KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

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: 2002.03.14:11:54

Welcome to the course!

The course should be fun.

We will dig deeper into Personal Communication System - 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.it.kth.se/edu/gru/NetArch

Staff Associated with the Course

Instructor (Kursansvarig)

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

Assistants for Recitation Sessions (Övningar)

Dr. Johan Montelius <jm@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 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 emhasis will be primarily focus on the range from LEO sattelites down to personal area networks.

The course consists of 10 hours of lectures, xx hours of recitations (övningar), and a project of ~50 hours effort.

Topics

- Personal Communication Systems (PCS): handoff, mobility, paging
- CDPD
- GSM, GPRS, SMS, International Roaming, Operation/Administration/Maintainence
- 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 one of the instructors **before** starting.

Assignment Registration and Report

- Registration: 5 April 2002, 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 **xx June 2002 + oral presentations scheduled xx June 2002**

- Send email with URL link to <maguire@it.kth.se>
- Late assignments will not be accepted

Note that it is pemissible 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), many students may want to do project which involve mobile, in this regard the following two books are useful sources:

- *Mobile IP: Design Principles and Practices* by Charles E. Perkins, Addison-Wesley, 1998, ISDN 0-201-63469-4.
- *Mobile IP: the Internet Unplugged* by James D. Solomon, Prentice Hall, 1998, ISBN 0-13-856246-6.

We will refer to other books, articles, and RFCs as necessary. A list of interesting literature will be available on the course web page.

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
  - 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/Maintainence (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 in number of users and in variety of systems. Some of these system (such as GSM) have 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.

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.

(Chapters 1-4, and 22)

Internet Architecture

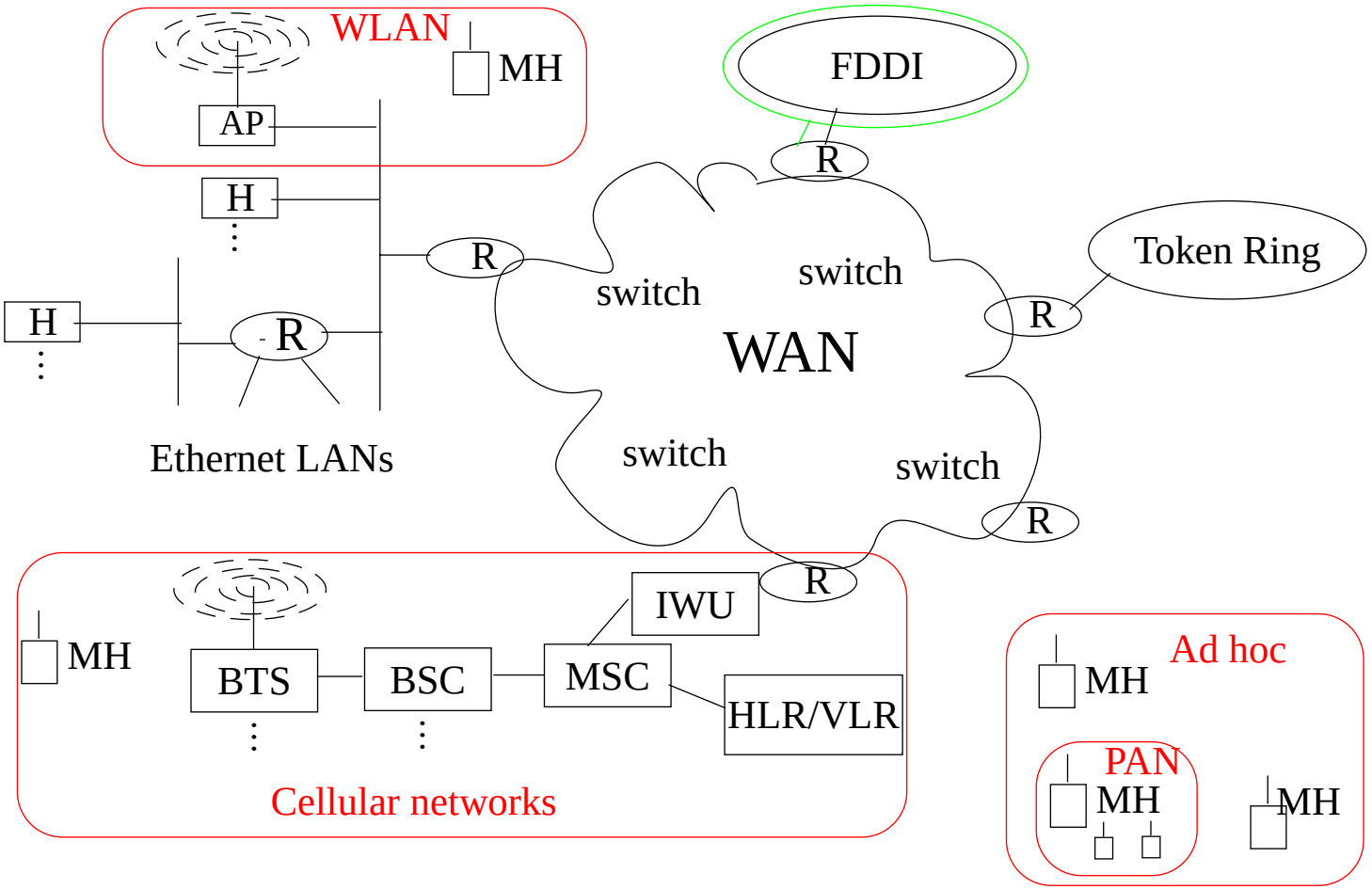


Figure 1: Multiple network technologies - internetworked together

More complete Architecture

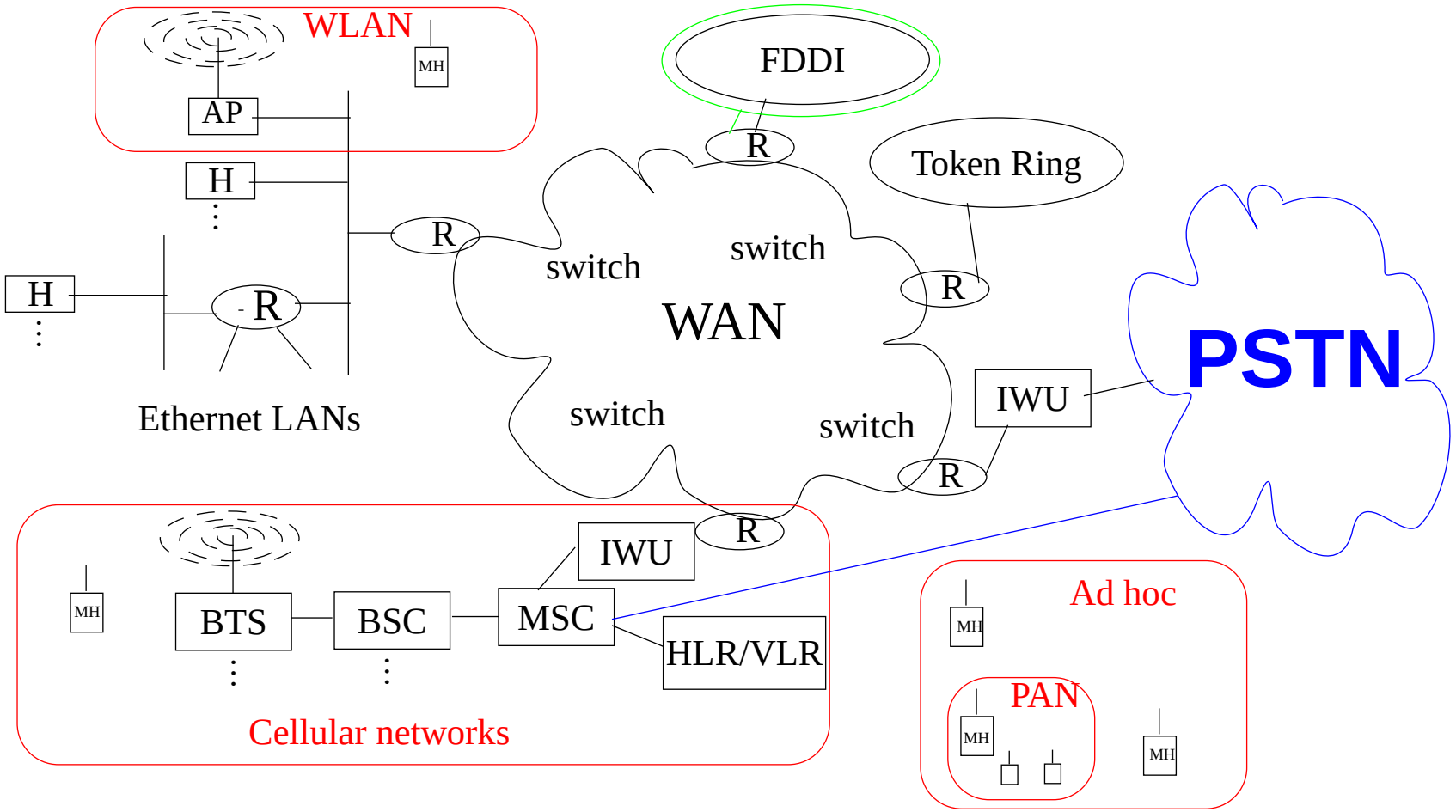


Figure 2: Internet and PSTN

- 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 is generally an adaptation to 64 kbps voice coding (for the course services). Increasingly these systems are also interconnected to the the Internet. 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 fall attempts at providing univeral 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 in-building and on campus), and homes (often equated with “personal or free-time usage”). However, we have seen that his market separation is increasingly converging rather than further diverging.

Traditionally, various PCS systems were connected to the Public Switched Telephony System (PSTN) and drived 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

- Frequency Division Multiple Access (FDMA)
  - Advanced Mobile Phone Service (AMPS)
- Time Division Multiple Access (TDMA)
  - D-AMPS, Global System for Mobile Communications (GSM)
- Code Division Multiple Access (CDMA)
  - IS-95 (developed by Qualcomm)

Low Tier Cellular and Cordless Telephony

Cordless Telephony, second generation (CT2) - 40 FDMA channles, in each the basestation to user and user to base station operate using time division duplexing (TDD).

Does not support handoffs, primarily supports out-going calls (incoming calls ate hard as there is no defined mobility database).

Digital Enhance Cordless Telephony (formerly Digital European Cordless Telephony) (DECT) - utilizes a picocellular design using TDMA with 24 time slots (generally 12 voice down and 12 voice up, i.e., TDD) per one 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.

Personal Handy Phone System (PHS) - another TDMA TDD system also supporting dynamic channel allocation - it has been used in Japan to for a public

low tier cellular system.

Personal Access Communications System (PACS) - a TDMA system supporting both TDD and frequency division duplex (FDD); it utilized mobile-controlled handoff (MCHO). It supports both circuit switched and packet switched access protocols.

Mobile Data

RAM Mobile Data (based on the swedish Mobitex system), Advanced Radio Data Information System (ARDIS) {developed for IBM's customer engineers}, Cellular Digital Packet Data (CDPD) {developed to provide data as an overlay on analog cellular systems; based on Mobile IP}

Generally low rate systems 2.4 - 8 kbps

Interestingly Mobitex had greater national coverage than even the analog cellular system, because the swedish military used it.

There were both public Mobitex systems (such as that operated by Telia) and private systems (such as the one at Arlanda Airport).

Paging

Within local paging areas or via satellite.

