KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

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: 2002.03.14:11:58

Lecture 2 (Chapters 5-8)

Network Signaling

Interconnection between a 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 maintenace

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 use connectionless transport.

TCAP message flow for a MS registration

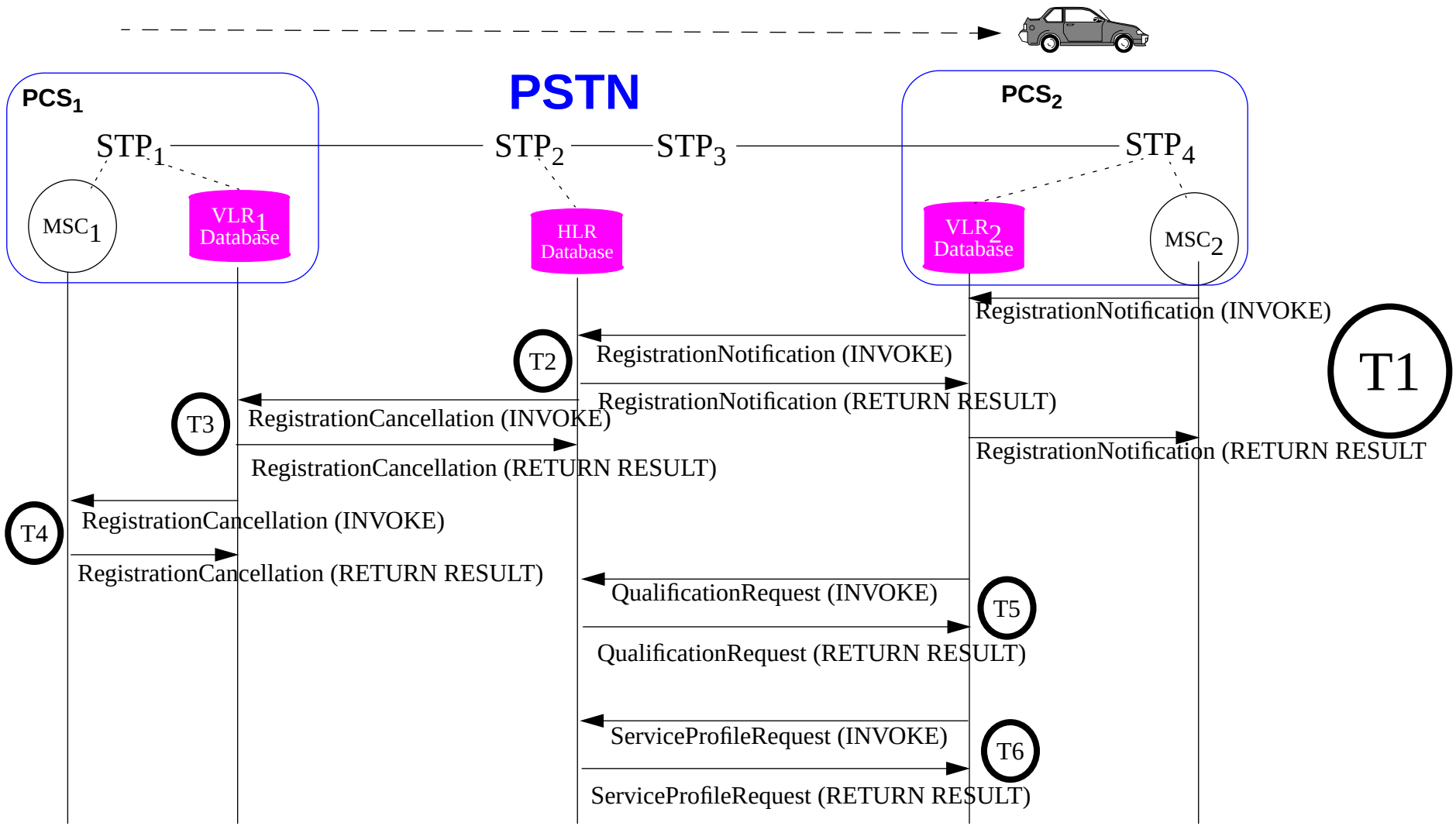


Figure 1: Mobile roams from PCS_1 to PCS_2

Transaction 2 - additional details

Signal Transfer Point$_3$ (STP$_3$) does a table lookup, i.e., Global Title Translation (GTT) on 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.

