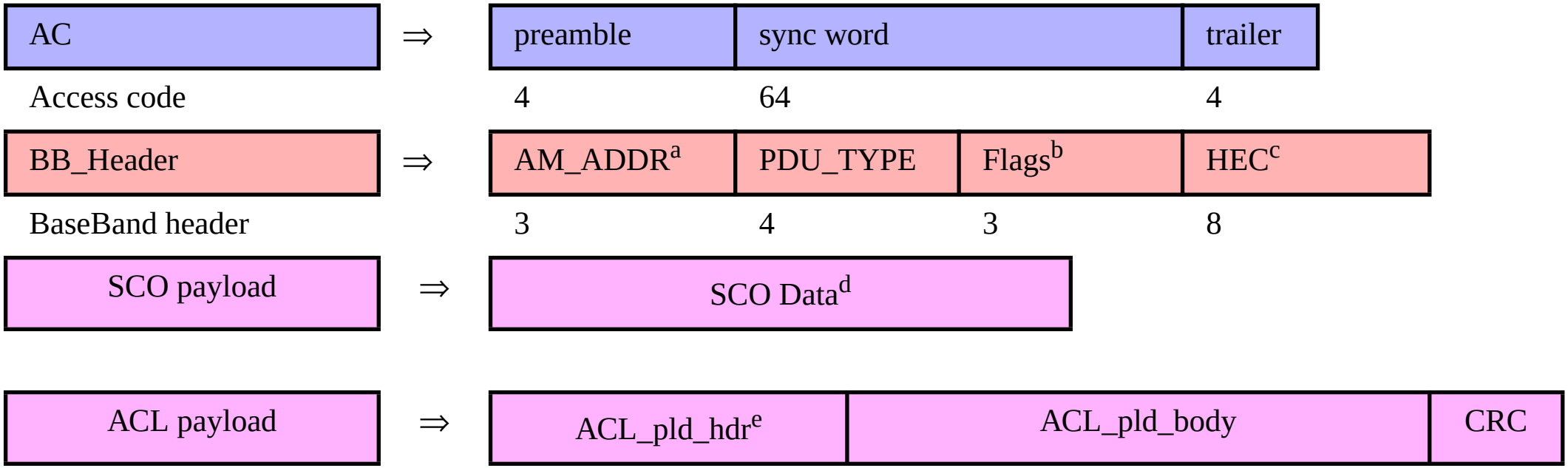
Baseband Packet formats

LSB				MSB
ID	AC			
(bit count)	68 or 72			
POLL/NULL	AC	BB_Header		
	68 or 72	54 (1/3 FEC)[a]		
FHS	AC	BB_Header	FHS payload	
	68 or 72	54 (1/3 FEC)	240 (2/3 FEC)	
ACL/SCO	AC	BB_Header	ACL or SCO payload	
	68 or 72	54 (1/3 FEC)	0-2744 ({1,2,3[b]}/3 FEC)	
DV	AC	BB_Header	SCO payload	ACL payload
	68 or 72	54 (1/3 FEC)	80	32-150 (2/3 FEC)

a. 54 bits includes the FEC bits (there are 18 bits of information with each bit repeated 3 times)

b. 3/3 FEC implies no FEC

Baseband Packet formats



a. Broadcast packet has address zero

b. Flow (=1 means receive buffer is full), ARQN (ACK represented by ARQN=1 and NAK by ARQN=0), SEQN (alternating bit)

c. Header error check (HEC)

d. 30 bytes (240 bits), error control code with rate 1/3, 2/3, or 1 (no FEC) used for source data size of 10, 20, or 30 bytes; note BB_Header flags for ARQN and SEQN are not used - since there is no flow control or retransmission, similarly the HEC is not used

e. L_CH (Logical CHannel) Field (3 bits) indicates whether payload is start or continuation of message, Flow field (1 bit) controls for data transfer at L2CAP level, Length field (8 bits) indicates the number of data bytes in the payload' header ends with 4 undefined bits

Synchronization Word Algorithm

1. Get 24-bit Lower Address Part (LAP) of Bluetooth device address (48 bit IEEE MAC address)
2. Append 6-bit Barker sequence to improve auto-correlation properties
3. XOR with bits 34 to 63 of full length, 64-bit Pseudorandom Noise (PN) sequence
4. Encode resulting 30-bit sequence with (64,30) BCH (Bose-Chaudhuri-Hocquenghem) block code to obtain 34 parity bits
5. 34-bit parity word XOR'd with the remaining bits, 0 to 33 of PN sequence to remove cyclic properties of block code

Note: 34 bits BCH parity word exhibits **very high auto-correlation** and **very low co-correlation** properties, therefore a correlator can be used to obtain a match between the received and expected (reference) synch word

Security

Some think that the high speed, pseudo-random frequency hopping algorithm makes it difficult to listen in on a connection - but of course this is false, because once you know the master's MAC address and clock you can calculate the next hop too!

Authentication and negotiation for link encrypting are both part of the Link Manager Protocol (LMP) specification.

- authentication is based on a challenge/response mechanism based on a common shared secret, a link key is generated through a user-provided PIN
- link level encryption using a public domain cipher algorithm SAFER+[1] generates 128-bit cipher keys from 128-bit plain text

1. J. L. Massey, On the Optimally of SAFER+ Diffusion, available at *http://csrc.nist.gov/encryption/aes/round1/conf2/papers/massey.pdf*

Link Control Protocol (LCP)

- configures and controls baseband
- packet level access control - determines what packet is going to be sent next
- high level operations: inquiry and paging
- configures and controls multiple links between devices and piconets
- does **not** require its own packets, but uses the (ARQN and SEQN) bits in baseband packets for SCO and ACL links to signal between link controllers - thus forming a logical LC (Link Control) channel

Link Control states

State	Description
Standby	inactive, radio not switched on
Inquiry	device tries to discover all Bluetooth enabled devices in the close vicinity; uses a special fast hopping sequence; FHS packets with device information, such as clock, frequency hop sequence, and BD ADDR, received from available devices; ⇒ a list of all available devices
Inquiry Scan	devices periodically enter the inquiry scan state to make themselves available to inquiring devices; a special slow hopping sequence used
Page	master enters page state and transmits paging messages to slave using access code and timing information which it learned earlier
Page Scan	device periodically enters page state to allow paging devices to establish connections
Connection-Active	Slave synchronizes to master's frequency hop and timing sequence. Master transmits a POLL packet to verify link, Slave sends NULL packet in reply
Connection-Hold	device ceases to support ACL traffic for a period of time, keeps Active Member address (AM_ADDR)
Connection-Sniff	device listens in pre-defined time slots only
Connection-Park	device listens for traffic only occasionally, gives up its AM address