The key to paging device's high performance is sleeping 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 - using a handset built for them by Motorola to operate over the wide variety of SMR channels which they bought.

Satellite

Especially Low Earth Orbit Satellie (LEO) - numerous attempt to field systems - one problem is that most of the time the satellites are over regions with few possible customers. Also most only are in range for ~10 minutes or so - so there are frequent handoffs.

Mid-earth orbit (MEO) and Geostationary (GEO) satellite - generally cover too large an area and do 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

cdma200, WCDMA, SCDMA

Local Metropolitan Area Networks (LMDS)

Point to point or multipoint (generally wideband) links - some operators have more than 700MHz worth of bandwidth available (in aggregate) in a given market (geographic) area.

Point-to-Point Optical links

Using laser light sources it is possible to achieve very high speeds for such point-to-point links.

Wireless Local Area Networks (WLANs)

- Frequency Hopping Spread Spectrum (FH-SS)
- Direct Sequence Spread Spectrum (DS-SS)
- Orthogonal Frequency Division Multiplexing (OFDM)
- IR links

Most of the radios have either used the Instrumentation, Scientific, and Medical (ISM) bands, National Information Infrastructure (NII) bands, or the HiperLAN band.

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

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.

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

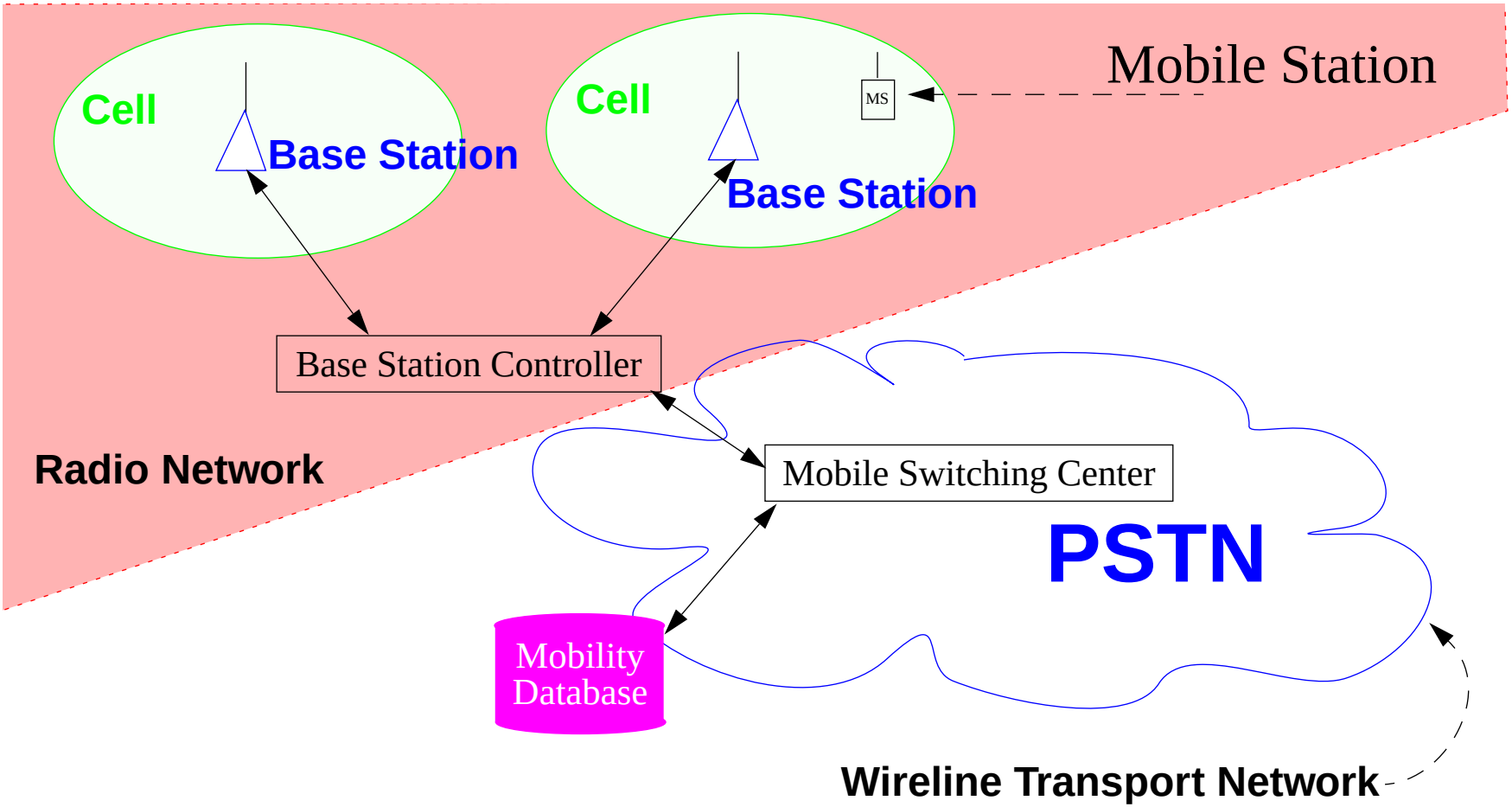


Figure 3: Basic PCS network architecture

Example of PCS Architecture

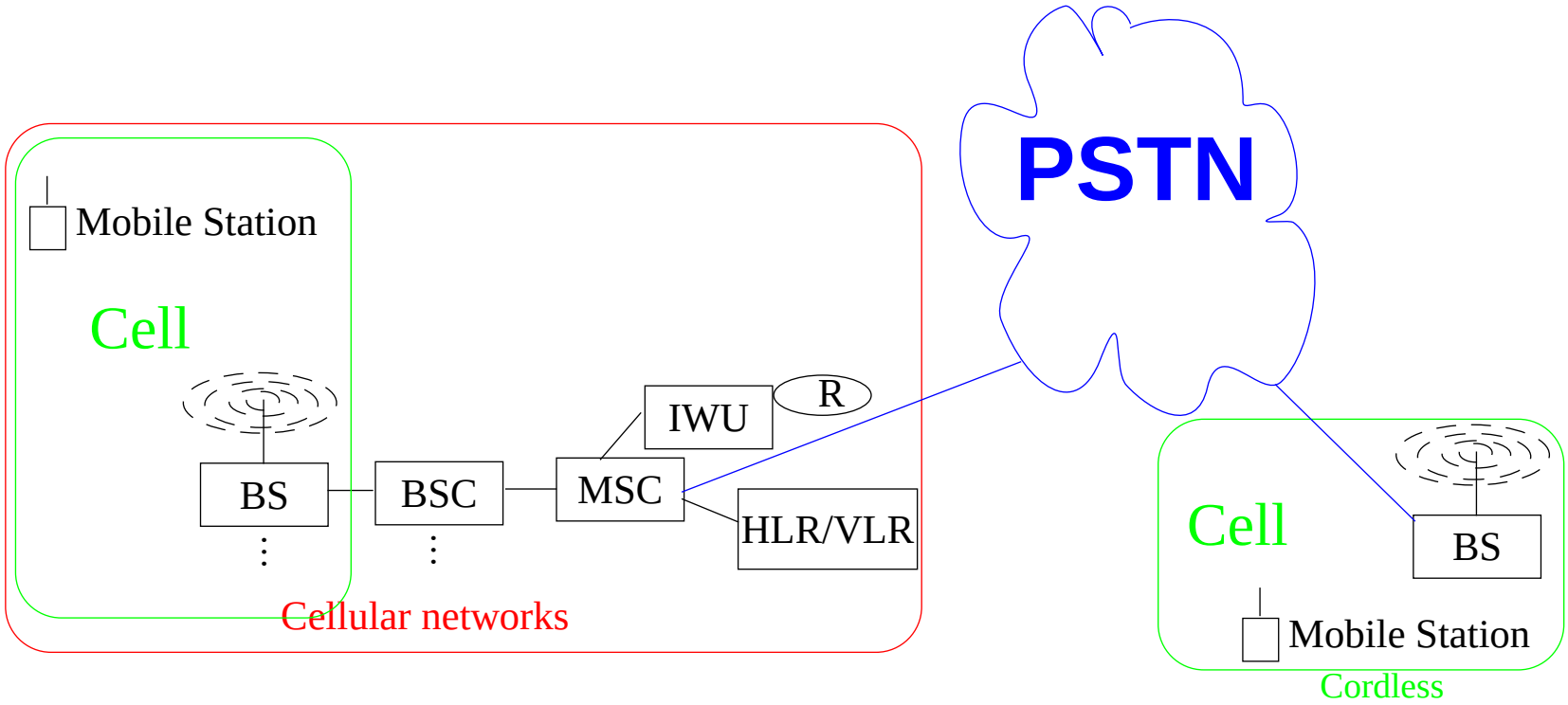


Figure 4: Cellular and Cordless networks

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

PCS network architecture supporting Mobility

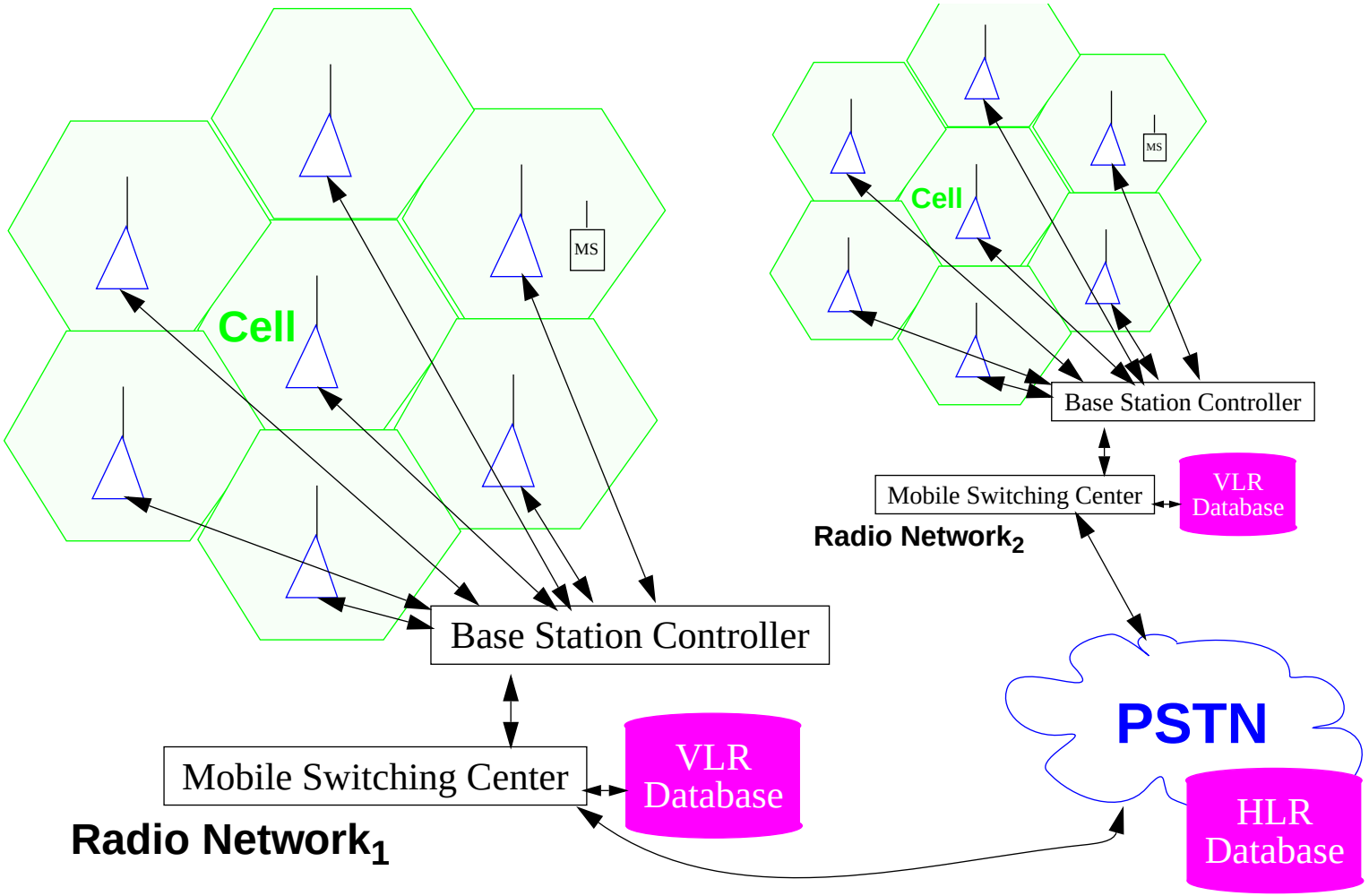


Figure 5: Basic PCS network architecture

Mobility Management

If mobile only **originate** 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)

Coming attractions:

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).