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 tranmitted 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

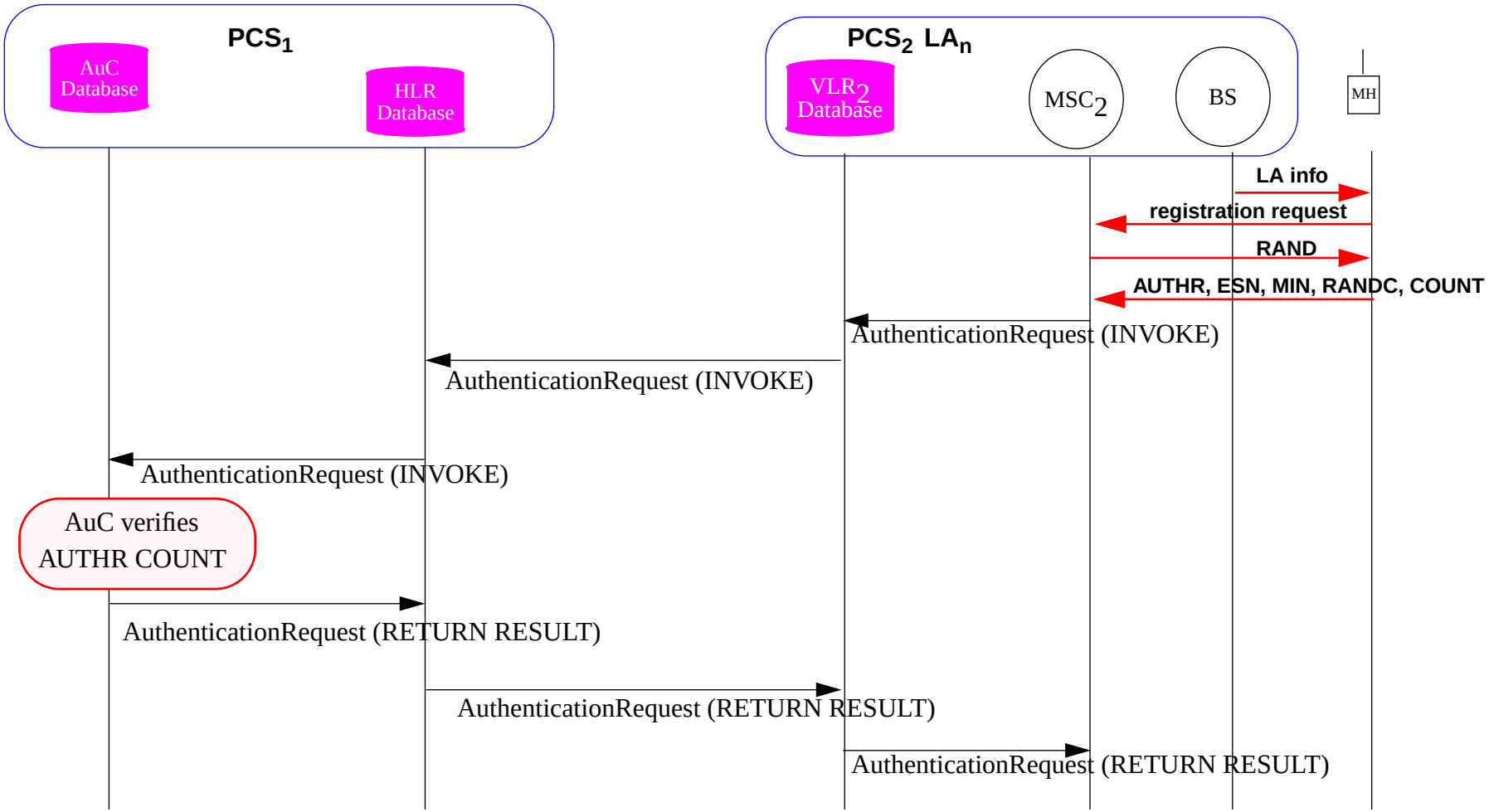


Figure 2: Mobile moves into a new Location Area (LA) at PCS_2

If authentication fails the result is RETURN ERROR.