Link Manager

Translates commands from **Host Controller Interface** (HCI) into operations at baseband level to implement the following operations:

- attaching Slaves to a piconet, and allocating active member addresses (AM addr)
- tearing down connections when slaves leave piconet
- configuring links, e.g., controlling Master/Slave switches
- establishing ACL and SCO links
- putting connections one of the low-power modes
- communicates with other LMs using the **Link Management Protocol** (LMP) which is a set of messages, or **Protocol Data Units** (PDUs), whose payloads contain the following fields:
  - single bit Transaction Identifier equal to 0 (1) for PDU sent from Master (Slave)
  - Operation Code (OpCode) defining type of message being sent
  - message parameters
  - PDUs sent as single slot packets on link management logical channel (L_CH =3)

Host Controller Interface (HCI)

- interface between a host and a Bluetooth module
- having a standard interface enables Baseband and Link Manager to run on a processor in the Bluetooth module while higher layers and applications running on host
- Bluetooth module can wake the host via a message across this interface

HCI Transport Layer

Three different transport interfaces are defined to transfer HCI packets from the host to the Bluetooth module:

USB	Universal Serial Bus
RS-232	serial interface with error correction
UART	Universal Asynchronous Receiver Transmitter, a serial interface without error correction

Logical Link Control and Adaptation Protocol (L2CAP)

L2CAP only transfers data and all applications **must** use L2CAP to send data.

provides:

- multiplexing to allow several higher layer links to pass across a single ACL connection
- segmentation and reassembly to allow transfer of packets larger than lower layers support
- Quality of Service (QoS) management for higher layer protocols

L2CAP Signalling

labels packets with channel numbers

L2CAP entities communicate with each other using control channels with a special channel number (used for connecting, configuring, and disconnecting L2CAP connections)

packet contains a length field (2 bytes), a channel identifier (2 bytes), and a data field (0 .. 65535 bytes)

L2CAP Command

OpCode	identifying contents of command
Identifier	used to pair up requests and responses
Length	of data field

More than one command can be sent within a L2CAP packet

Configuring a Connection

Parameters which can be configured are:

- Maximum Transmission Unit (MTU) < 65,535 bytes
- Flush timeout -- time (in milliseconds) a device will spend trying to transmit an L2CAP packet before it gives up
- QoS option can select best effort, or a guaranteed QoS

Disconnecting and Timeouts

Two ways for an L2CAP channel to be closed down:

- disconnection request from higher layer protocol or service
- time out: every time L2CAP sends a packet, a Response Timeout Expired (RTX) time is started; if the RTX timer expires before a response is received, the channel may be disconnected

For A to talk to B

Step 1: Discovering a Bluetooth device:

- device A transmits one or more inquiry packets[1]
- device B replies with Frequency Hop Synchronization (FHS) packet which contains device class information (including its BD_ADDR)

Step 2: Connecting to service discovery database:

- ACL baseband connection is established
- Logical Link Control and Adaption Protocol (L2CAP) connection is set up over ACL channel
- L2CAP adds Protocol and Service Multiplexor (PSM) to L2CAP packets to distinguish between different higher layer protocols and services (PSM=0x0001 for service discovery)
- Service Discovery Protocol (SDP) connection over L2CAP channel
- device A receives Dial-Up Networking (DUN) info from B's service discovery database
- device A disconnects

Step 3: Connecting to Bluetooth service:

- ACL link is set up
- device A utilizes Link Management Protocol (LMP) to configure link
- L2CAP connection using the RFCOMM protocol (RS-232 serial cable emulation) is set up (PSM=0x003)
- DUN connection is set up using RFCOMM connection

---

1. A piconet master may explicitly page devices to join its piconet; if it knows their BD_ADDR it can skip the inquiry process and directly paging the device

Service Discovery Protocol (SDP)

- only provides information about services, does not provide access to these services
- “optimized” for usage by devices with limited capabilities over wireless links
  - uses binary encoding of information
  - unique identifiers (UUIDs) describe services and attributes of these services such that you don’t need a central registration authority for registering services
  - generally UUIDs are 128 bits long; however, for known services 16-bit and 32-bit UUIDs may also be used.

RFCOMM Protocol

- provides a serial interface over the packet-based transport layers
- emulates the signals on the nine wires of an RS-232 cable
- based on the ETSI 07.10 standard (also used by GSM terminals), allows multiplexing (via L2CAP) several serial ports over a single transport
  - supports flow control on individual channels
  - has a reserved Protocol and Service Multiplexer (PSM) value used by L2CAP to identify RFCOMM traffic
- no error control
- enables legacy applications -- written to operate over serial cables -- to run without modification

RFCOMM Frame Types

Five frame types (the first 4 are control frames):

SABM	Start Asynchronous Balanced Mode (startup command)
UA	Unnumbered Acknowledgement (response when connected)
DISC	Disconnect (disconnect command)
DM	Disconnected Mode (response to a command when disconnected)
UIH	Unnumbered Information with Header check • each RFCOMM channel has a Data Link Connection Identifier (DLCI) • UIH frames with DLCI = 0 are used for control messages, while DLCI ≠ 0 are used data

Telephony Control Signaling (TCS) Protocol

TCS-AT	Telephony control can be performed using the AT command set use the RFCOMM to send and receive control signaling based on the AT command set (for example to implement a dialer application)
TCS-BIN	(BIN stands for the binary encoding of information), that runs directly on top of L2CAP; supports normal telephony control functions such as placing and terminating a call, sensing ringing tones, accepting incoming calls, etc. TCS-BIN supports point-to-multipoint communications as well, for example, a cordless base station can pass the ringing signal of an incoming call to several cordless headsets associated with the base station.

Bluetooth Profiles

- specifications for building interoperable applications
- All profiles depend on the Generic Access Profile (GAP) -- defines the basic rules and conditions for connecting devices with each other and establishing Bluetooth links and L2CAP channels.