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 see any changes when the mobile moves with in 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 Mgmt: 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 particularily 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.

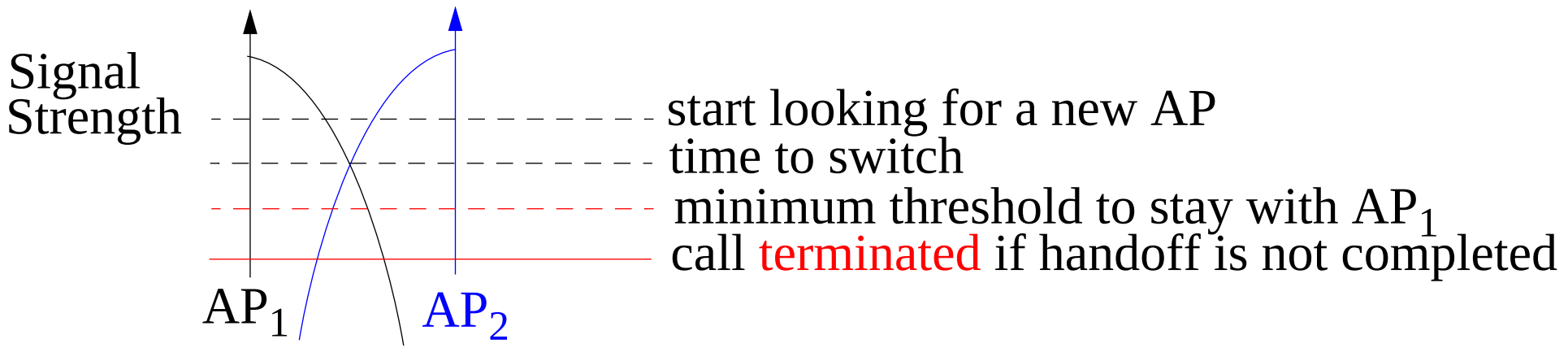
Handoff Criteria

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):

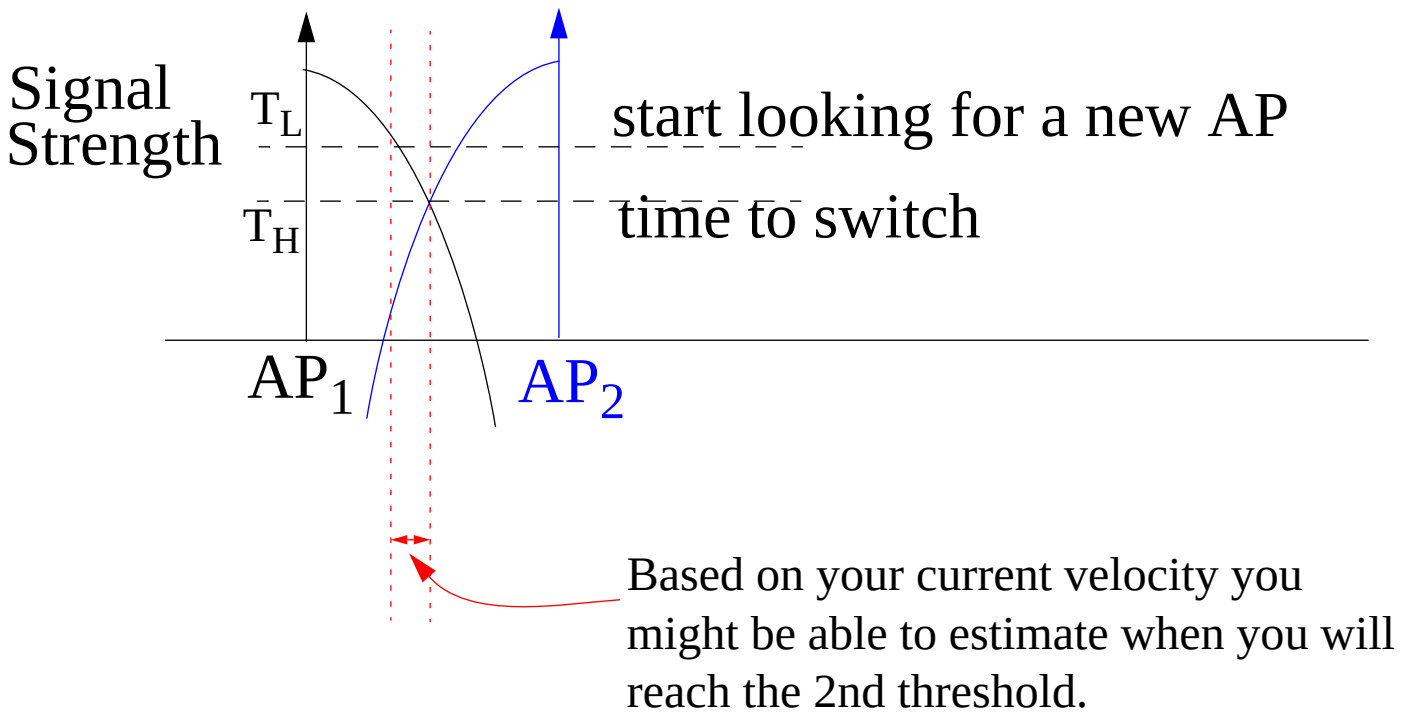


Handoff Goals

- 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, … - the handoff has to deal with this
- efficiency - the handoff should result in improved effciency (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 - the 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 MS and the Base Station experience a channel which varies - due to user movement, movement of other users, reflections, diffractions, … :

- Rapid-fading
  - Rayleigh-distributed evelope 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 measuremets of the channel:

- Word Error Indicator (WEI) - based on the receiver being able to decode the received signal correctly
- Received Signal Strength Indication (RSSI) - a measure of the received signal strength (in units of dB)
- Quality Indicator (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 technqiues (bit interleaving, convolutional coding, equalizers, …)

For further information about these techniques - see:

William C.Y. Lee, *Mobile Cellular Telecommunications: Analog and Digital Systems*, Second Edition, 1995, ISBN 0-07-038089-9

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

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

Who makes the handoff decision?

- Network controlled handoff (NCHO) - the network makes the decision; used in CT-2 Plus and AMPS
- Mobile assisted handoff (MAHO) - the mobile provides data which the network uses to make the decision; used in GSM and IS-95 CDMA
- Mobile controlled handoff (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 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 MN's new cell. In telephony systems this often involves setting up a "bridge" to copy traffic to both the new and the old channels.

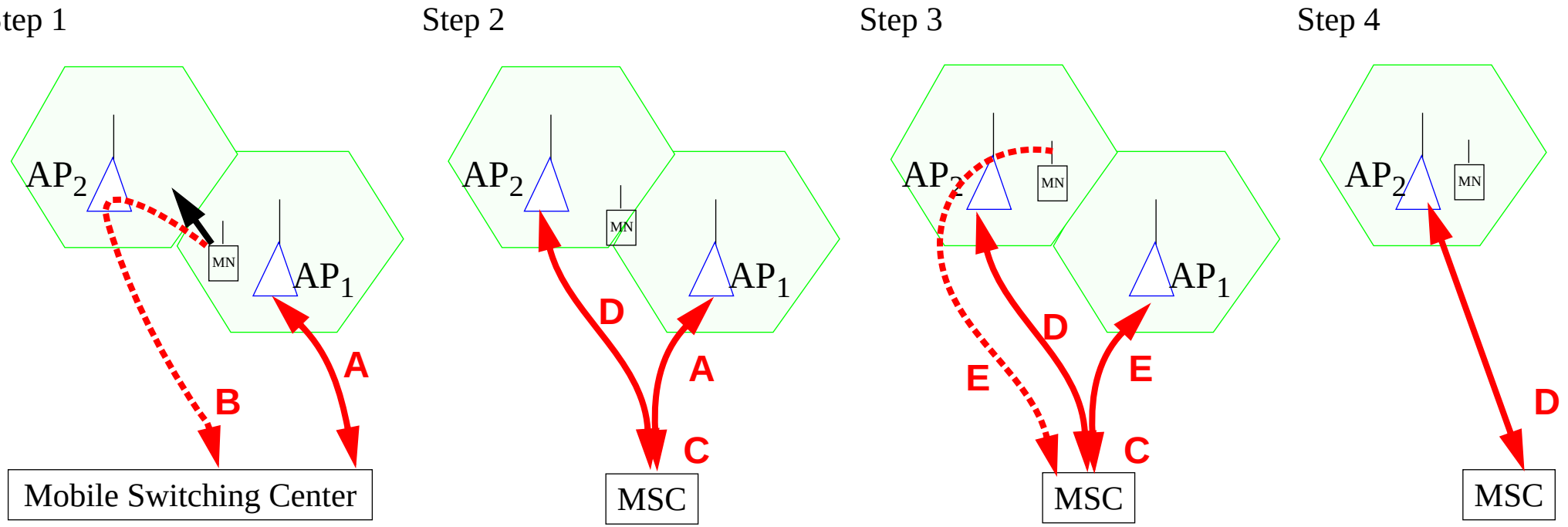


Figure 6: steps in handoff within the control of one MSC (not showing the BSC)

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 the same as new calls)

- handover is block - 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 buffer a wiating queue of 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.

