Cellular Networking Perspectives

David Crowe [Editor] • Phone: 1-800-633-5514 • Fax: 403-289-6658 Vol. 5, No. 7, July 1996

In This Issue...

Perspectives by Email!

We will soon be starting a beta trial for distributing Cellular Networking Perspectives by email. If you would like to participate, please email Muneerah Vasanji at cnpsales@cnp-wireless.com. We will send volunteers one or two sample email newsletters and ask that you fill out a short survey giving your impressions of alternative distribution methods.

Look forward to your next issue on: August 1, 1996

IS-41 Rev. C Update: Name Change and Prioritization

IS-41 Rev. C will soon no longer be an Interim Standard, but a full ANSI standard. Unfortunately, this means that its name will change. Once the ANSI standard (currently in the ballot process) is approved for publication, you will have to get used to the new moniker ANSI/TIA/EIA-689. This may mean that IS-41 Rev. D will never appear, as such, but probably a revision of ANSI/TIA/EIA-689 instead.

Whatever it is called, IS-41-C is big, weighing in at around 2,000 pages. The CTIA has recognized that manufacturers and carriers will implement its capabilities in stages, and are concerned that this may lead to incompatibilities. They released a memorandum on January 29, 1996 that categorizes IS-41-C features as high, medium or low priority.

High Priority Features

- Call Delivery
- Calling Number Identification Presentation (CNIP) and Restriction (CNIR)
- Message Waiting Notification (MWN)
- PIN (both control channel and voice channel variants)
- Voice Message Retrieval (while roaming)
- Authentication
- Triggers (allowing an HLR query during call processing for a roamer)
- Short Message Service
- CDMA-Analog handoff

Medium Priority Features

- Call Forwarding (busy, default to voice mail, no answer and unconditional)
- Call Waiting
- Extension phone services (flexible alerting and mobile access hunting)
- Preferred language
- Selective Call Acceptance
- Three Way Calling
- Power Down Registration
- CDMA-CDMA Handoff
- Priority Access & Channel Assignment (PACA)

Low Priority Features

- Call Transfer (controlling party drops out of call)
- Conference Calling (more than 3 parties)
- Do Not Disturb
- Password Call Acceptance (poor man's call screening)
- Remote Feature Control (e.g. call forwarding a mobile from a hotel or pay phone)
- Voice privacy

Most of these features are described in more detail in the October, November and December 1993 issues of *Cellular Networking Perspectives.* ❐

Quote of the Month

"We believe authentication will end fraud."
Mike Redden,
AT&T Wireless Services,
quoted in USA Today

Cellular Networking Perspectives (issn 1195-3233) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cr. NW, Calgary AB T2N 3W1, Canada. Phone: 1-800-633-5514 or 1-403-274-4749. Fax: 403-289-6658. Subscriptions: CDN$300 in Canada (incl. GST), US$300 in the USA and US$400 elsewhere. A surcharge of up to US$200 per year is required for faxing to international subscribers. Payment by cheque, money order or American Express. Issues are faxed or mailed 1st class. Copies: Subscribers may make up to 10 copies of each issue. Rates available for more copies. Discounts: Educational & Small business 25% off any order, by mail only. Back Issues: Phone for price list and list of contents.

Life on the Border, Part III: The Rearguard

The major line of defence when border cell problems are encountered in cellular systems is inter-system paging, described in the June, 1996 issue of *Cellular Networking Perspectives*. This defence, however, does not alleviate every type of problem, and three other defences are available:

1. 'Simultaneous' Registration Discrimination

   This tool assists with multiple access problems (i.e. the same message being received by two different control channels) and internal network race conditions (messages arriving out of order because they traverse different network paths to a common point, such as an HLR).

2. Mobile Marking

   By marking a mobile for special treatment after it originates a call without first registering, the subsequent loss of incoming calls can be reduced in likelihood. The special treatment is to do more extensive inter-system paging for such mobiles. This technique has nothing in common with the method dogs use to mark trees and posts on the border of their territory.

3. Authentication Coordination

   This solution, introduced in IS-41 Rev. C, solves an important (and recently introduced) border cell problem relating to the random numbers used in CAVE authentication. It is an important solution to prevent fraudsters from taking advantage of border cell anomalies to circumvent authentication.