Profile	Description
serial port profile	defines how RFCOMM runs on top of the Bluetooth transport protocols
generic object exchange profile	defines how objects can be exchanged using the OBEX protocol running on top of RFCOMM

add more profiles - such as LAN access

Management

- needed to manage links, but not defined by Bluetooth spec!
- could provide fault, accounting, configuration, performance, and security management
- link level encryption using a public domain cipher algorithm SAFER+ generates 128-bit cipher keys from 128-bit plain text

Low Power Modes

sniff mode	a slave agrees with its master to periodically listen for the master's transmissions; the period is configured through LMP transactions
hold mode	a device (in a piconet) agrees to remain silent (in that particular piconet) for a given amount of time; note: **keeps** its temporary address, AM_ADDR
park mode	a slave device agrees with its master to park until further notice; **relinquishes** its active member address, AM_ADDR, periodically listens to beacon transmissions from the master • device can either be invited back (by the master) to active communications using a broadcast transmission during a beacon or • if the slave wants to be unparked, it sends a message to the master in the slots following the beacon

Although the radio is often the biggest power drain on a Bluetooth device, the voltage controlled oscillator (for the Bluetooth clock) also consumer power and can be shut off -- instead you can use a less accurate lower power oscillator when the accuracy of the normal oscillator is not needed (for example when sleeping)

IEEE 802.15 standard

Bluetooth proposal chosen to serve as the baseline

- IEEE 802.15.1draft standard is in its final stages
- IEEE 802.15.2 task group studies coexistence issues between 802 wireless technologies
- IEEE 802.15.3 task group developing standards for high-rate radios (>20 Mbps)
- IEEE 802.15.4 task group developing standards for low-rate radios (<200 kbps)

Further reading

The lecture notes are based on material from:

[89] “Bluetooth: Part 1: Overview”, Kjell Jørgen Hole <Kjell.Hole@ii.uib.no>, NTNU, UiB, *http://kjhole.com/Bluetooth/Downloads.html*

which is in turn based on Ch. 1, 2, and 3 of:

[90] Bluetooth 1.1: Connect Without Cables by Jennifer Bray and Charles F. Sturman

[91] C. Bisdikian, “An overview of the Bluetooth Wireless Technology”, IEEE Communications Magazine, pp. 86-94, Dec. 2001.

[92] Bluetooth specification, *http://www.bluetooth.com*

KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

8. WLAN

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Last modified: 2003.03.13:11:57

Lecture 9 &10

- Wireless Local Area Networks (WLANs)

IEEE 802.11 Medium Access Control (MAC) protocol uses Carrier sense multiple access (CSMA) with collision avoidance (CA) medium access scheme.

Several variants:

IEEE 802.11b	1, 2, 5.5 and 11 Mbps - DS-SS Wireless Ethernet Compatibility Alliance certifies its members' equipment as conforming to the 802.11b standard. Compliant hardware is stamped **Wi-Fi (Wireless Fidelity)** compatible; operates in 2.4GHz band
IEEE 802.11g	enable data transmission speeds of up to 54 Mbps, with backwards compatibility to 802.11b infrastructure; operates in 2.4GHz band
IEEE 802.11a	using OFDM (Orthogonal Frequency Division Multiplexing) achieves upto 54 Mbps - currently **not** approved for use in Sweden; operates in 5 GHz band
IEEE 802.11h	designed to adapt 802.11a to the european HiperLAN/2 requirements; operates in 5 GHz band

Two possible network configurations

Independent configuration	Mobile stations communicate directly to each other with no access point (base station) support, i.e., peer-to-peer (**ad hoc**) networking
Infrastructure configuration	Mobile stations communicate only via access points (APs)

Terms

Basic Service Set (BSS) - a group of stations that are under the direct control of a single coordination function (PCF or DCF)

Independent BSS (IBSS) - also known as an ad hoc network, defined as a BSS which exist without an access point (AP)

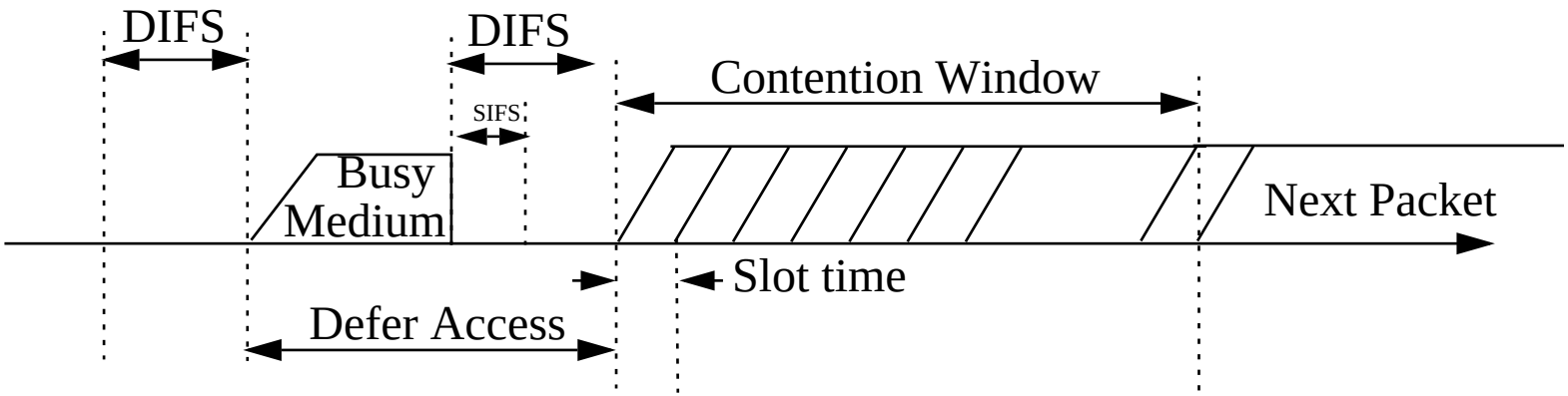
Infrastructure network - a network of wireless stations along with APs, which enables stations in one BSS to communicate with stations in another BSS

Distribution System (DS) - a backbone network between the two or more access points

Extended Service Set (ESS) a series of overlapping BSSs (each with its own AP) connected together by means of a Distribution System (DS)

Hidden node - a node is said to be hidden when its transmissions cannot be heard by some other node in the network (although it can be heard be one or more other nodes)