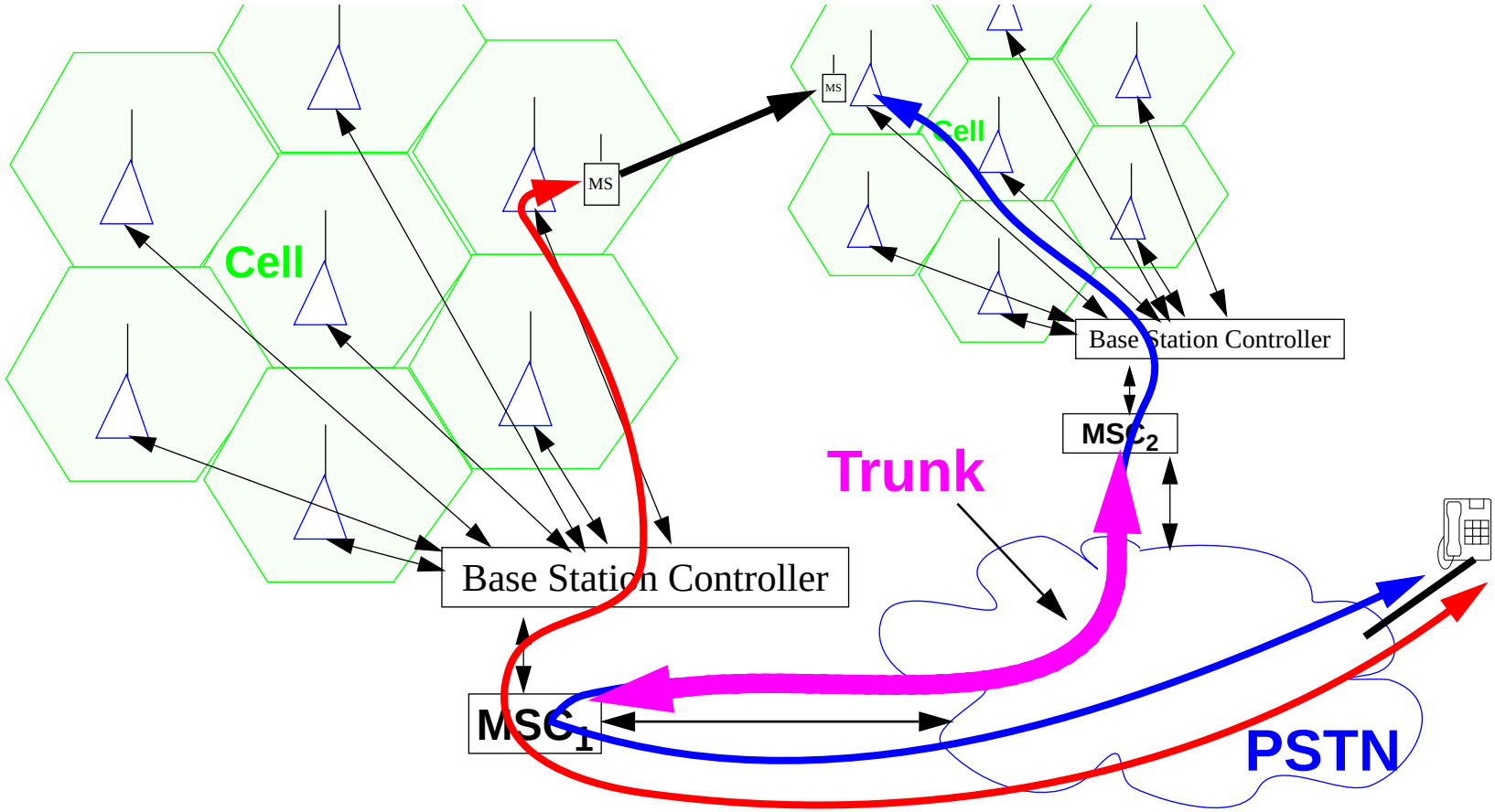
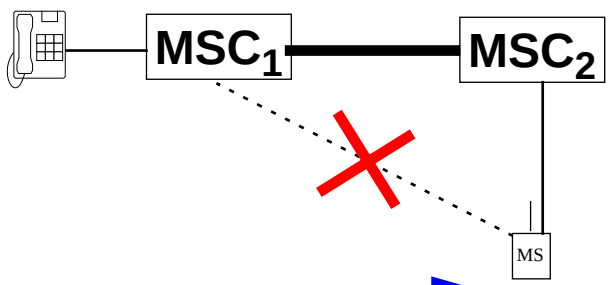
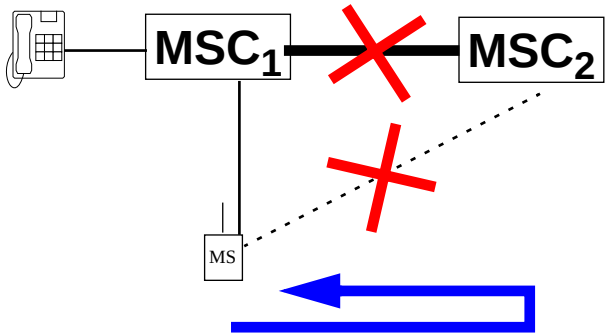


Figure 7: Handoffs between two MSCs

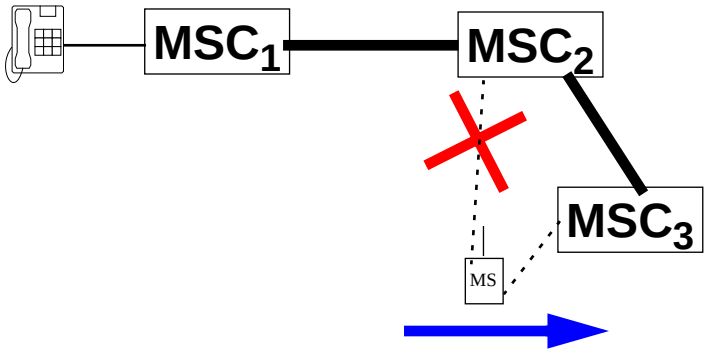
What happens if the mobile moves gain?



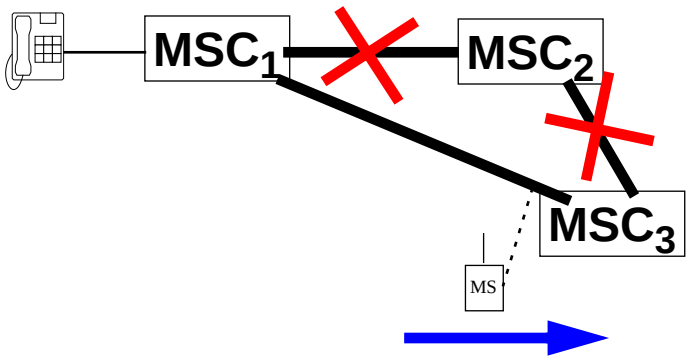
a. Forward handoff



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 existance (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 address later in the lectures).

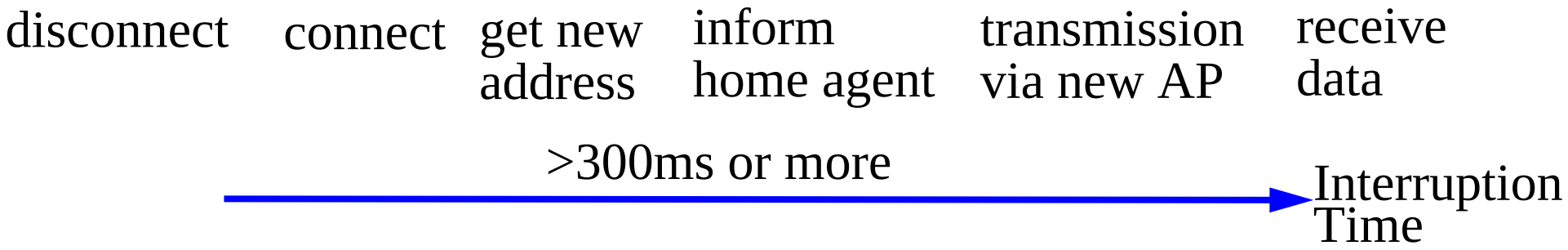
Fast Mobile IPv4 handoff via Simultaneous Bindings

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). Home Agent duplicates all packets destined for the MN for the time of the handoff and relays all data to 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!

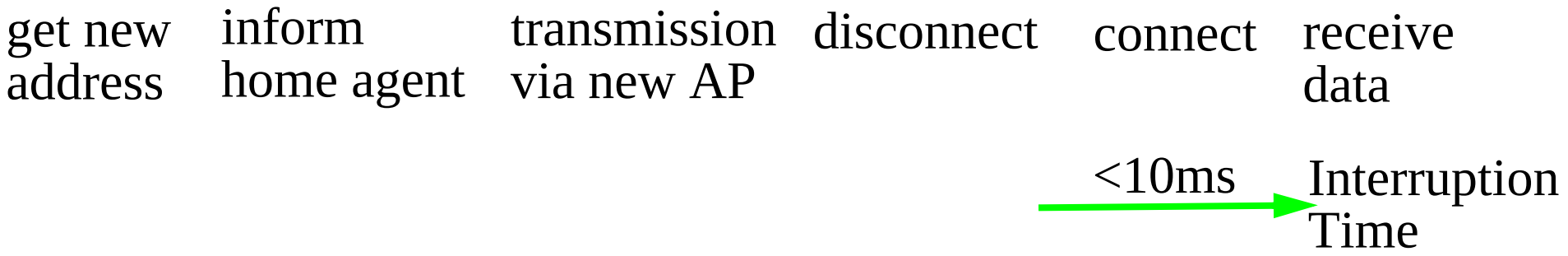
Fast handover timeline

a

Traditional Mobile IP: “break before make”



Enhanced Mobile IP: “make before break”



a. Figure adapted from http://www.ccrle.nec.de/Figure3.gif which is part of *http://www.ccrle.nec.de/Hand-off.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.

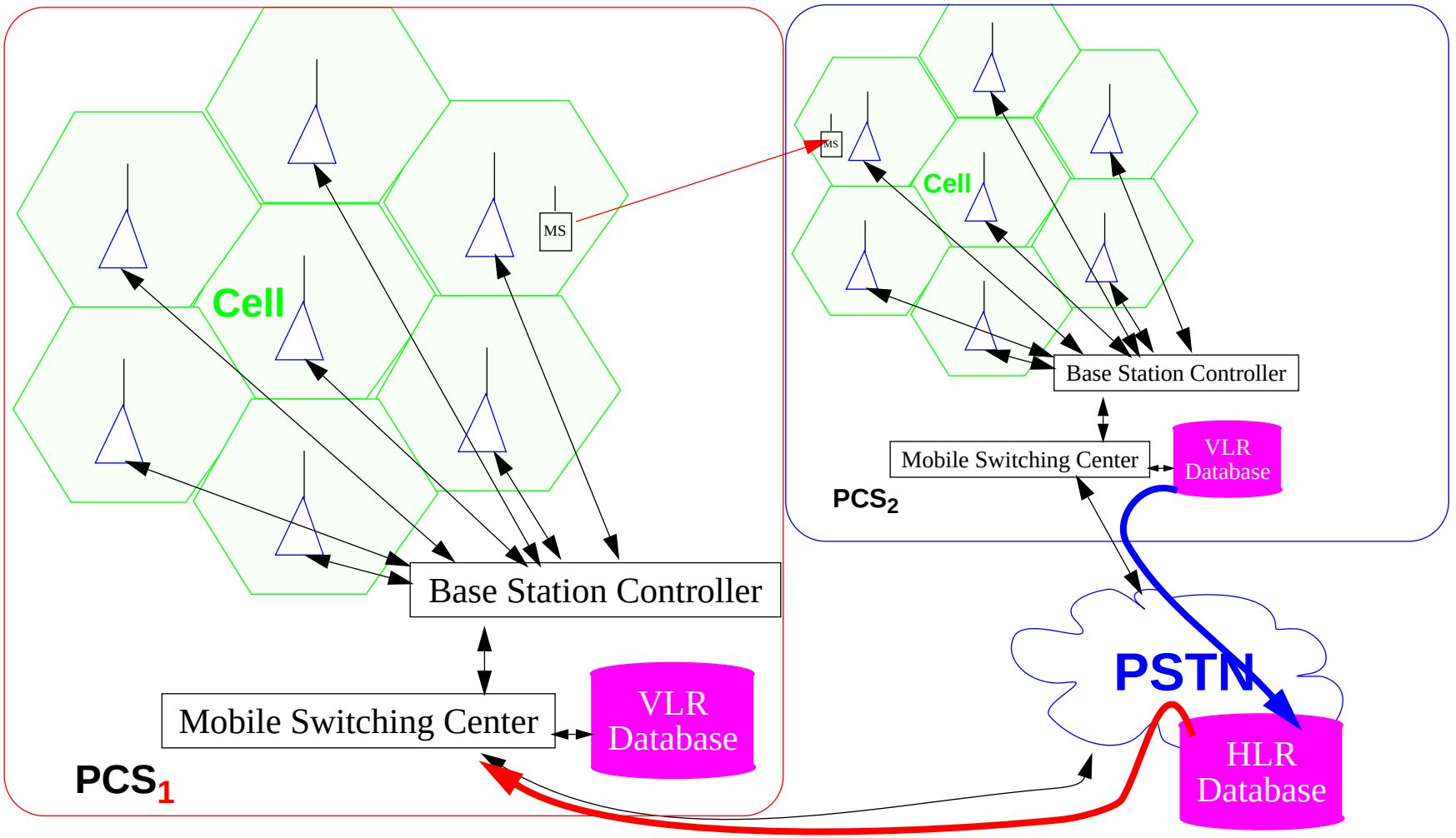


Figure 9: Mobile roams from PCS_1 to PCS_2

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) - this exists at the user's *home system*

visitor location register (VLR) - this is a temporary record at the *visited system*

Roaming example

A user from Kiruna has been visiting in Göteborg, they arrive in Stockholm.