Without-Sharing Call Origination

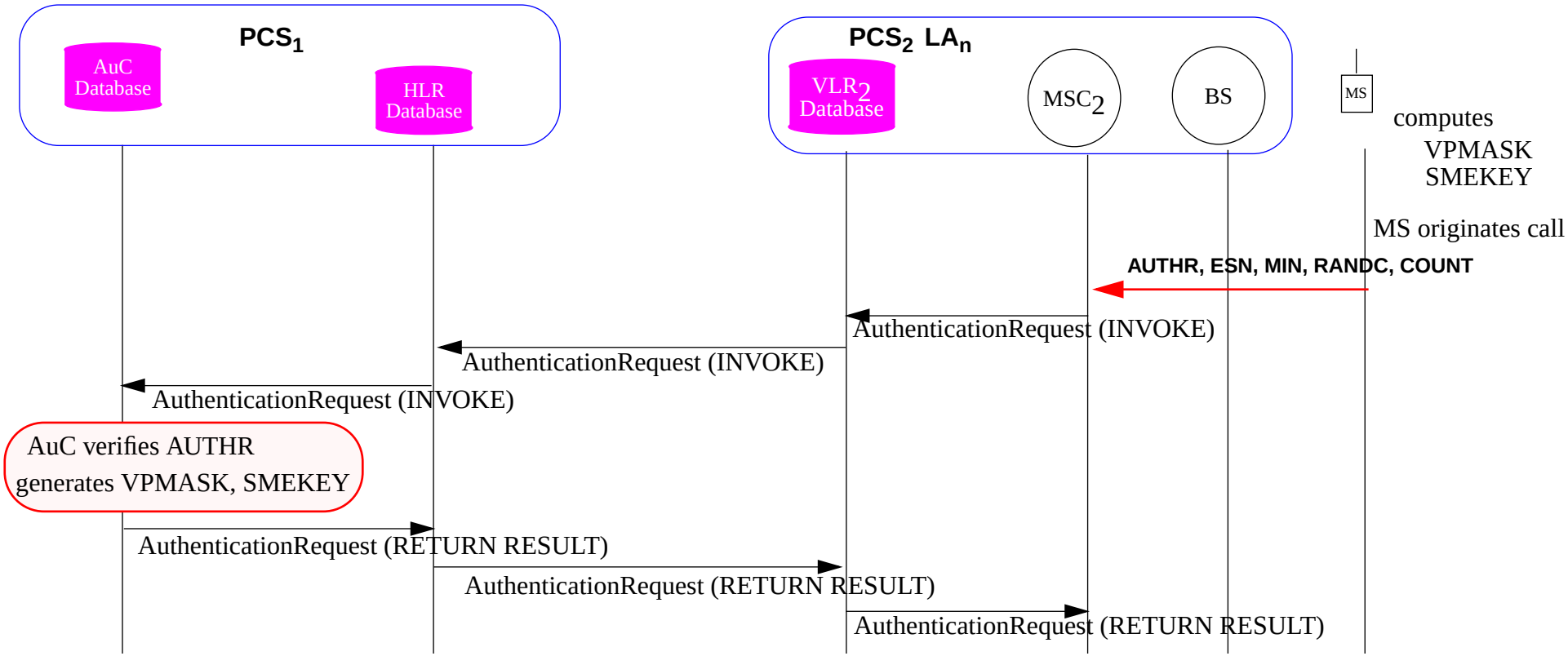


Figure 3: Mobile places a call in PCS_2

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

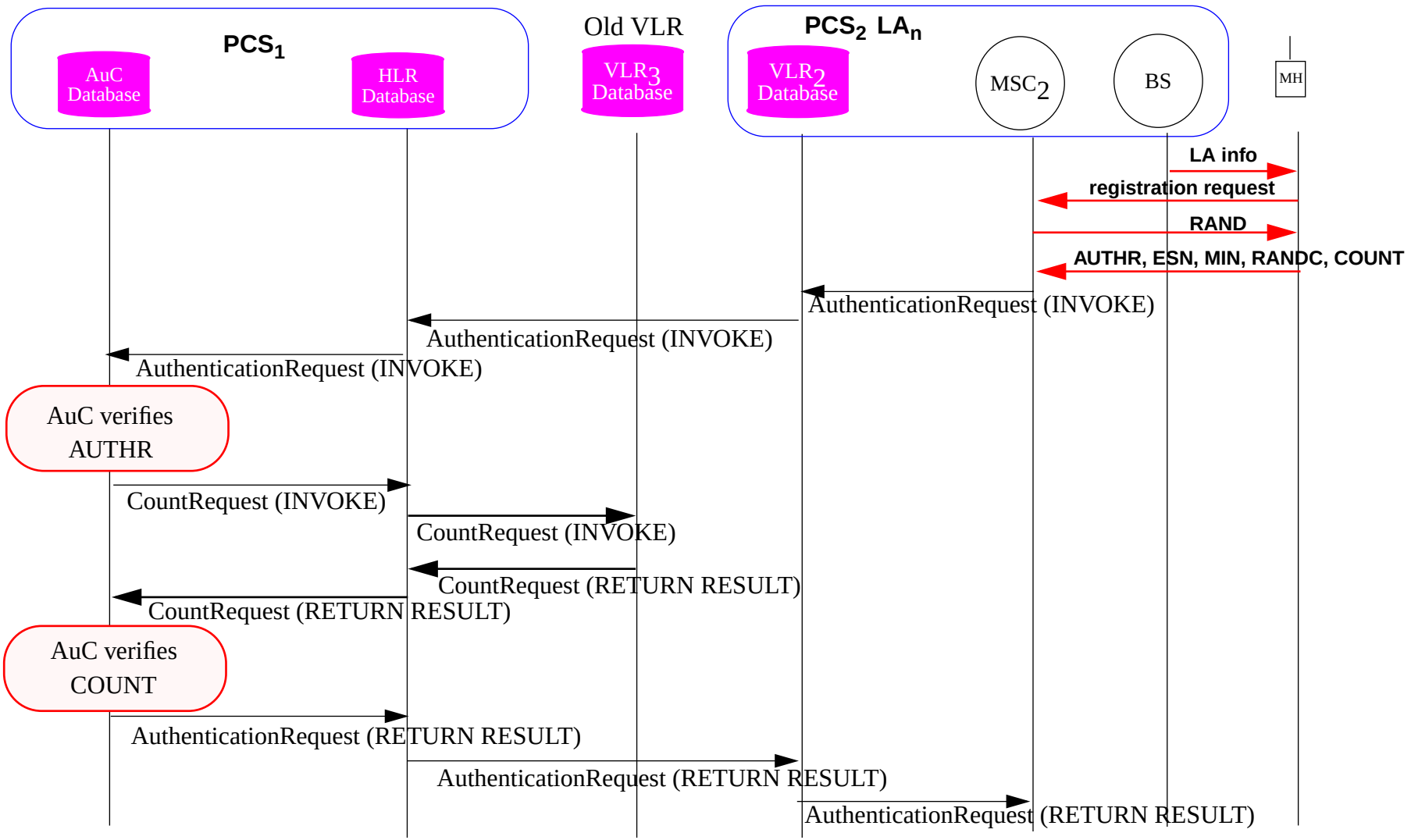


Figure 4: Mobile moves into a new Location Area (LA) at PCS_2 registration using Sharing scheme