IEEE 802.11 Basic Access Method



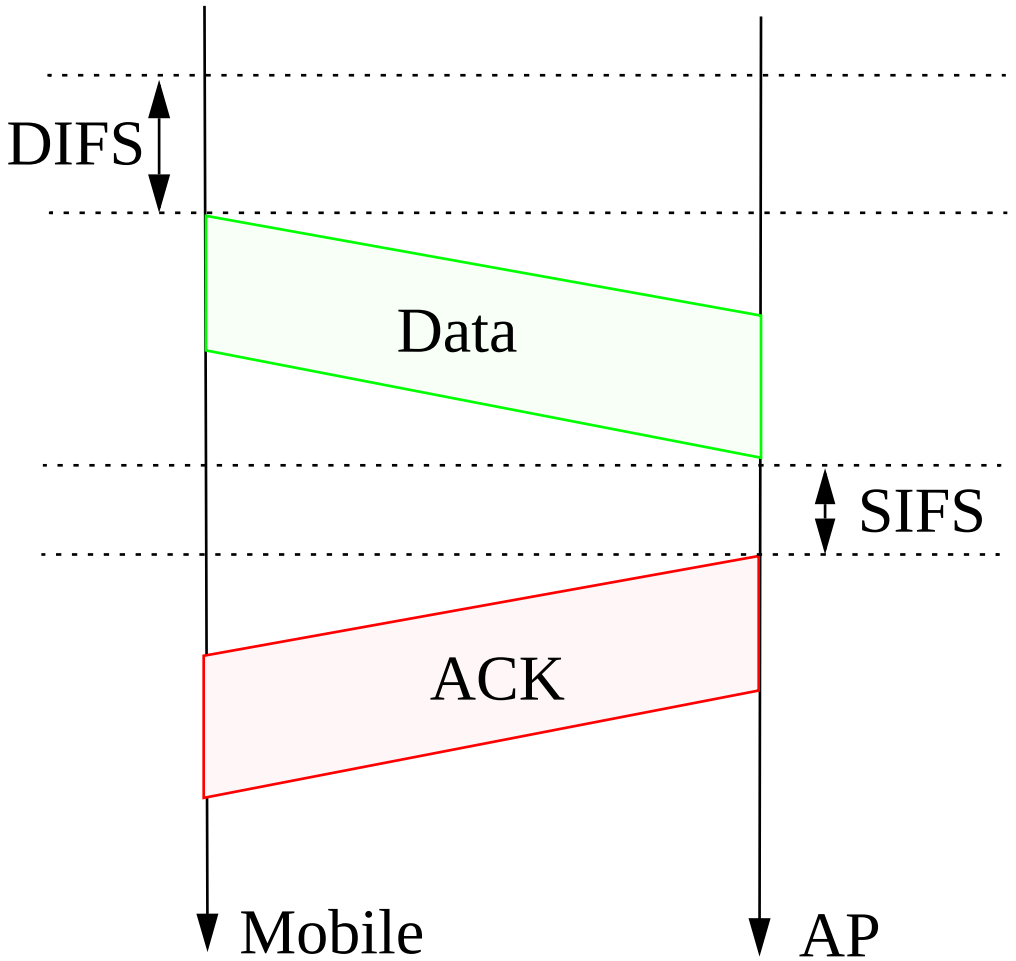
IFS	Inter Frame spacing - during this time the medium is idle
SIFS	Short IFS - transmission after SIFS is reserved for ACKs, Clear To Send frame, or to send a fragmented MAC protocol data unit (MPDU)
DIFS	if after DCF-IFS (DIFS) a station finds the media free it can transmit a pending packet; otherwise it sets a backoff timer after selecting a random backoff value (BV) {selected from a uniform distribution over [0 .. CW-1], where CW is the width of the contention window in slots} if medium become busy before time goes off, then the value is frozen until the next DIFS interval, where upon it continues the count down CW is doubled after collisions and reset to CW_{min} after a successful transmission
EIFS	Extended IFS - used when the receiver can't correct the received packet

Distribution Coordinating Function (DCF)

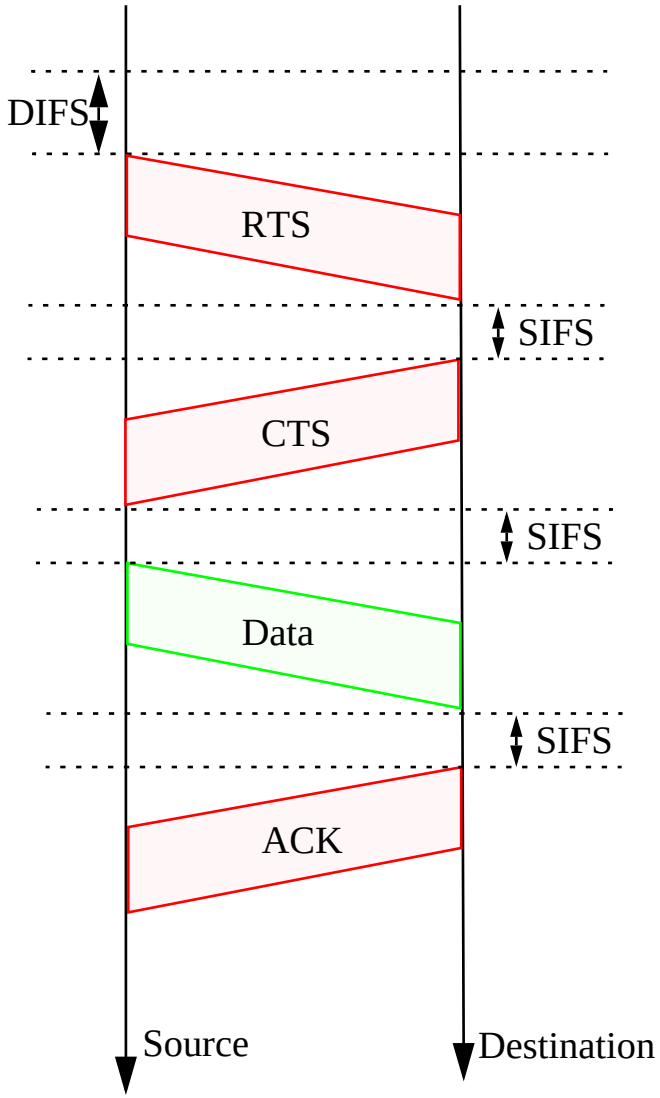
Distribution Coordinating Function (DCF) is based on carrier sense multiple access with collision avoidance (CSMA/CA)

Receivers send an ACK if they successfully receive a packet, otherwise the transmitter re-sends.

CSMA/CA with ACK in infrastructure network



IEEE 802.11 RTS/CTS mechanism



IEEE 802.11 Frame Format

Frame Control	2 bytes
Duration/ID	2 bytes
Address 1	6 bytes
Address 2	6 bytes
Address 3	6 bytes
Sequence Control	2 bytes
Address 4	6 bytes
Frame Body	0 .. 2312 bytes
CRC	4 bytes

IEEE 802.11 Frame Control

B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version		Type		Subtype				To DS	From DS	More Frag	Retry	PwrMgt	More data	WEP	RSVD
2		2		4				1	1	1	1	1	1	1	1

Protocol Version	currently 00, other values reserved
To DS/From DS	1 for communication between two APs
More Fragments	1 if another fragment follows
Retry	1 if packet is a retransmission
Power Management	1 if station is in sleep mode
More date	1 if there are more packets to the terminal in power-save mode
WEP	1 if data bits are encrypted

Startup, then Join a network

- Turn on & discovery phase
  - determine AP or other stations exist
  - get SSID and other parameters
- Negotiate for connection
  - Authentication & Association