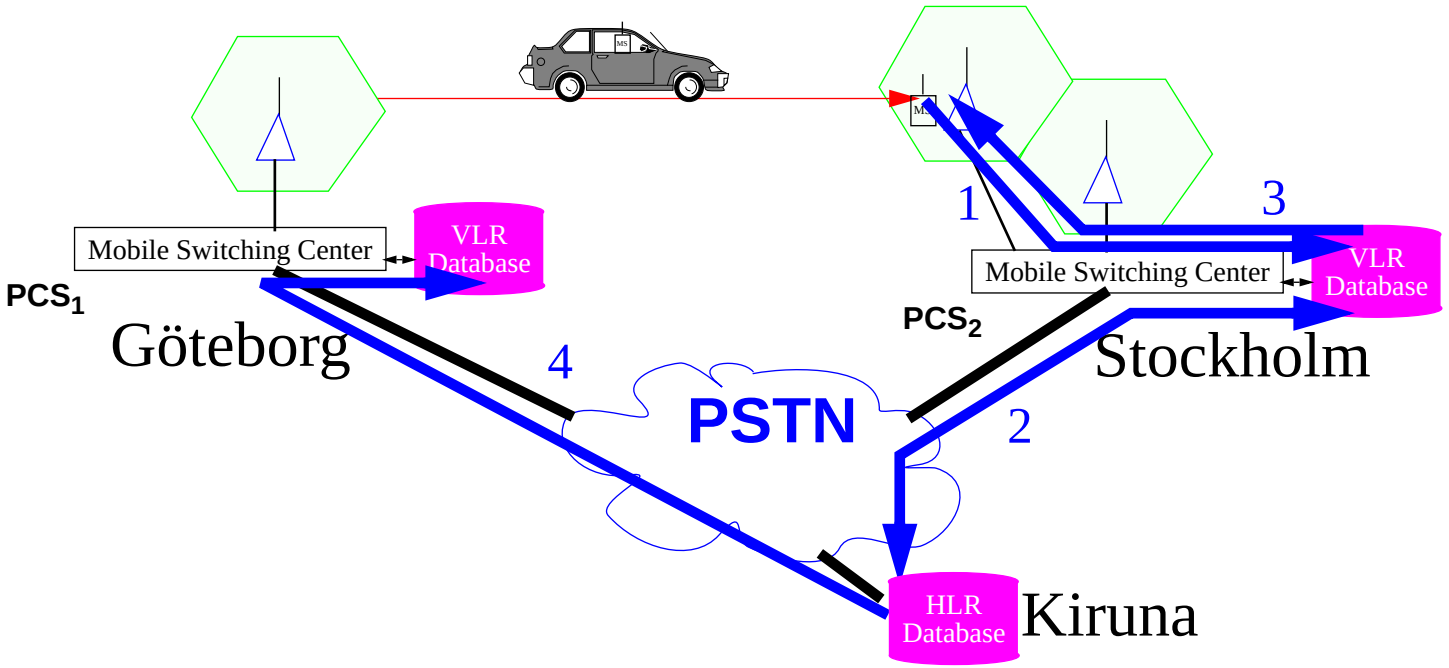


Figure 10: Mobile roams from PCS_1 to PCS_2

1. When the user (and their MS) arrives in Stockholm, then have to register with the VLR for PCS_2.
2. PCS_2's VLR informs the user's HLR of the user's current location (i.e. that the HLR should point to the VLR in PCS_2). HLR send 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 - the MS periodically registers with the VLR, if there is no reregistration within a time out period - the 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 extened via:

1. sending a page to a user and then have the call in

2. calling into a meeting point - which patches two 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 by using the mobile to help the handoff times can be reduced.

For example, in GSM the MS transmits measurements twice a second.

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 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

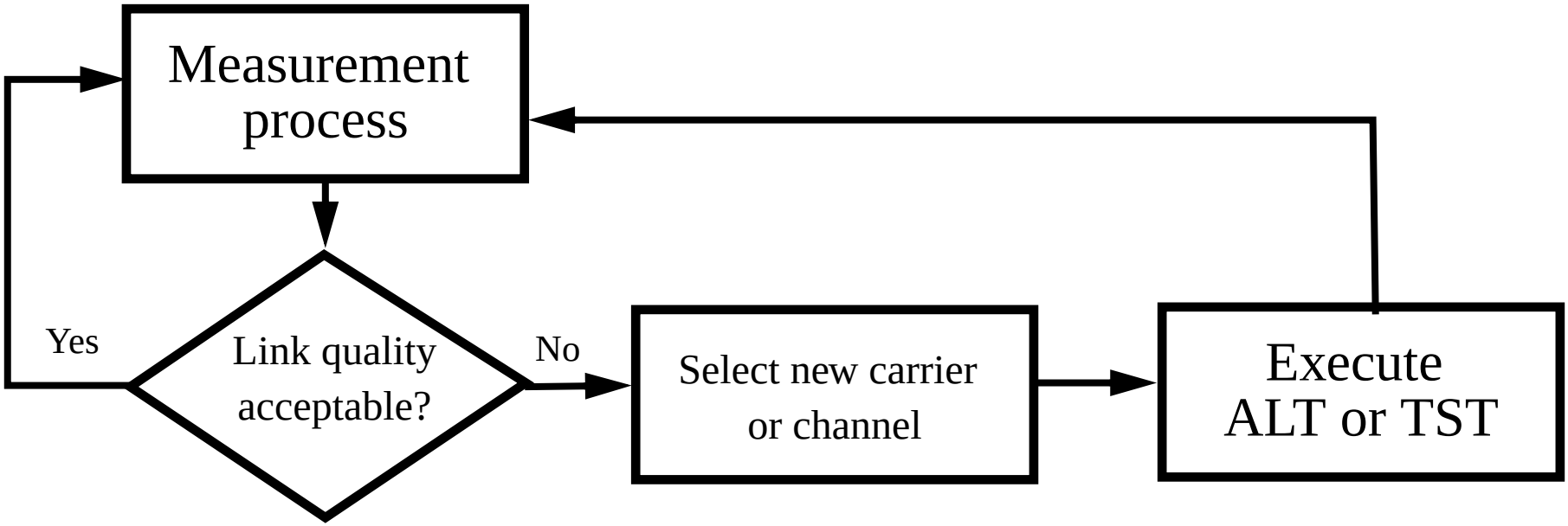


Figure 11: MS-quality maintenance processing

Different systems use different approaches to the measurement process. For example, some DECT implementations can measures the RSSI of all channels simulatneously. 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 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 give servce quality
- use a simple algorithm
- require a minimium 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 block 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 codes 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	connects only to a single base station at a time
soft handoff	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