Sharing Call Origination

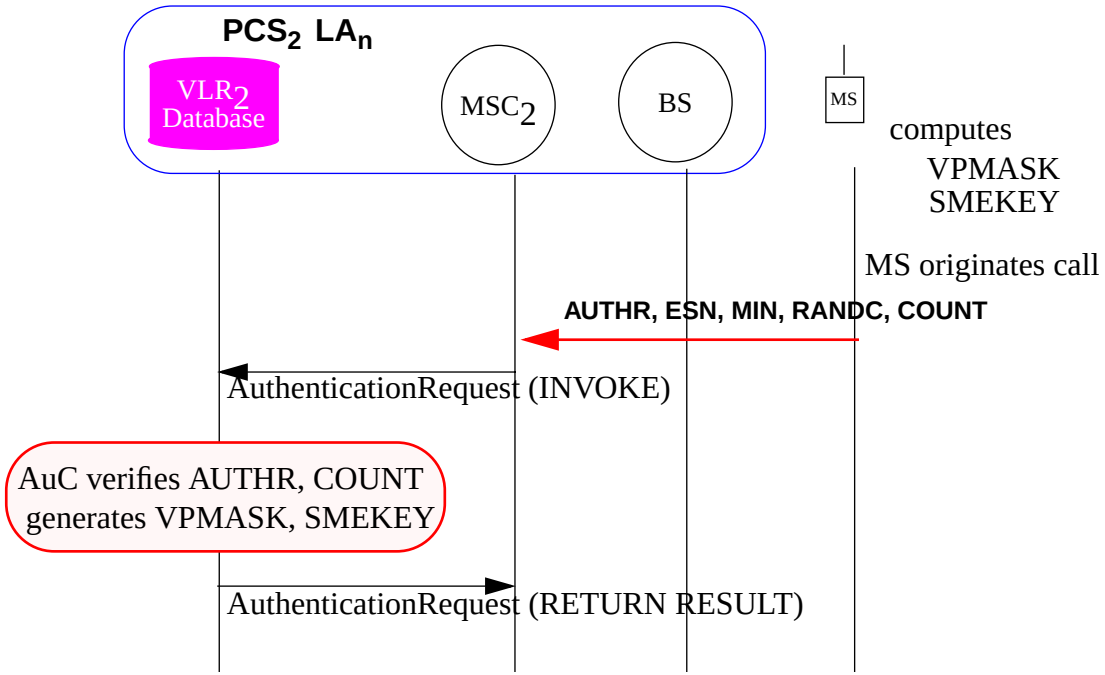


Figure 5: Mobile places a call in PCS_2 using sharing scheme

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

When should you use WS vs. S

Use WS when number of registration operatons > call origination/termination.