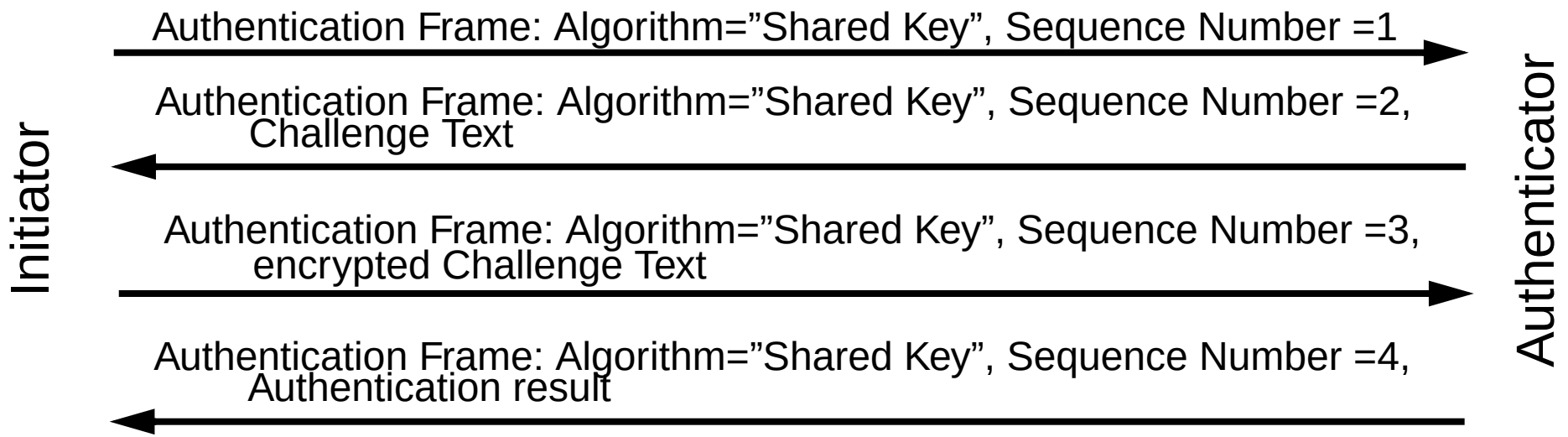
Discovery Phase

Enter scanning mode: Passive / Active scanning mode

- Passive
  - Listen for a Beacon for ChannelTime period
  - From Beacon get the SSID & parameters
- Active
  - Transmit a probe frame (including the SSID that you wish to join)
  - Wait for a period for responds by AP or other stations

Authentication

- Open system authentication
  - **Default** mode
  - Flow:
    - send: Authentication Frame: Algorithm=”Open”, Sequence Number =1
    - response: Authentication Frame: Algorithm=”Open”, Sequence Number =2, result=accept/reject
- Shared key authentication
  - Somewhat higher degree of security
  - Need to implement WEP
  - Flow:



Wire Equivalent Privacy (WEP)

IEEE 802.11 featured **Wire Equivalent Privacy (WEP)** - this proved to be rather insecure; there are efforts to fix it - but meanwhile or in any case one can use VPNs.

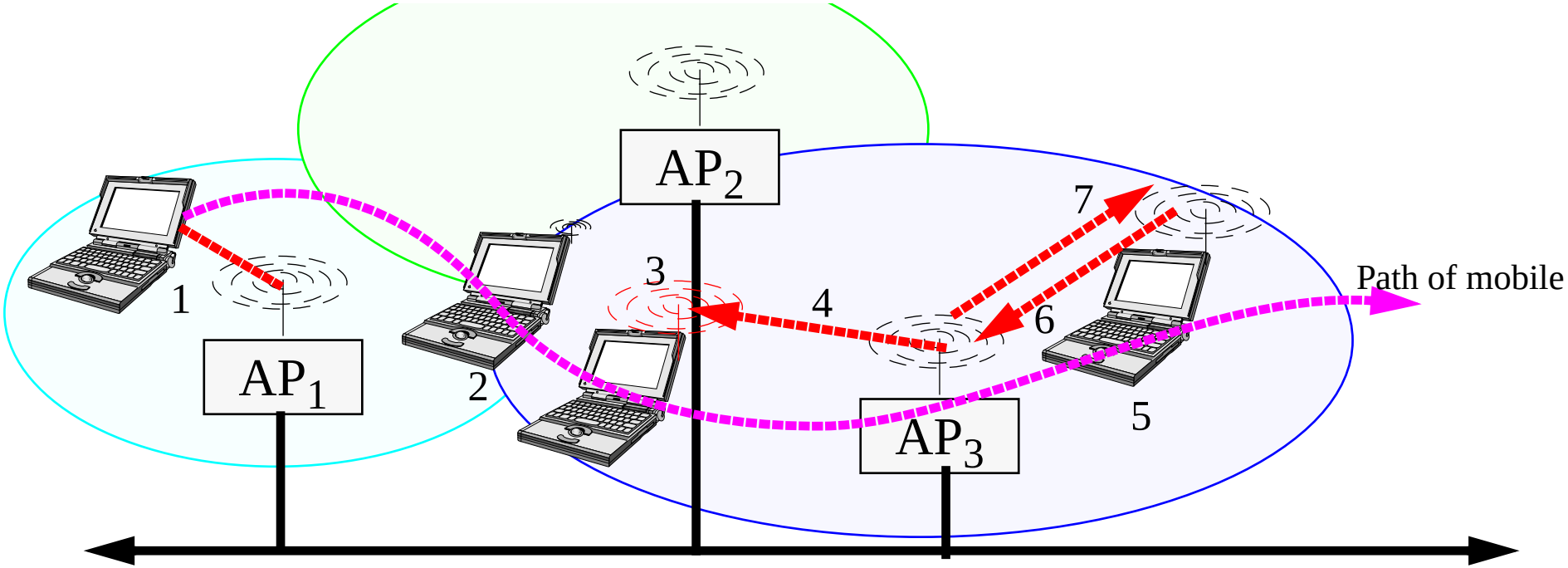
WEP use for data encryption & shared key authentication

- Encryption of data through RSA RC4 algorithm
- 40-bit secret key + 24-bits Initialization Vector (IV)
- IV in frame in clear text
- Integrity Check Value (ICV) included in frame
- When WEP is enabled, Shared Key Authentication is enabled

Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”, AT&T Labs Technical Report TD-4ZCPZZ, Revision 2, August 21, 2001
http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

see also *http://www.cs.umd.edu/~waa/wireless.html*

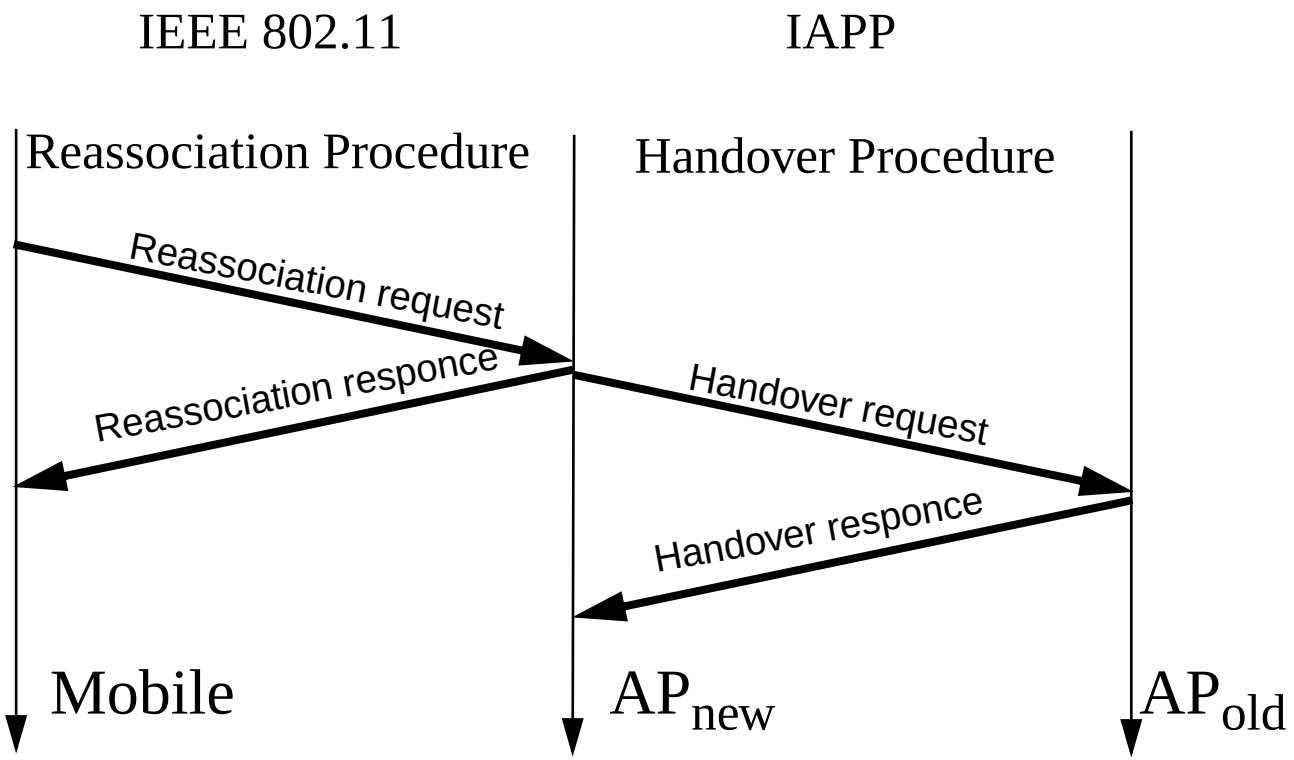
Handoff



1. Mobile starts with a strong signal from AP_1
2. The signal from AP_1 is now weaker, so mobile starts to look around for a better AP
3. Mobile sends a Probe Request
4. AP_3 send probe response
5. Mobile chooses AP_3 as the best AP
6. Mobile sends Reassociation request
7. AP3 sends a Reassociation Response

Inter-Access Point Protocol (IAPP)

Project 802.11f: IAPP Inter Access Point Protocol



Fast Handoff

- 802.11 being used in PDAs, WLAN phones, lots of new devices (especially for multimedia)
  - Multimedia applications sensitive to connectivity loss (when the loss of data exceeds that which the playout buffers can cover up)
  - TCP sensitive to multiple losses
    - Loss of an entire window causes connection to go into slow-start
- basic handoff is fast and simple, but insecure
  - Authentication occurs prior to reassociation so pre-authentication is possible
  - Management frames are not authenticated, thus no cryptographic operations in critical path
  - If APs involved in the handover use the same WEP key, no inter-AP communication is required
- Unfortunately 802.1x complicates 802.11 handoff
  - now STAs have dynamic per-session keys
  - authentication occurs **after** reassociation, not before
  - If re-authentication is required, then STAs need to complete authentication before recovering connectivity
  - Authentication and key management methods requiring public key operations (e.g. EAP-TLS) -- this can take several seconds to complete
  - Using a TLS continuation can decrease the number of round-trips (from 3.5 to 2.5)
  - if authentication server is far away, then disconnection time can be large

for further information see [100]

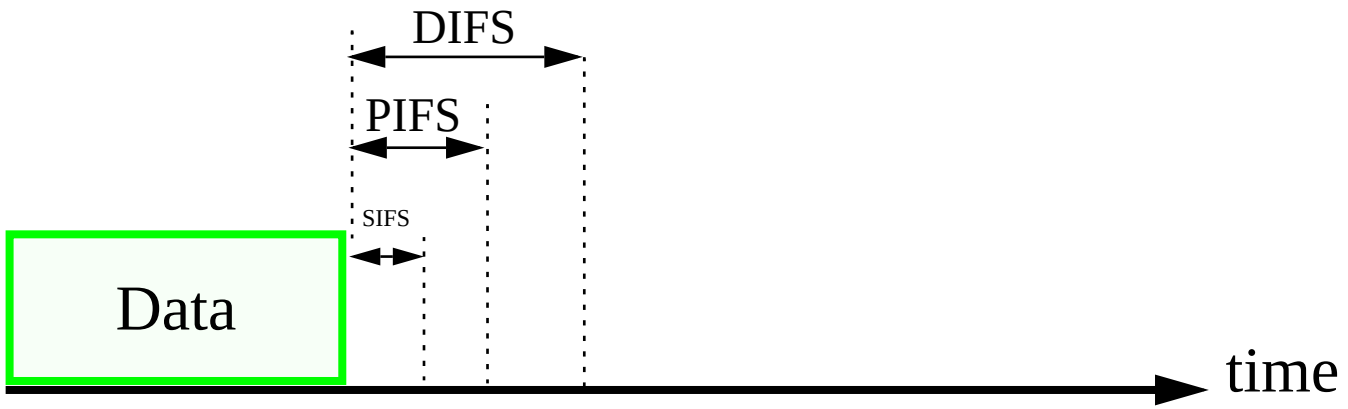
Point Coordination Function (PCF)

Point Coordination Function (PCF) an optional extension to DCF that provides a time division duplexing capability to accommodate time bounded, connection-oriented services.