'Simultaneous' Registration Discrimination

A common problem in real-time and distributed computer systems (of which cellular and PCS networks are just one example) is a 'race condition', that occurs when two events occur at nearly the same time and conflict with each other, possibly simply by being handled in a different order from which they were generated due to transmission delays.

Registration race conditions can occur either when the same registration is detected by multiple cells (see Figure 1) or when two or more registrations occur in rapid succession (see Figure 2). Unfortunately, the natural inclination of the network is to handle the situation in the worst possible way.

One Registration Heard by Multiple Cells

In a radio based system it is possible to constrain, but not train, transmitted signals. Any message, including a registration, may be received by several cells other than the intended one. Cells that are 'next door' neighbours will not hear the signal because their control channels are at different frequencies. However, with the limited number of control channel frequencies, some fairly close cells will hear the registration, often at a reasonable signal strength. The analog cellular standards (e.g. EIA/TIA-553, IS-91) allow some discrimination by providing four Digital Color Codes (DCC) that allow a base station to ignore most erroneously received messages. This number is increased to 60 in more recent analog and all digital standards. However, particularly with the older standards, registration messages can still be accepted by multiple cells.

This situation can cause two different problems for an HLR. One is that two IS-41 RegistrationNotification messages are received by the HLR. If the false registration is received first, it can cause the serving MSC/VLR to erroneously forget about the mobile. If the false registration is received second, it will cause the HLR pointer to be set incorrectly. What is more likely, however, is that the HLR only receives one RegistrationNotification - the false one! This situation arises if the mobile is already registered in the system that it was aiming the registration at. This system need not bother the HLR with a registration, since the HLR already knows where the mobile is. The HLR, being ignorant of this registration, accepts the false registration and causes a cancellation at the true serving system. Although the scenarios can be quite different, the result is that the mobile is lost, and calls cannot be delivered.

Rapid Registration Repetition

A variation on the one-registration multiple-cell problem occurs when a mobile registers more rapidly than it takes the IS-41 messages to traverse the network (see Figure 2). The worst situation occurs when a mobile is registered in one system (CS-B.1 in Figure 2) and then, moving into a coverage hole, registers in the best cell it can find (in a different system). Almost immediately, the new cell is lost and the mobile returns to the old cell. This can also result in a lost mobile, as the true serving system may, again, decline to notify the HLR. The HLR will see one registration, and cancel the registration in the current serving system. The serving system will see a registration, followed quickly by a cancellation from the HLR, which it will obey. Consequently, the HLR, and both MSC's, believe that the mobile has moved. Only the mobile knows which system it really is in until it registers again.

Solutions

The solution to multiple registration problems is to nest the RegistrationCancellation message within the IS-41 RegistrationNotification (see Figure 3). This gives the current serving system an opportunity to use the accompanying signal strength of the access and the time of arrival to discriminate between 'good' and 'bad' registrations. For example, a RegistrationCancellation received one-tenth of a second after a local re-registration (which may not be passed on to the HLR) may be ignored by a serving system, but would have been accepted if received 10 seconds after the most recent registration. TSB-65 and IS-41 Rev. C allow the signal strength of a registration (or whatever type of access triggered an implied registration) to be included in registration messages. Weak registrations may be rejected.

If a RegistrationCancellation is rejected by a serving MSC/VLR, the HLR will also reject the registration attempt.