Can use an adaptive algorithm:

- based on statistics move between WS and S schemes
- once you make a call, then use S scheme; but if you move without making a call, then revert back to WS 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 [3].

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

- David Wagner (University of California at Berkeley graduate student) and Bruce Schneier[1] & John Kelsey (both of Counterpane Systems) announced they they had broken the Cellular Message Encryption Algorithm (CMEA)[5] 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”[6] - 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

Further reading

TIA

[1] TIA public documents
ftp://ftp.tiaonline.org/tr-45/tr45ahag/public%20documents/

TSB-51

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

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

[4] 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*

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

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

[6] 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

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

PAC 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 SCP.

PACS Architecture

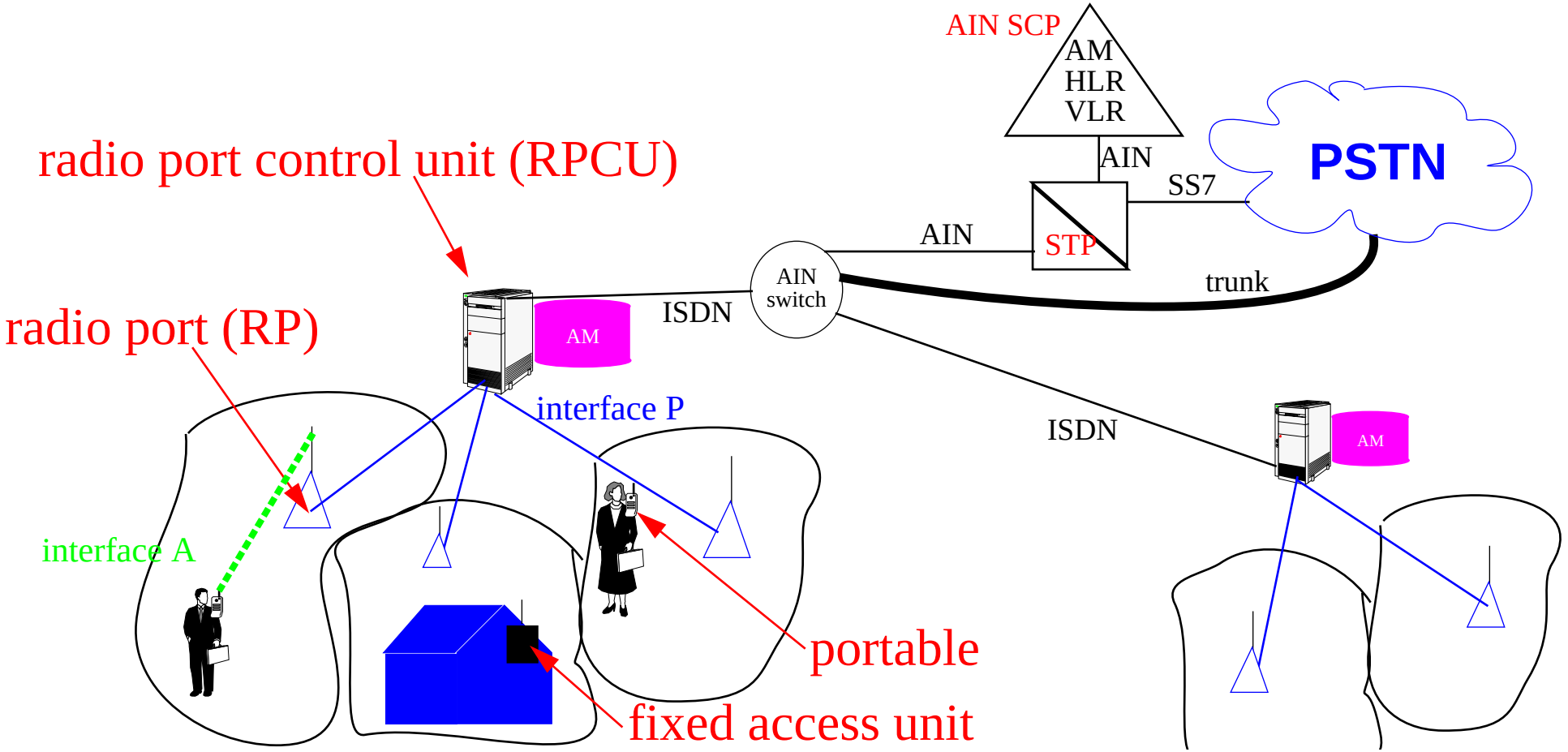


Figure 6: PACS Architecture

Access Manager (AM)

The access manager in the 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-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 text often refers to this as the AIN 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 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 authentification - **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 SCP

Provides service logic, databases, and operations to support:

- HLR
- VLR
- AM
- AuC

Communications:

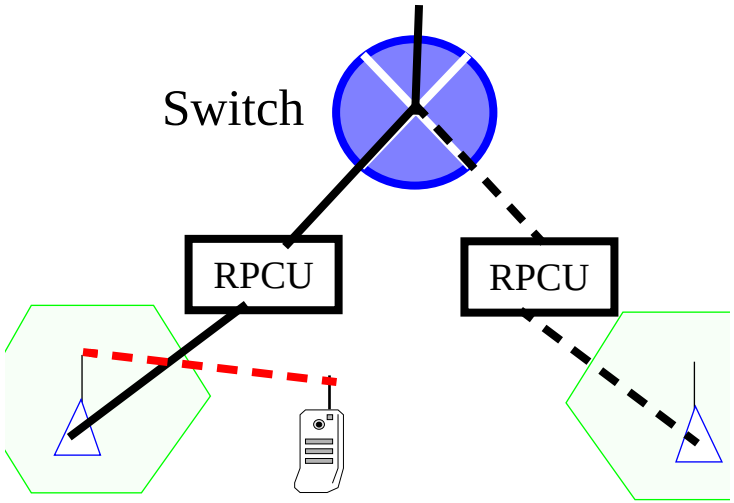
- with the switch AIN TCAP
- with external PCS databases via IS-41 protocol

PACS Intersystem Handoff

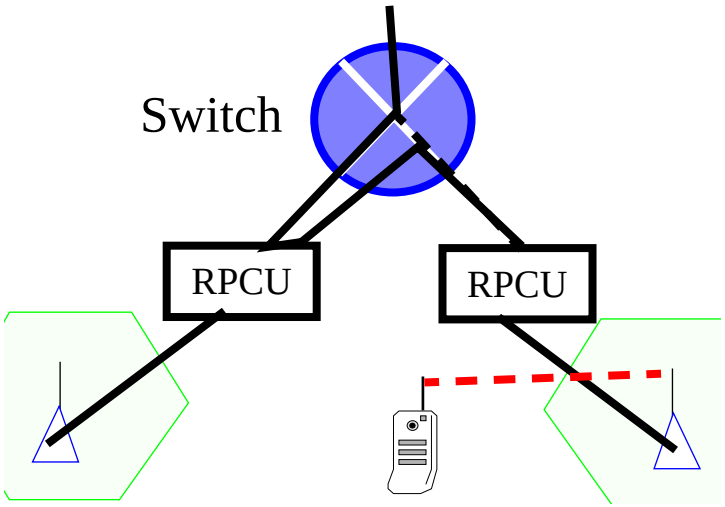
PACS Intersystem Handoff/automatic link transfer (ALT) follows IS-41 anchor switch approach.