AP polls each station:

- enabling the polled station to transmit without contending for the medium
- Contention free period repetition interval (consisting of contention free period (CFP) and contention period (CP) is initiated by the AP through a Beacon frame.
  - If AP finds the medium idle, it waits for a PCF inter frame spacing (PIFS) period of time and then transmits a beacon frame with a polling frame following SIFS seconds after it
  - when a station receives the poll from the AP, the medium is reserved for the duration of its transfer (upto the length of CFP), when the data transfer complete (or the reserved time is up), the AP waits for PIFS seconds and polls another station - it continues until the CP interval is up - then the system operates in DCF mode.
- note: AP can transmit data along with the polling frame

Spacing



Timing and Power Management

Synchronization (to within 4 µs plus propagation delay) of all clocks within a BSS maintained by periodic transmission of beacons containing time stamp info. AP (in infrastructure mode) is the timing master and generates all timing beacons.

Power saving modes:

awake — STAs (aka mobiles) are fully powered and can receive packets at **any** time.

doze

- unable to transmit or receive data, but uses little power
- STA must inform the AP it is entering the doze mode, then AP does not sent packets simply buffers them
- Unicast:
  - When AP has packets queued for STAs in doze state, a traffic indication map (TIM) is broadcast as part of the timing beacon
  - STAs in the doze mode power up receivers to listen for beacons, if identified by the TIM, they return to awake mode and transmit a PS-Poll message so the AP knows that they are ready to receive data
- Broadcast/multicast:
  - buffered broadcast/multicast packets queued in the AP are indicated in a delivery traffic indication message (DTIM) that is broadcast periodically to awaken all STAs and alert them to a forthcoming broadcast/multicast message; the message is then sent **without** the AP **waiting** for PS-Poll messages.

AAA

IEEE 802.1x -port-based network access control for authentication, authorization, and security[99]

See also Juan Caballero Bayerri and Daniel Malmkvist, “Experimental Study of a Network Access Server for a public WLAN access network”, M.S. Thesis, KTH/IMIT, Jan. 2002 [98].

IEEE Extensible Authentication Protocol

An authentication protocol which supports multiple authentication mechanisms, runs directly over the link layer without requiring IP and therefore includes its own support for in-order delivery and re-transmission. Originally developed for use with PPP: Larry J. Blunk and John R. Vollbrecht, “PPP Extensible Authentication Protocol (EAP) standard”, RFC 2284

Roaming

Roaming is dependent on the underlying networks providing you service and if they are to charge -- knowing who to charge and how much to charge.

Unlike macrocellular systems where you generally only face roaming when making large scale movements (between countries or major regions of a country), in WLAN systems the intersystem movement may occur with little of no movement!

Clearinghouse

Clearinghouse to perform settlements between the various operators, see for example Excilan (*http://www.excilan.com*).

Interconnect Provider

Sören Nyckelgård, Telia's Golden Gate and its Interconnect Provider Role, Telia Golden Gate - Technical Overview, available January 23, 2002 at

http://www.telia.se/filer/cmc_upload/0/000/030/185/ResearchGoldenGateTec1Overv2.doc

and

Martin Altinkaya and Saman Ahmedi, “SIP in an Interconnector and Service Provider Role”, M.S. Thesis, KTH/IMIT, Dec. 2001.

Since IEEE 802.11 specifies only upto the interface to the 802.2 link layer all mobility management is outside the scope of the standard.

Proxies

Numerous proxy based proposals exist to “improve” performance across wireless links - especially targeted to TCP (most have problems keeping TCP/IP’s **end-to-end** semantics)

See:

Luis Muñoz, Marta Garcia, Johnny Choque, Ramón Agüero, and Petri Mähönen, “Optimizing Internet Flows over IEEE 802.11b Wireless Local Area Networks: A Performance-Enhancing Proxy Based on Forward Error Control”, IEEE Communications Magazine, December 2001, pp. 60-67.

HiperLAN2

Developed by the European Telecommunications Standard Institute (ETSI)
Broadband Radio Access Networks (BRAN)

- Dedicated spectrum (in Europe) at 5 GHz
- uses Orthogonal Frequency Division Multiplexing (OFDM) with 52 subchannels, 48 subchannels for data, and 4 subchannels for pilot symbols
- TDMA/TDD frames with fixed duration of 2ms
- Maximum gross data rate of 54 Mb/s
- MAC protocol was designed to support multimedia services

For more information see HiperLAN2 Global Forum *http://www.hiperlan2.com/*

and ETSI standards documents at:

http://www.etsi.org/frameset/home.htm?/technicalactiv/Hiperlan/hiperlan2.htm

802.11a and 802.11h

IEEE 802.11a and ETSI's HiperLAN2 standards have nearly identical physical layers, but are very different at the MAC level

IEEE 802.11h adds **Transmit Power Control (TPC)** to limit a device from emitting more radio signal than needed, and **Dynamic Frequency Selection (DFS)**, which lets the device listen to what is happening in the airspace before picking a channel

- TPC and DFS were introduced to satisfy European requirements
- 802.11h is to be sold under the name Wi-Fi5 (to build on the Wi-Fi branding)

Multihop

MeshNetworks Inc. (*www.meshnetworks.com*) MeshLAN Multi-Hopping software:

- designed for use with Wi-Fi hardware
- extending useful range by adding multi-hopping peer-to-peer capabilities to off-the-shelf 802.11 cards

QDMA (quad-division multiple access)

MeshNetworks' proprietary radio technology developed (by ITT Industries (www.itt.com)) for and currently used by the military.

- IP from end to end
- supports high-speed mobile broadband access
- infrastructure-free, i.e., ad hoc peer-to-peer networking

Claims they can deliver up to 6 Mbps to each user in a QDMA wireless network.

Products have built-in GPS (Global Positioning System) capabilities and QoS for IP voice and video.

First implemented in 2.4GHz as prototype routers, relays, and PDA-size client devices; now developing equipment for MMDS (2.5GHz) licensed operators.

They have FCC experimental license to build a (US) nationwide 4,000-node test network.

All IP networks

Numerous efforts have shifted from simply using IP (rather than ATM) in the backbone and have been moving to an all IP network (i.e., IP directly to/from MS and in the infrastructure).

- Airvana Inc. (www.airvananet.com): all-IP architecture for radio access network equipment for 3G using CDMA2000 1x Evolution-Data Only (1xEV-DO) wireless technology, data rates up to 2.4 Megabits per second (Mbps) under ideal circumstances, with average sustained rates expected to be 300 to 600 kbps

Some view "4G" as the Fourth Generation **IP-based** wireless network.