Figure 1: One Registration Heard by Multiple Cells

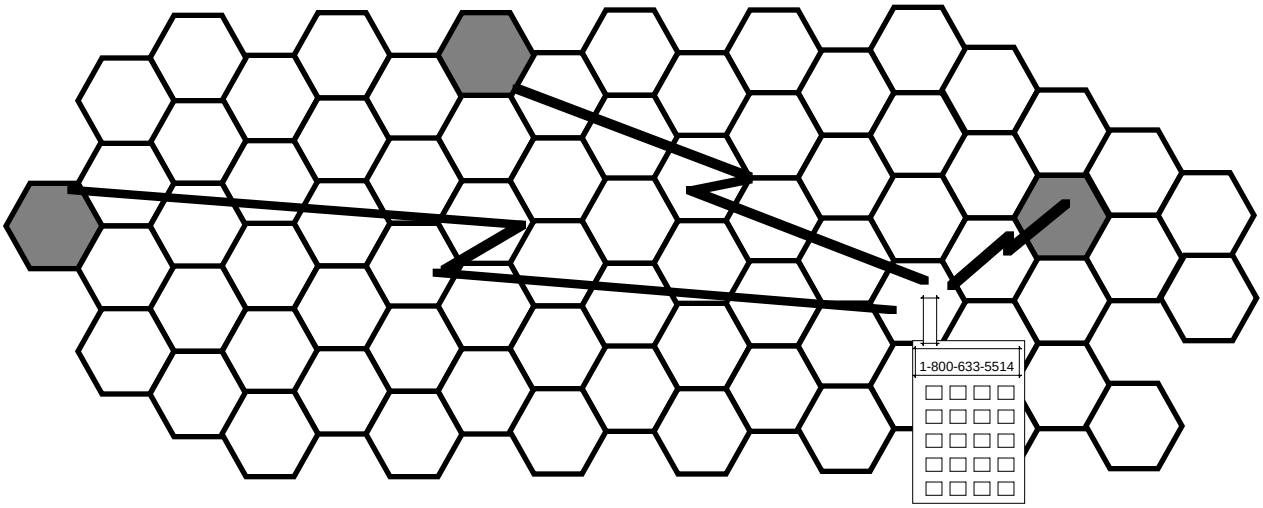


Figure 2: Rapid Registration Repetition

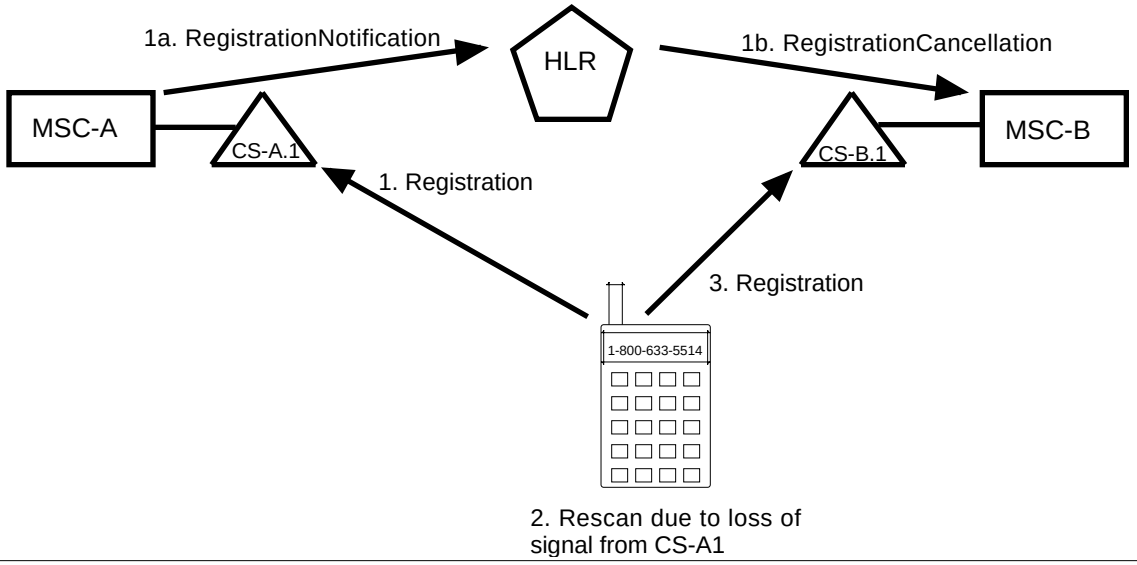
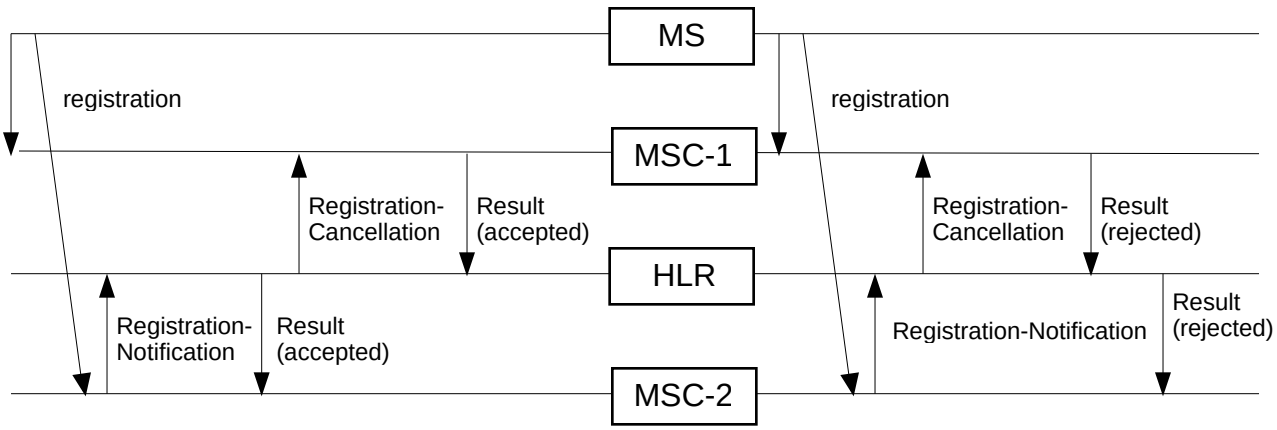