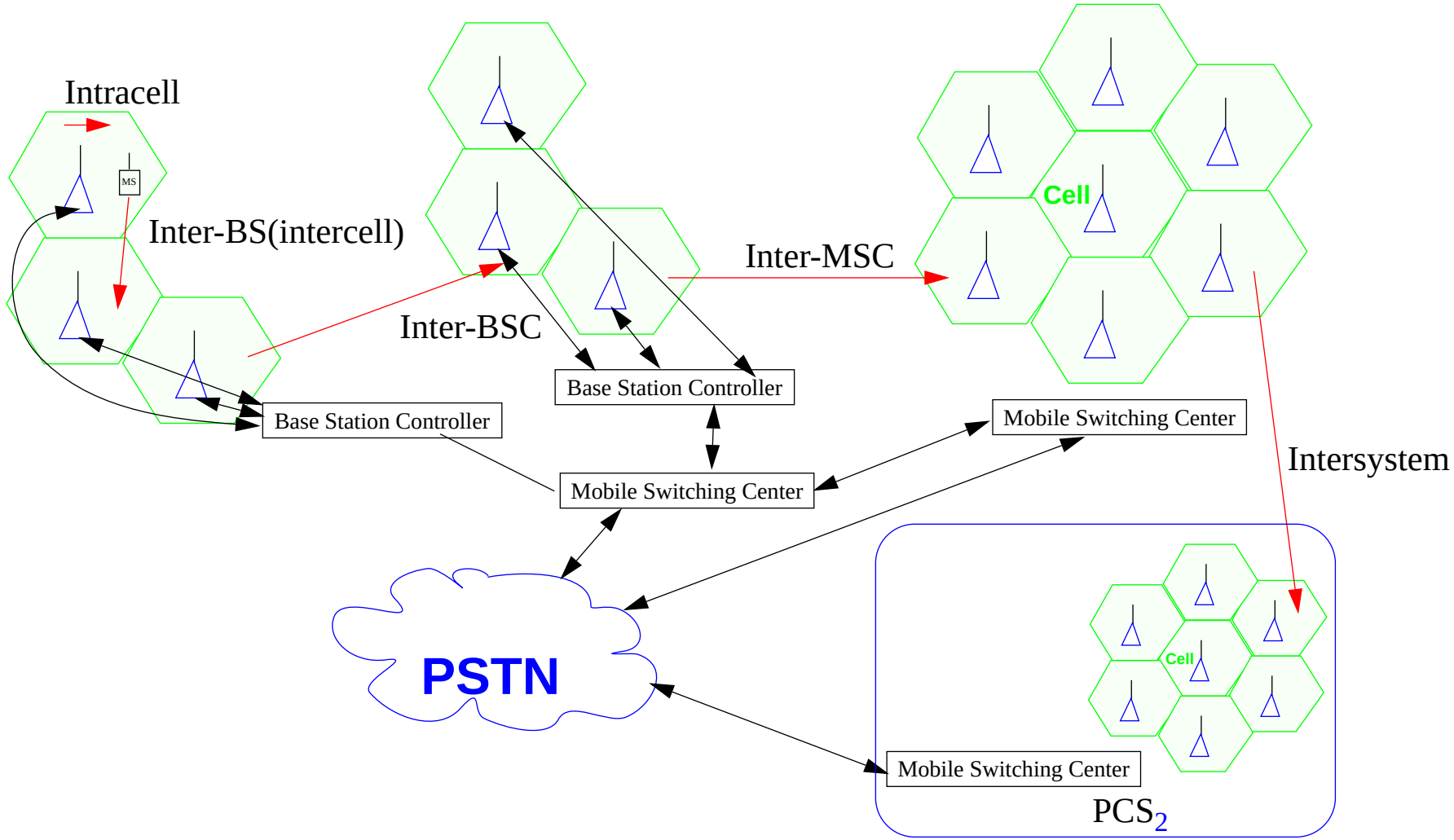


Figure 12: Handoffs, mobile moves within PCS_1 and then on to PCS_2

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

From onw BSC | With Two BSCs | With Two MSCs | Between systems

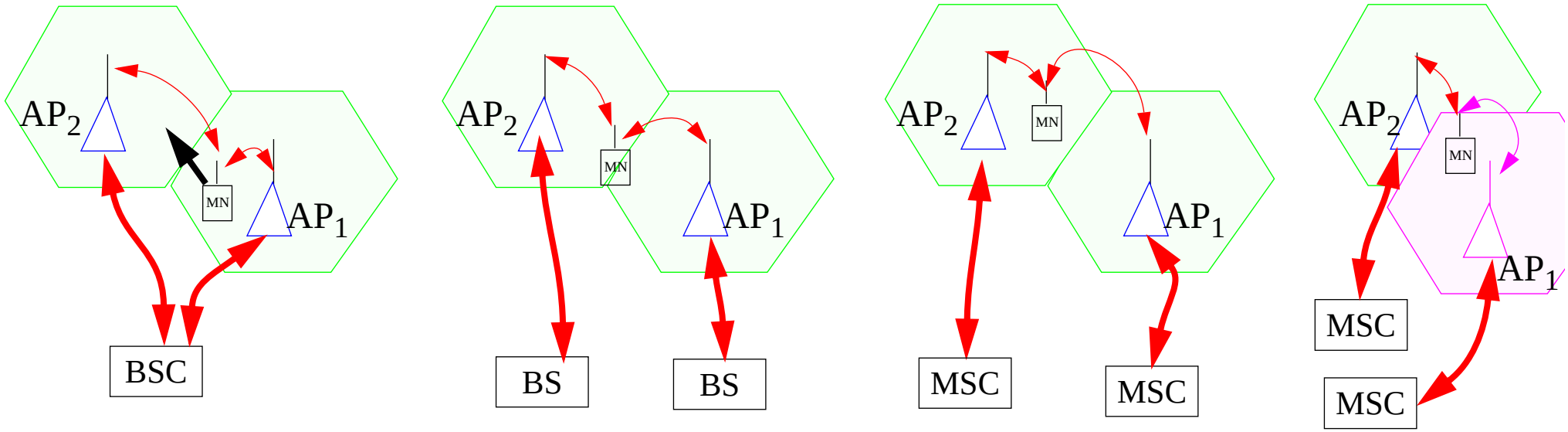


Figure 13: Soft handoffs

Some CDMA systems use very precise link level timing to enable the signals from mutiple 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

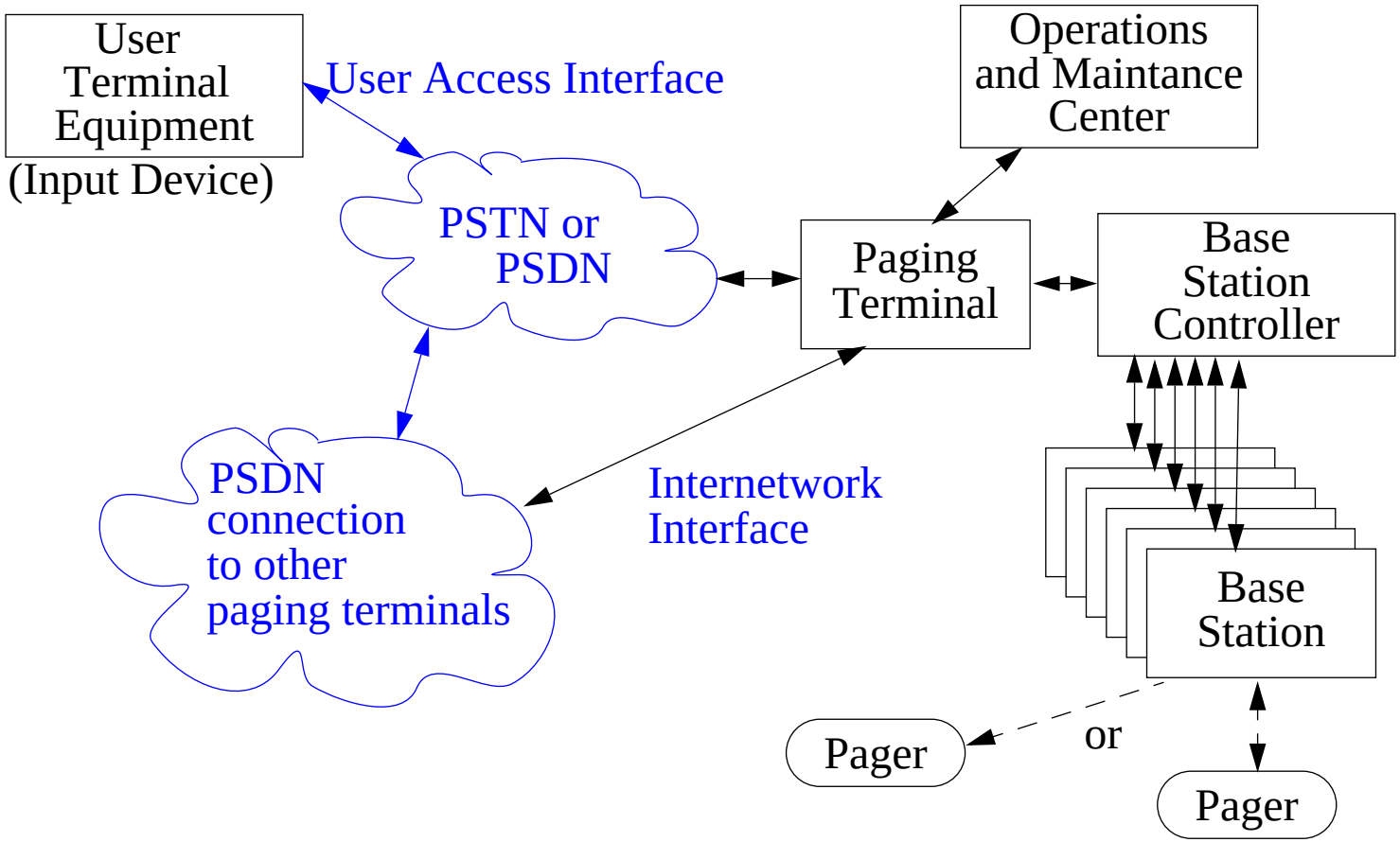
Originally a one-way personal altering/messaging system invented by Charles Neergard in 1949 (annoyed when hospitalized by the voice paging over the public address system).

A transmitter sends a stream of addresses and messages. Pages 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 call back number (or code) is entered by the sender, which then appears on the pager's display
Alphanumeric	late 1980's, display a text message

http://www.motorola.com/MIMS/MSPG/Special/explain_paging/ptoc.html

Paging Architecture



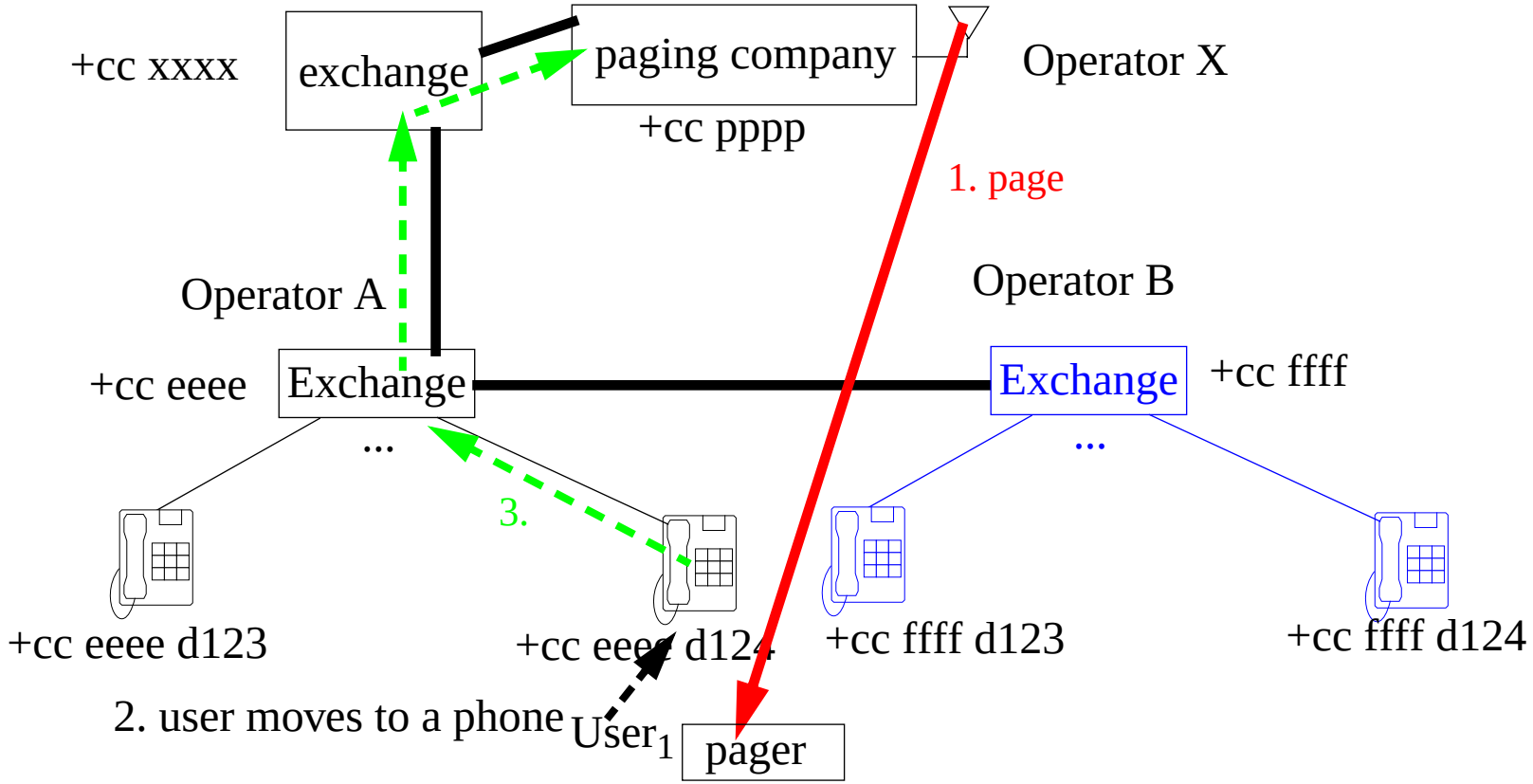
Paging terminal has DB of customers, cap code, pager number, types of msgs, …; convert voice msg to text (for alphanumeric pagers); store in mailbox for pager; forward to other paging terminals; send to relevant Base Station Controller(s)