3 alternative inter-RPCU handoff methods

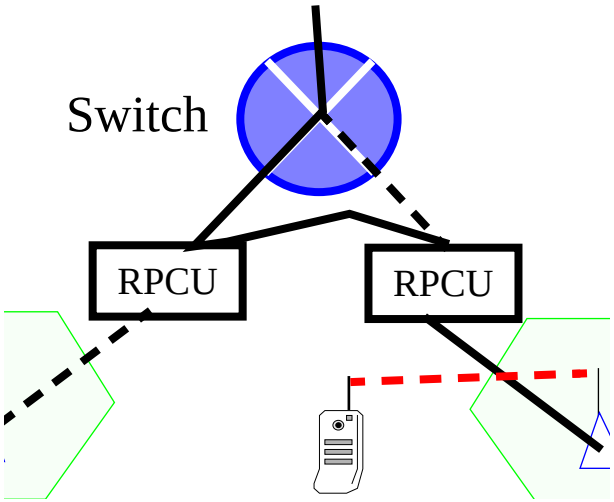
a. Before ALT



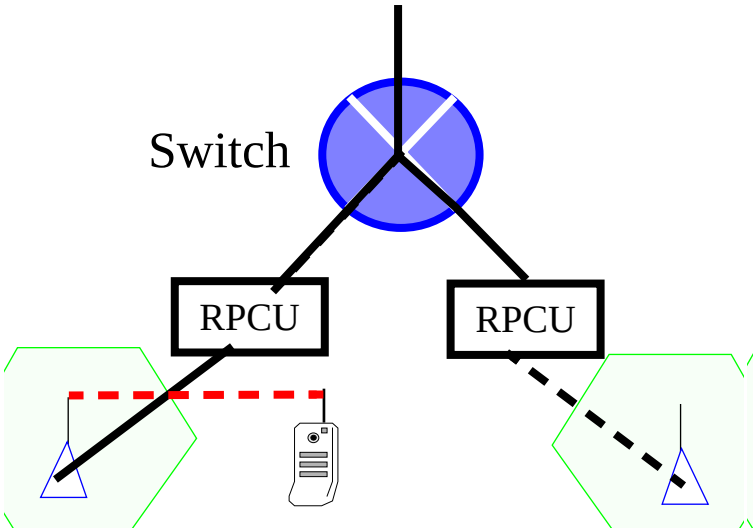
b. After ALT (Switch Loopback)



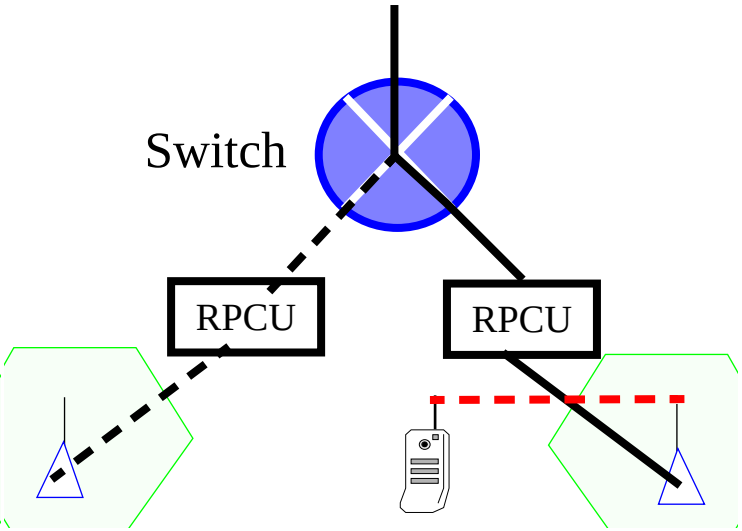
c. After ALT (Direct Connect)



d.During ALT
(Three-Way Calling Connections)



e. After ALT
(Three-Way Calling Connections)



CDPD

In 1992, AT&T Wireless Services developed cellular digital packet data (CDPD) protocol, a data-only protocol that (re-)uses the AMPS or IS-136 network. Packets (typically some 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 networks 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.