Figure 3: Nested RegistrationCancellation



Before TSB-65/IS-41-C:
HLR accepts registration without hesitation even when it shouldn't

TSB-65 and IS-41-C:
Old serving MSC is given a chance to reject an erroneous registration cancellation

Mobile Marking

If a mobile originates a call in a system that it is not registered in, it may become lost after the call is over, resulting in an inability to deliver calls to it, unless inter-system paging is performed. This problem can be predicted and, by marking the mobile for special treatment, inter-system paging can be undertaken with greater enthusiasm.

The problem arises due to the mandatory rescan that occurs when a mobile originates a call. If the mobile rescans into a system it is not registered in, it will originate a call anyway. This system will treat the origination as an implicit registration, in order that call waiting work correctly during the call. The mobile does not consider an origination to be equivalent to a registration, however.

Consequently, at the end of the call, if the mobile stays in the system that it is registered in (where it originated the call), it will register unnecessarily. While that is not a problem, if the mobile rescans back to its previous serving system (where it still thinks it belongs), it will not register. Thus the mobile is lost.

This can be detected by the system that supported the origination by marking the mobile's record for special treatment. If a registration (or any other sign of the mobile's presence) is received, special treatment can end. However, if a call delivery attempt is made while the mobile is still marked, inter-system paging should be given priority, as local paging is probably futile.

Authentication Coordination

Our friend, the rescan problem (see the May, 1996 issue for more details), can cause havoc with the new technology of authentication in border areas. TIA CAVE authentication (see the December, 1995 and January, 1996 issues for more details) relies on a global challenge broadcast from an authenticating cell to all mobiles, using a 32-bit random number, known as RAND. This number can be changed at intervals to increase the security of authentication as the response to the RAND challenge (known as AUTH) will be unpredictably different for each mobile and for each value of RAND. If a rescan occurs as part of normal call processing, a mobile can use the a RAND from a neighbouring cell to generate AUTH and be denied service. If service is allowed in border areas even with an invalid AUTH, an enormous fraud hole would be opened.

This problem is somewhat alleviated by the mobile transmitting the 8 most significant bits of RAND (known as RANDC) back to the base station as a check. However, this does not completely solve the problem, and actually increases the number of different sub-problems:

1. RANDC = 0

   This is a sign that a mobile has not obtained RAND from any base station, and is using a value of 0 as a substitute.

2. RANDC Match, RAND Mismatch

   Just because the RANDC sent from a mobile matches a portion of the base station's RAND does not mean that the full values match! In this case, authentication will fail.

3. RANDC Match, Other Authentication Failure

   An authentication failure may be due to other reasons, including attempted fraud. However, this case cannot be easily distinguished from case #2.