Paging Service area

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

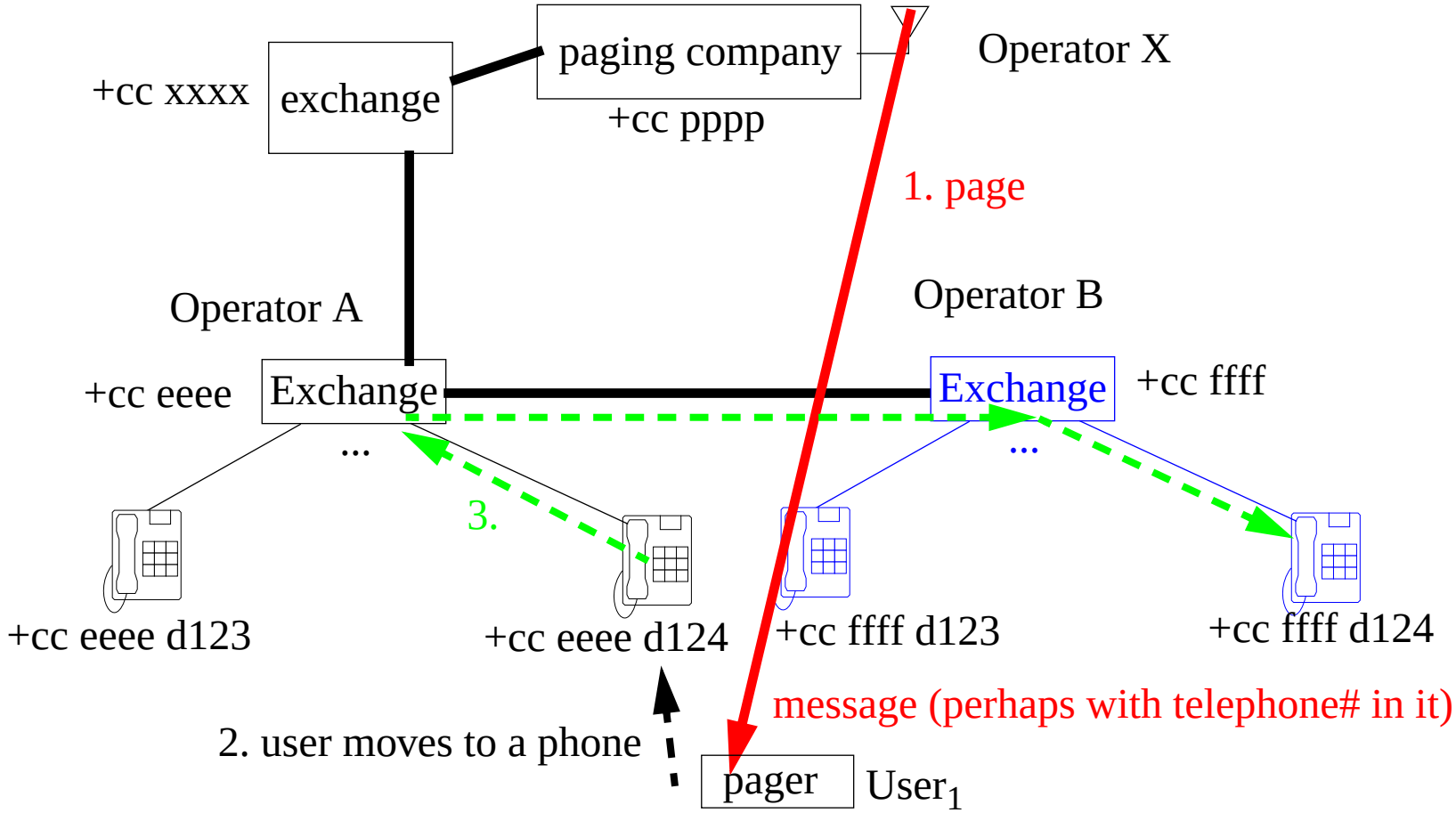
If the user temporarily left the paging service area or if the signal could not reach them, then they would miss it. Motorola's ReFLEX technology, a two-way paging system, keeps transmitting a paging message until the user's pager sends a confirmation that it has been received.

Introduction of paging systems



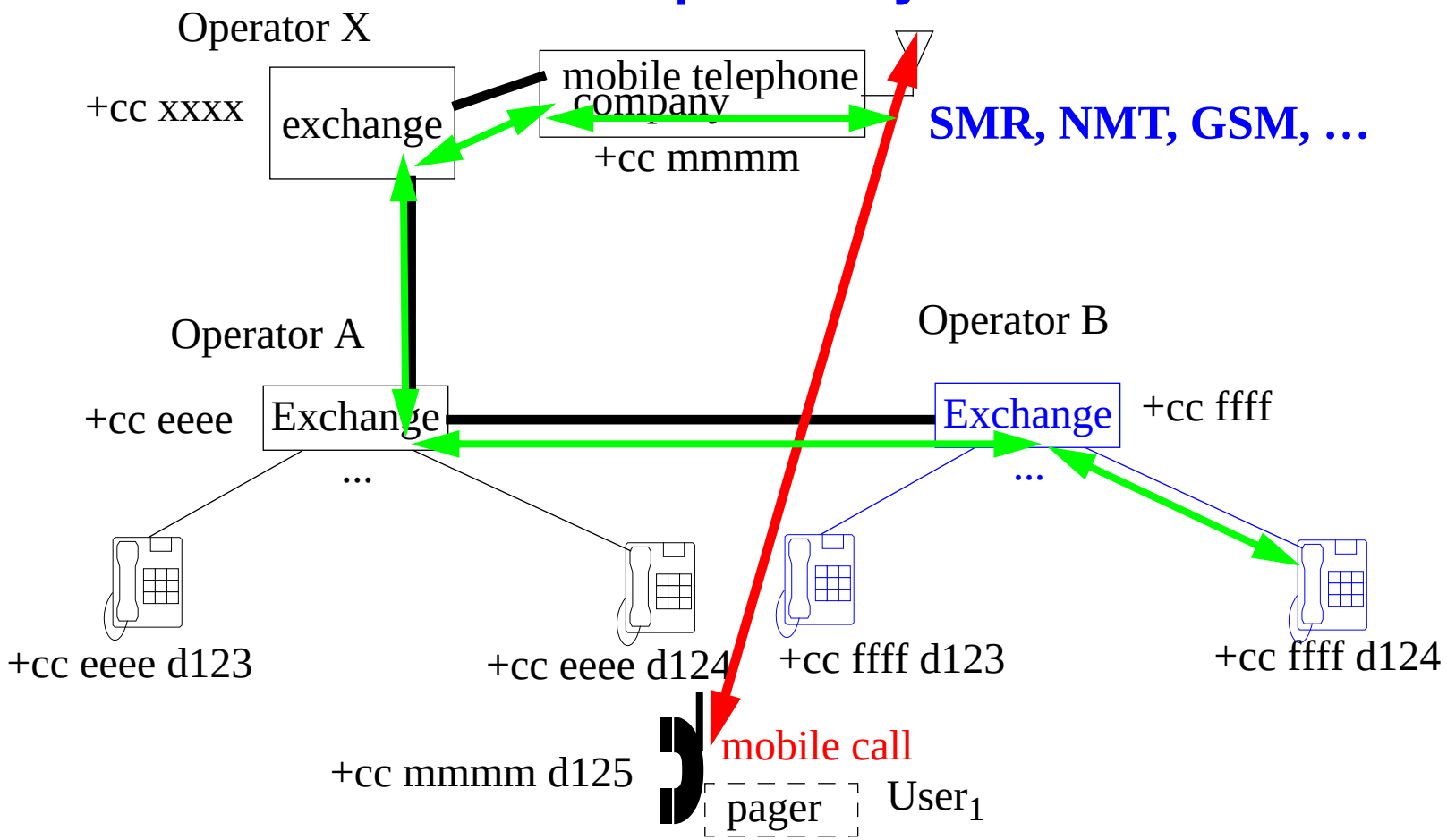
Upon a page, user moves to nearest phone, calls paging company,company operator tells the user what telephone number to call - perhaps they (also) convey a short message. The mobile user can be contacted and told by the operator at the paging company to connect to the fixed telephone network. [i.e.,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

Alphanumeric paging systems



Upon a page, user moves to nearest phone, calls a number based on the content of the (page) message; 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

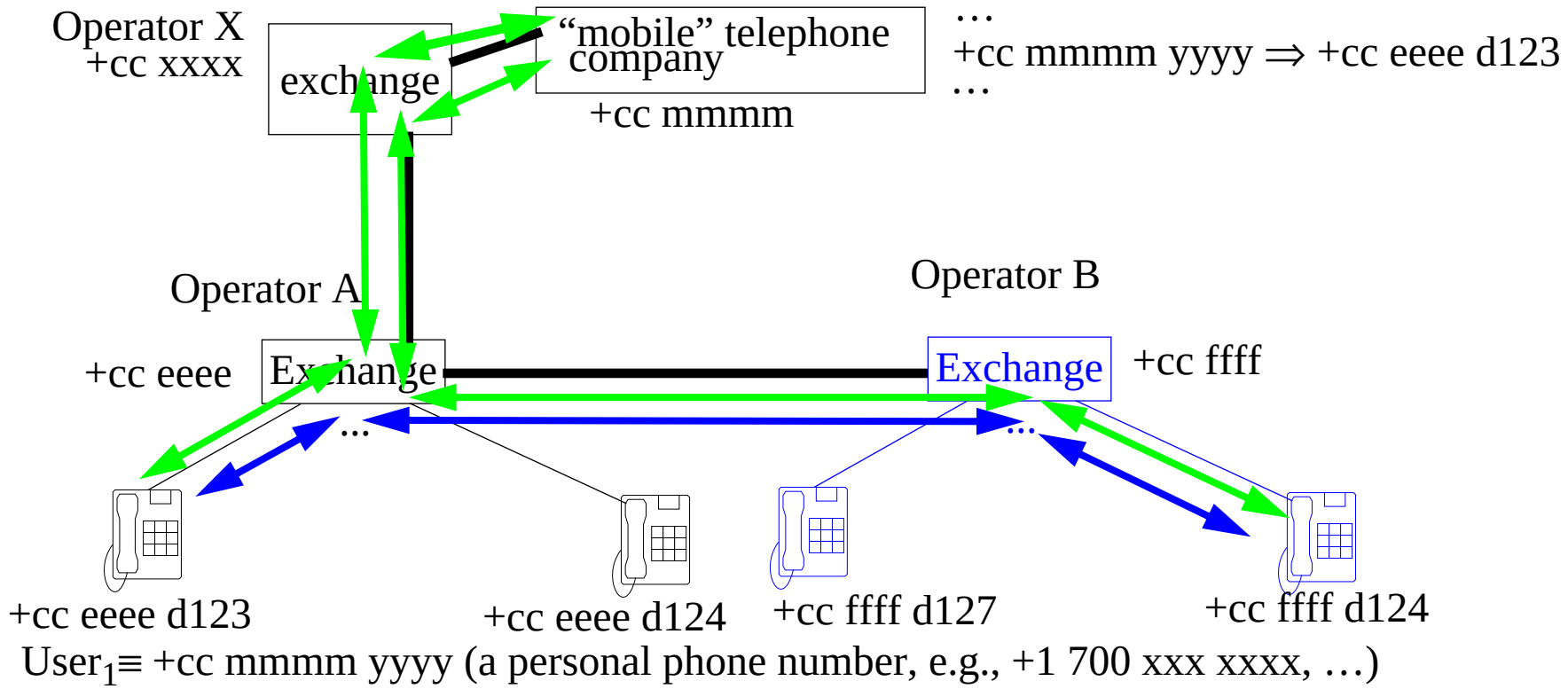


The mobile user is directly reached by the call through the mobile telephone network.