Motivation for CDPD

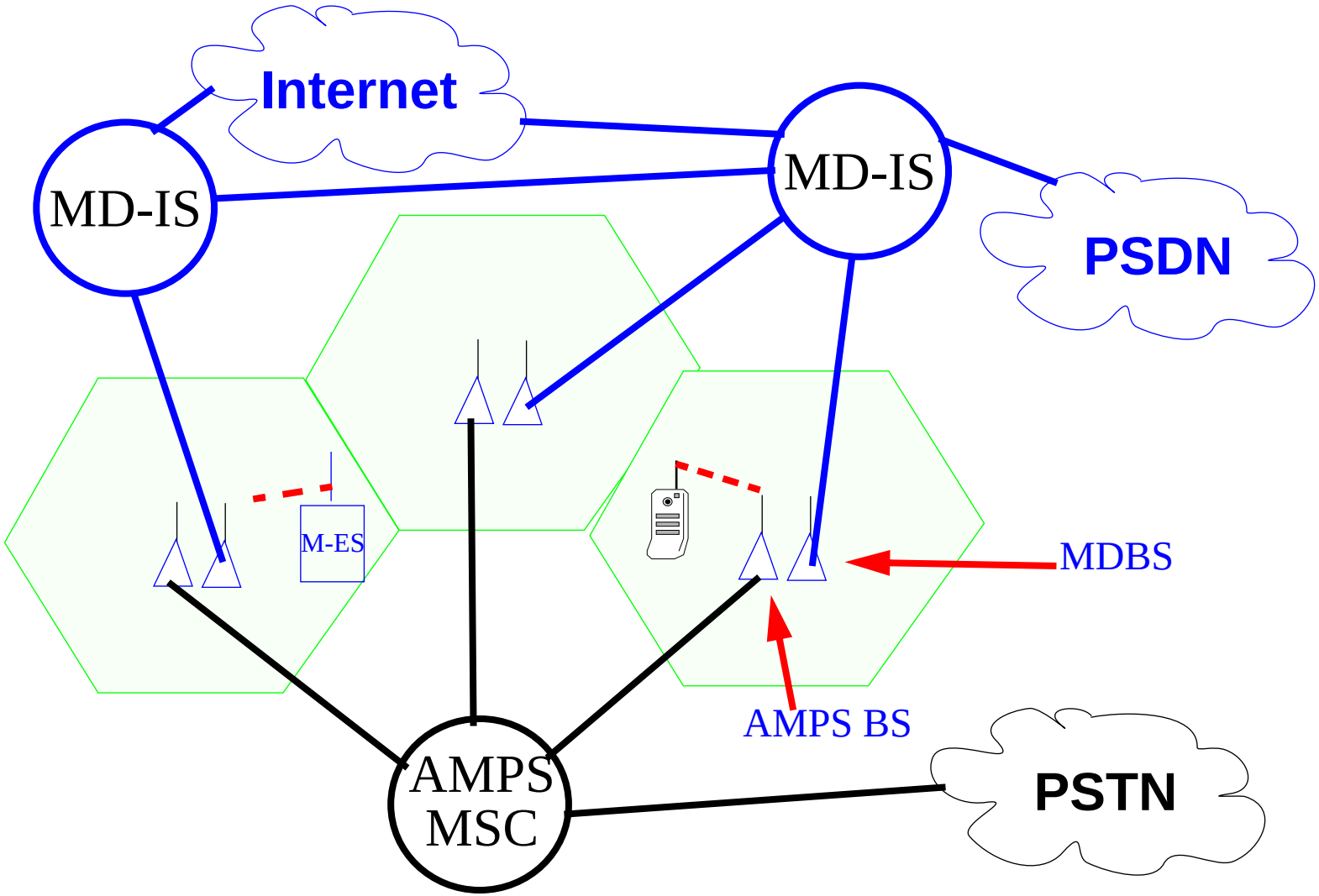
- Most traditional cellular systms (such as AMPS) are unsuited for packet data
  - Long call setup times - many seconds (vs. CDPD with from under 1 to 4 sec)
  - Modem handshaking required - this modem training can take more time than the data transfer time!
  - Analog providers already have AMPS allocation
- Re-use AMPS channels to provide data service.
  - Must not interfere with existing analog service (i.e., 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	tranditional non-CDPD host	
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 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

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 there is data for it, it send 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) {a Mobile IP **Home Agent**}.

Home MD-IS keeps **location directory** of the MD-IS currently serving each of its mobiles

Each MD-IS keeps a registration directory listing currently visting mobile (Mobile Serving Functon (MSF)) {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 handles 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, …
- Handheld/laptop IP access

Price Plans- 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.

http://www.navtrak.net/technologies.html

Wireless WebConnect!, Inc., *http://www.wwc.com/press/press20010806.html*

$59.95	unlimited local usage plus 400 KB of usage in non-local areas (roaming)
$129.95	unlimited local usage plus 1500 KB of roaming
$199.00	unlimited local usage and up to 3000 KB of roaming.

http://shop.store.yahoo.com/dreampages/novwirmin540.html

$29.99	“Handheld Local Unlimited Plan” unlimited local usage in areas where AT&T operates wireless data, $0.05/kbyte when roaming
$54.99	AT&T’s PC Card Local Unlimited Plan - if you load an OS other than PalmOS or Pocket PC

Operators and coverage maps

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

Further reading

CDPD

[8] 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

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

[10] Sun Jong Kwon, Yun Won Chung, and Dan Keun Sung, “Performance Analysis of CDPD Sleep Mode for Power Conservation in Mobile End Systems”, IEICE Transactions on Communications, VOL. E84B, no. 10, Oct. 2001
http://cnr.kaist.ac.kr/~ywchung/paper/APCC2001sjkwon.pdf

[11] 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