Eliminates SS7 (Signaling System 7) telecommunications protocol

Flarion *http://www.flarion.com/* RadioRouter™ base stations used to build all-IP network

…

Space Data Corporation

Space Data Corporation *http://www.spacedata.net/* to provide low data rate wireless (messaging and later voice) service to rural and suburban US (about 90% of the land mass, but only 20% of the population); Piggyback their repeaters on US National Weather Service biodegradable latex weather balloons “SkySites”.

Each balloon goes up to about 100,000 feet ~ 30km and stays there for ~1.5 days; balloons are launched from 70 sites twice each day; the repeater has power for 16 hours (12 for operation and the rest as a reserve). They expect to use 50,000 balloons per year, each repeater costs US$300

Their business model does not depend on any recovery of balloons (although they are adding GPS to theirs)

- US National Weather Service gets 18% of their back - they put a mailing address and promise to pay the postage on their payloads
- lots of knowledge of winds from 60 years of weather balloons

Space Data has a license for 1.4 MHz of bandwidth nationwide (license US$4.2M)

Wireless Internet Service Providers (WISPs)

- **Location specific** WISP - exploiting high value sites (airports, hotels, coffee shops, …)
  - example: Surf ‘n Sip, MobileStar, and Wirelessbolaget
  - Advantages: often have “exclusive” offering
  - Disadvantages: users may also want access in other locations -- hence roaming agreements will be important
- **Single site** or **campus** WISP - a subset of the location specific WISP category (e.g., university or corporate campus, a single conference center/exhibition hall)
  - example: KTH and SU’s IT-University campus, CMU’s campus, …
  - Advantages: they know the site very well, generally they have “exclusive” offering, users are trapped - so they will have to pay and pay and pay or it is part of the tele/datacom offering
  - Disadvantages: for some sites the users are only there for a short period (hours to days), very high turn over in users (so low administrative costs are very important); in university and corporate campus settings very high demands/expectations

- **Mobile carrier** WISP - mobile (WWAN) operator also offering WLAN
  - examples: Telia HomeRun (Sweden), Sonera wGate (Finland), and VoiceStream (Germany / US) {due to their acquisition of MobileStar in the US - what happens if they bring this technology back to Europe?}
  - Advantages: they know where their users spend time (from their existing traffic and location data) so they can easily build out hotspots; retain customers with whom they already have a billing relationship
  - Disadvantages: offering WLAN might reduce their income (as they might have been able to charge (a lot) for the traffic via the WWAN in these same spots)
- **ISP WISP** - existing ISP that extends their network via WLAN access points
  - example: Sweden's PowerNet
  - Advantages: pretty straight forward extension of their existing network, by shipping dual xDSL/cable/… + AP devices[1]; retain customers with whom they already have a billing relationship
  - Disadvantages: offering WLAN might reduce their income since neighbors can share rather than installing their own service
- **WISP** - a pure wireless internet service provider
  - example: Sweden: Wirelessbolaget, DefaultCity, U.S.: Wayport
  - Advantages: this is their business
  - Disadvantages: this is their business but they depend on an ISP for back haul

1. Actiontec Electronics

- **Operator Neutral** WISP - an Internet eXchange (IX) to which several independent ISPs (or WISPs) are connected
  - example: StockholmOpen.net
  - Advantages: enable multiple operators
  - Disadvantages:
- **Franchising** WISP -
  - example:
  - Advantages: they simply sell the idea, starter kit, supply backup support, …
  - Disadvantages: dependant on getting a cut from the franchise
- **Virtual** WISP - no actual network, … - but rather they simply rent/buy capacity for their users; thus their major role is to support and bill users
  - example: Boingo
  - Advantages: very low to near zero costs for infrastructure
  - Disadvantages: they must provide either high service level and/or low prices to retain their customers
- **Community/Grassroots** WISP - altruistic providers
  - example: NYC Wireless
  - Advantages: people making their WLAN available to others “because it is the right thing to do”
  - Disadvantages: Support way or many not exist

Herslow, Navarro, and Scholander classify the WISPs based on whether they are “for fee” or for “free” and coverage area: hotspot vs. wide area.

MIT's AI Lab: Project Oxygen

> ‘‘Enabling people "to do more by doing less," that is, to accomplish more with less work.
>
> Bringing abundant computation and communication, as pervasive and free as air, naturally into people's lives.’’
>
> -- *http://oxygen.lcs.mit.edu/*

Utilizing self-configuring network with devices embedded in desks, walls, homes, … to create intelligent spaces

Handheld devices to support speech interfaces and reconfiguration for various protocols.

This is one of several projects trying to exploit ubiquitous/pervasive computing and communication.

Intelligent/Smart Spaces

Knowing what is around you is very useful for configuring devices and offering services, there are several proposals for how to do this:

- SUN's Jini
- Microsoft's Universal Plug-and-Play

For further information see Theo Kanter's dissertation "Adaptive Personal Mobile Communication -- Service Architecture and Protocols":
http://ps.verkstad.net/Thesis/Final/theoDissertation.pdf

and also his defense slides:
http://ps.verkstad.net/Thesis/Defense/theoDefense.pdf

Further reading

WISPs

[93] Louise Herslow, Carl-Johan Navarro, and Joakim Scholander, “Exploring the WISP Industry - Analysing Strategies for Wireless Internet Service Providers”, Masters thesis, Institute of Economic Research, Lund University, Sweden, January 2002.

http://www.scholander.com

[94] David Alvén and Reza Farhang, “Does it take a WISP to manage a wisp of hotspots? - Analysis of the WLAN market from a WISP perspective”, Masters Thesis, Department of Microelectronics and Information Technology, Royal Institute of Technology, Sweden, February 2002.
http://www.e.kth.se/~e96_rfh/wisp_analysis.pdf

IEEE 802.11

[95] *http://standards.ieee.org/getieee802/*

[96] *http://www.80211-planet.com/*

[97] Rusty O. Baldwin, Nathaniel J. Davis IV, Scott F. Midkiff, and Richard A. Raines, “Packetized Voice Transmission using RT-MAC, a Wireless Real-time Medium Access Control Protocol, Mobile Computing and Communications Review, V. 5, N. 3, July 2001, pp. 11-25.

AAA

[98] Juan Caballero Bayerri and Daniel Malmkvist, *Experimental Study of a Network Access Server for a public WLAN access network*, M.S. Thesis, KTH/IMIT, Jan. 2002.
http://www.e.kth.se/~e97_dma/FinalReport.pdf

[99] IEEE 802.1x Port Based Network Access Control
http://www.ieee802.org/1/pages/802.1x.html

[100]Tim Moore and Bernard Aboba “Authenticated Fast Handoff”, IEEE 802.11 Task group i, November 2001, doc. IEEE 802.11 submission
http://www.drizzle.com/~aboba/IEEE/11-01-TBD-I-Authenticated-FastHandoff.ppt