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

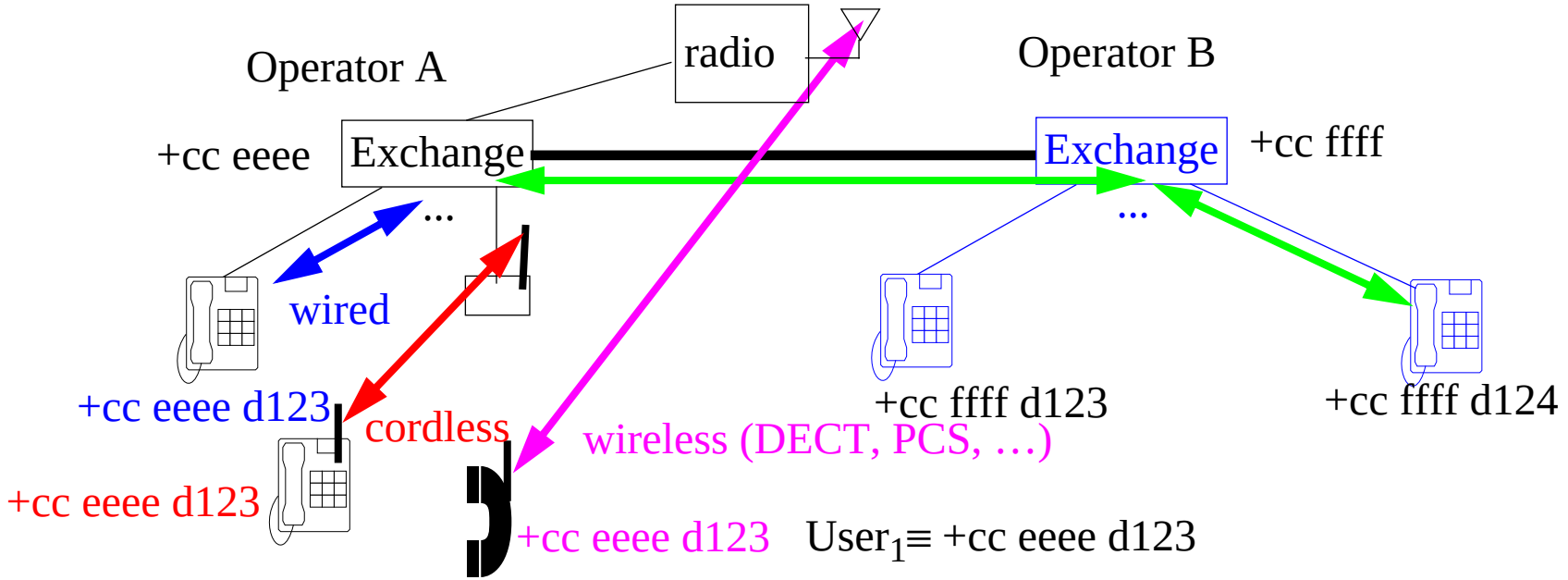


The mobile user is indirectly reached through the fixed telephone network.

- 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)

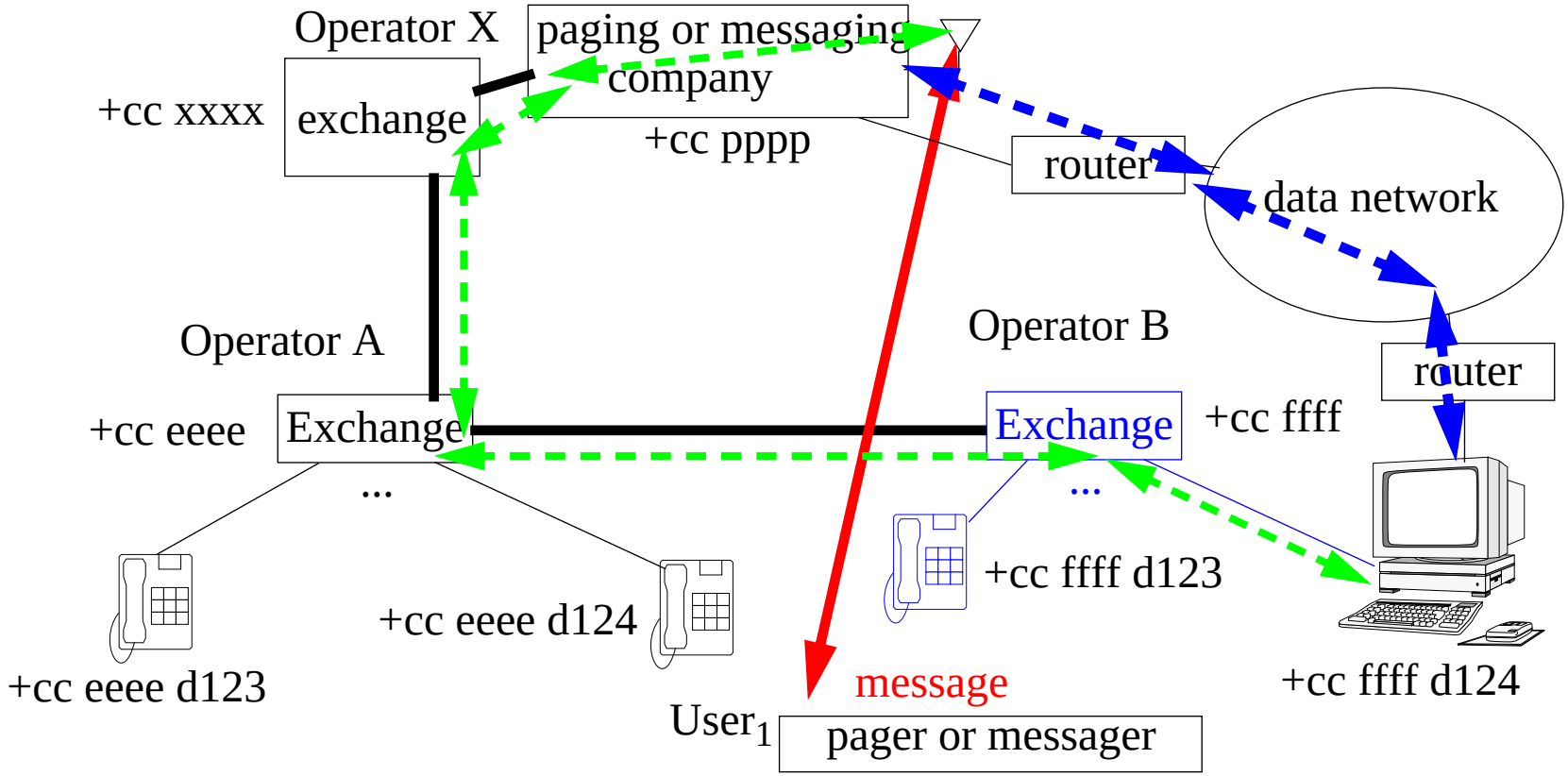


The mobile user is reached by local redirection (which may utilize local wireless links) of the call coming from the fixed telephone network.

- 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).

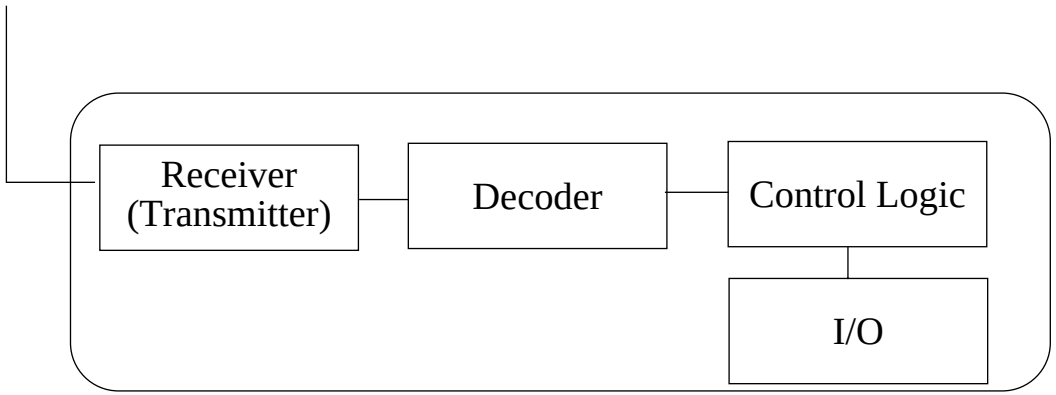
Two-way paging and messaging systems



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

- Traditionally the paging or messaging system was a separate data network, but GSM supports **Short Message Service** which provides alphanumeric paging via the same infrastructure.
- The messaging device is likely to 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 was adopted 1995; Telocator Message Entry (TME) protocol - the inputer 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 (over comes the proprietary protocols to/from paring terminals - such as Glenayre Link Module, Spectrum Data Link Handler)

Software:

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

http://www.linuxdoc.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

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*

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 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).

References and Further Reading

See the summary in section 2.5 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 the ideas are worth understanding.

User profiles

[1] 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

[2] C. Perkins. IP Mobility Support. Internet RFC, RFC 2002, October 1996.

[3] D. B. Johnson and C. Perkins. Mobility Support in IPv6. Internet draft, draft-ietf-mobileip-ipv6-13.txt, November 2000. Work in progress.

Hierarchical Mobile IP

[4] E. Gustafsson, A. Jonsson, and C. Perkins. Mobile IP Regional Registration. Internet draft, draft-ietf-mobileip-reg-tunnel-04.txt, March 2001. Work in progress.

[5] H. Haverinen and J. Malinen. Mobile IP Regional Paging. Internet draft, draft-haverinen-mobileip-reg-paging-00.txt, June 2000. Work in progress.

Fast handoff

[6] K. El-Malki and H. Soliman. Fast Handoffs in Mobile IPv4. Internet draft, draft-elmalki-mobileip-fast-handoffs-03.txt, September 2000. Work in progress.

Proactive handoff

[7] P. Calhoun, T. Hiller, J. Kempf, P. McCann, C. Pairla, A. Singh, and S. Thalanany. Foreign Agent Assisted Hand-off. Internet draft, draft-ietf-mobileip-proactive-fa-03.txt, November 2000. Work in progress.

TeleMIP

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

Cellular IP

[9] A. T. Campbell, J. Gomez, S. Kim, A. G. Valkó, C-Y. Wan, and Z. Turányi. Cellular IP. Internet draft, draft-ietf-mobileip-cellularip-00.txt, January 2000. Work in progress.

HAWAII

[10] R. Ramjee, T. La Porta, S. Thuel, and K. Varadhan. IP Micro-Mobility support through HAWAII. Internet draft, draft-ramjee-micro-mobility-hawaii-00.txt, March 1999. Work in progress.

[11] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, and L. Salgarelli. IP micro-mobility support using HAWAII. Internet draft, draft-ietf-mobileip-hawaii-01.txt, July 2000. Work in progress.

An Edge Mobility Architecture

[12] A. O'Neill, G. Tsirtsis, and S. Corson. Edge Mobility Architecture. Internet draft, draft-oneill-ema-01.txt, March 2000. Work in progress.

[13] A. O'Neill and S. Corson. An Approach to Fixed/Mobile Converged Routing. Technical Report TR-2000-5, University of Maryland, Institute for Systems Research, March 2000.

Comparison of IP Mobility protocols

[14] 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

Intersystem Handoff

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

http://www-sop.inria.fr/mistral/personnel/Eitan.Altman/SAT/NAB00.ps

Details of wireless channels

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