4. RANDC Match, Authentication Succeeds

   If authentication succeeds, it is known that the mobile and base station used the same value of RAND.

5. RANDC Mismatch

   The MS has definitely picked up a value of RAND from another BS. Authentication will always fail in this case, and should not even be attempted, unless the matching value of RAND that the mobile used can be determined.

There are several solutions to these RANDC problems:

1. Don't transmit a RAND with the RANDC bits zero.

   The 8 bits of RAND that will be used as RANDC should never be zero, to avoid confusion with a RAND/RANDC value of zero, which should be reserved to indicate that the mobile did not have time to receive a value of RAND.

2. Monitor RANDC=0

   Mobiles that consistently use RANDC=0 may be attempting fraud, and should be monitored.

3. Synchronize RAND with Neighbours

   IS-41 Revision C (not TSB-51) provides a new transaction (Random VariableRequest) that is specifically designed to allow the efficient coordination of RAND values with neighbours to avoid RANDC overlaps, and to obtain the values of the neighbour's RAND.

   This message can also be used pre-emptively, every time a value of RAND is chosen, to ensure that no neighbouring system is using the proposed value. It can also be used when a RANDC mismatch is detected, to determine which neighbouring system is using that value. If used judiciously, the RAND and RANDC values of all neighbouring systems will be coordinated without a significant amount of inter-system messaging.

   Alternatively, a UniqueChallenge (see December 1995 issue) can be issued every time a RANDC mismatch or other authentication failure occurs.❐

Status of IS-41 Rev. B Implementation

Cellular Networking Perspectives

Editor David Crowe • Phone: 1-800-633-5514 • Fax: 403-289-6658 *Last Published 02/96*

Vendor1	Vendor2	Status	Date	Type	Location
Alcatel SEL	EDS PC	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
	GTE TSI	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
	Lucent	Commercial	2Q'95	H V D S	Orlando, Florida (BellSouth)
	Motorola	Commercial	2Q'95	H V D S	Richmond, Virginia (BellSouth)
	Nortel	Commercial	2Q'95	H V D S	Mobile, Alabama (BellSouth)
Astronet*	Lucent	Commercial	2Q'96	V DX	Hoffman Estates, IL (Ameritech)
Celcore	Alcatel SEL	Commercial	05/96	V D S	Yorkville, TN
	Ericsson	Field Trial	09/95	V D S	Chicago (Cellular One)
	Lucent	Field Trial	09/95	H V DX	Cleveland, Ohio (GTE Mobilnet)
	Motorola	Field Trial	12/95	V DX	Little Rock, AR
	Nortel	Field Trial	05/96	V D S	Seattle (Westem Wireless)
	Tandem (HLR)	Lab Trial	11/95	V D S	Seattle(AT&T-WS)
EDS PC	Alcatel SEL	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
Ericsson	EDS PC	Planning		V X	*Location not announced*
	Motorola	Field Trial		H V D S	*Location not announced*
GTE TSI*	Alcatel SEL	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
	Others	Commercial	3Q'95	V DX S	*Rev. A plus TSB-55 compatibility*
Harris	NACN	Field Trial	07/96	V DX	All NACN locations
Lucent	Alcatel SEL	Field Trial	03/95	H V D S	South Florida (BellSouth)
	NEC	Commercial		H V D S	Brazil
	Nortel	Planning		H V DX T	*Location not announced*
Motorola	Alcatel SEL	Commercial	2Q'95	H V D S	*Multiple locations*
	NEC	Commercial		V D S	Brazil
NEC	Lucent	Commercial		H V D S	Brazil
	Motorola	Commercial		V D S	Brazil
Nortel	Alcatel SEL	Commercial	4Q'95	H V D S	Orlando, FL & Jackson, MS
	Lucent	Lab Trial	TBD	H V DX	Windsor (Bell Mobility)
	NEC	Commercial	2Q'94	H V D S	Brazil
Plexsys	Ericsson	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
	Lucent	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
	Motorola	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
	NEC	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
	Nortel	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
Telos	Lucent	Field Trial	3Q'96	V D S	Vancouver, BC (BC Tel)
	Nortel	Lab Trial	04/'96	V D X	Vancouver, BC (BC Tel)

Explanation:	*	This vendor is using IS-41 Rev. A with TSB-55 for compatibility.
	Status:	Development, Planning, Lab Trial, Field Trial or Commercial.
	Date:	Date of actual or expected completion of listed phase of testing.
	Code	Capability Being Tested
	H	Handoff forward and back ('+' indicates path minimization & flash handling)
	V	Validation ('+' indicates authentication using TSB-51).
	D	Includes call delivery.
	X/S/I	X.25 / ANSI SS7/ ITU-T(CCITT) SS7 datalink protocol.
	T/C	Uses TDMA (IS-54, IS136) / CDMA(IS-95) digital mobiles.
	Location:	Location of test and carrier. Usually listed for first trial only.

Note: IS-41 Rev. A systems are no longer listed as Vendor2, for space availability reasons.

TIA TR-45.1
Analog Air Interface
Standards Report

Editor David Crowe • Phone: 1-800-633-5514 • Fax: 403-289-6658 *Last Published 01/96*

Analog Air Interface Standards - First Generation

Standard	Description (not the official title)	Comment
IS-3 (Rev. A,B,C,D)	**Original Analog Air Interface Standard (see EIA/TIA-553-0)**	**Rescinded 09/89**
EIA/TIA-553 Rev. 0	Analog Air Interface Standard	Published 09/89
IS-19-B	**Mobile minimum performance standards**	**Published 06/88**
IS-20-A	Base Station minimum performance standards	Published 06/88
TSB-35	Cellular mobile receiver dynamic range	Published 04/92
TSB-39	Message Type Assignment for Extended Protocol	Published 03/93

Analog Air Interface Standards - Second Generation

Standard	Description (not the official title)	Comment
EIA/TIA-553 Rev. A	**Reaffirmation of EIA/TIA-553 (including authentication)**	**In press**
IS-88	Narrowband (3:1) analog air interface ("NAMPS")	Published 02/93
IS-89	IS-88 base station performance standards	Published 02/93
IS-90	IS-88 mobile performance standards	Published 02/93
IS-91 Rev. 0	Analog air interface (including "NAMPS" and Authentication)	Published 10/94
IS-94	In-building analog air interface ("FreedomLink")	Published 05/94
IS-680	**Personal ("cordless") base station PSTN interface**	**Published 05/96**
TSB-70 Rev. A	**Cross Reference for FSK Control Channel**	**Development**

Analog Air Interface Standards - Third Generation

PN/SP	IS/TSB	ANSI	Description (not the official title)	Comment
PN-3476	**IS-91-A**		**Revised version of IS-91 (including IS-94, IS-680 (cordless) and sleep mode)**	**In Press**
SP-3495	**IS-19-C**	**EIA/TIA-690**	**Mobile minimum performance standards**	**Ballot**
PN-3477	**TSB-71**		**IS-94 Enhancements & Issues**	**Published 10/95**
PN-3597	**IS-20-B**		**Base Station minimum performance standards**	**Development**
SP-3665		**EIA/TIA-691**	**ANSI version of IS-91-A(without IS-680 cordless)**	**Ballot**
PN-3668			**Upbanded (1800 MHz) NAMPS**	**Development**

Analog Air Interface Standards - Fourth Generation

PN/SP	IS/TSB	ANSI	Description (not the official title)	Comment
SP-3598		**EIA/TIA-553-A**	**Analog standards, with authentication, w/o NAMPS**	**Ballot**
PN-3610	TSB-70-A		Updated version of TSB-70 cross reference	Ballot
PN-3666	**IS-91-B**		**Revised version of IS-91 (including IMSI, PCS band support, voice privacy, over-the-air-activation, priority access, 9-1-1 and voice-paging)**	**Development**
PN-3667	**TSB-xxx**		**EIA/TIA-553-A without authentication (for international distribution)**	**Development**
PN-3668	**IS-xxx**		**IS-91-Awith 1900 MHz frequency capability**	**Development**

Note: 1. IS- Interim Standard, TSB- Telecommunications Systems Bulletins, PN- Project Number, SP- ANSI Standards Proposal, J-STD- TIA/ATIS Joint Technical Committe standard.

2. **Bold Type** indicates modification since previous publication.