Cellular Networking Perspectives

Editor David Crowe • Phone 403-289-6609 • Fax 403-289-6658 Vol. 2, No. 4 April, 1993

In This Issue ...

IS-41 is a large, complex and still growing standard that facilitates mobility management for roamers in the AMPS cellular network: handoff, validation, call delivery etc. This issue provides an overview of IS-41, which will be the basis for later, more detailed discussions.

The TIA TR45.2 sub-committee is currently working on a large number of standards and TSB's. The current status of each document is summarized below.

TR45.2 working group VI, which studies issues related to the international applications of cellular, is discussed this month in our continuing examination of the seven working groups that make up this subcommittee. WG VI has recently been revitalized by the appointment of a new chairperson.◊

TR45.2 News

There are several standards documents currently under development by the TIA TR45.2 sub-committee responsible for standardization of non-radio cellular interfaces. The status of each of the most important unpublished documents following the April TR45.2 meeting was:

Authentication, Signaling Message Encryption and Voice Privacy• Describes modifications to IS-41 Rev. B handoff and call delivery procedures to support IS-54 authentication and encryption of roamers. In publication as *TSB-51*.

IS-41 Rev. A Test Plan•An application level test plan for IS-41 Rev. A and IS-53 Rev. 0. *Published on March 29, 1993 as TSB-56.*

TechNotes•Will resolve several ambiguities in IS-41 that have resulted in incompatibilities between implementations of IS-41 Rev. A. Remaining open issues are being reviewed by a WG II task force before preparation of a document for publication as *TSB-41*.

Border Cell•A draft document that will resolve several problems that occur on the border of cellular systems is being reviewed by WG I. These extensions to IS-41 will be published as *IS-87*.

Rev. A Compatibility• Procedures to allow IS-41 Rev. A implementations to be forward-compatible with Rev. B. Remaining open issues are being resolved by WG II. The document will be published as *TSB-55*.

IS-41 Rev. B Test Plan• An application level test plan for IS-41 Rev. B is being developed by a WG II task force. The first draft is currently being reviewed for publication as *TSB-42*.

IS-41 Revision C• Work on this revision to IS-41 is on the back burner until all the TSB's affecting IS-41 Rev. B are completed. Some work is going on in the development of IS-41 changes to support IS-53 Rev. A features, CDMA mobiles and TDMA data terminals.

Subscriber Features•Draft text for a major revision to the cellular Features Description standard is being reviewed by WG V for publication as *IS-53 Rev. A*.

PSTN Interface•A definition of both the analog (i.e. MF signaling) and digital (SS7 signaling) interfaces required to connect MSCs to the PSTN is being developed. This document may supersede Bellcore TR-NPL-000145 (1986) which is currently used to define analog interfaces for cellular. WG VII has scheduled publication for 4Q'93.

Intersystem Non-Signaling Data Communications• 600 pages of draft text describing procedures and messages for the on-line transfer of call detail records are being reviewed by WG IV with publication scheduled for mid-year. The two main purposes of call detail record transfer are faster and more accurate billing and faster fraud detection.◊

IS-41 Explained

IS-41 is the ugly duckling of TIA cellular standards. For several years this cellular networking standard has been painstakingly developed by an “obscure group of telecommunications experts”, as the TIA TR45.2 subcommittee once was called. While close attention was being paid to the analog air interface and then to TDMA digital and then to CDMA digital, a small but increasing number of industry insiders were realizing that the future of cellular was more in the networking of systems than in the specific choice of air interface. Whether TDMA or CDMA, or a mixture of both, becomes the air interface of the future is not a critical issue for the industry at large. However, the intelligent networking to support enhanced services and control fraud is necessary for digital cellular, unlike its simpler analog counterpart, to succeed. This growing realization accounts for the increasingly higher profile of cellular networking technology, such as IS–41.

This issue of *Cellular Networking Perspectives* attempts to correct the oversights of the past by focussing on the important features that IS-41 provides, and how it provides them. We will avoid techno-babble and unnecessary acronyms (UFA’s) and give a succinct but accurate account. Let us know how well we have succeeded.

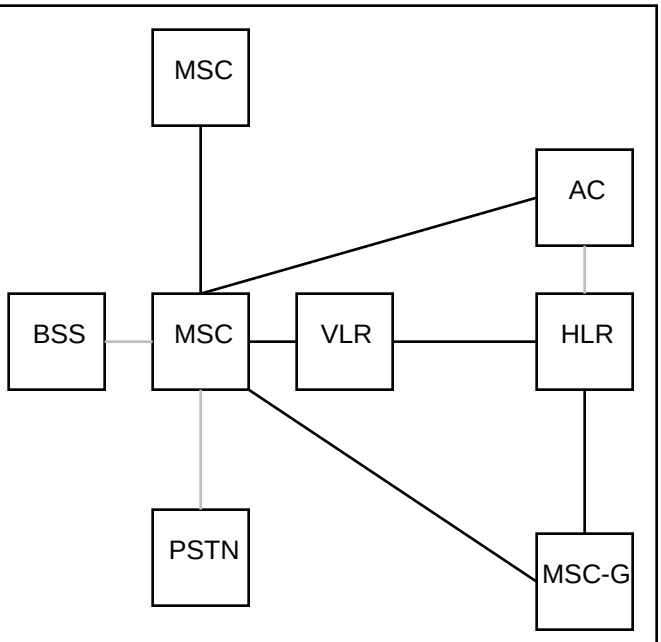
Our discussion of IS-41 is divided into several sections:

- An overview of the standard.
- Document structure.
- Revisions and related documents.
- Compatibility.
- Features of IS-41.
- Protocols and Networking.
- Field trials and testing.

IS-41 Overview

IS-41 provides inter-system operations between elements of a cellular network that uses one or more of the TIA air interfaces: Analog (TIA/EIA-553), TDMA digital (IS-54) or CDMA digital. IS-41 implements these operations by defining data messages that may be sent between logical network elements, and procedures for using its messages.

The network elements relevant to cellular networking are described in a *Network Reference Model*. They are called *logical* because they do not have to exist as separate physical entities, but may be combined. IS-41 allows, for example, an MSC and a VLR to be combined, as they usually are. The network reference model shown below has been simplified from the one normally used in TIA discussions. In this diagram solid lines indicate interfaces currently standardized by IS-41, dashed lines indicate interfaces not standardized currently (e.g. the MSC/BSS interface) or being standardized outside IS-41 (e.g. the MSC/PSTN interface).



IS-41 Network Reference Model

The meanings of the acronyms for network elements in the diagram are listed below. Names of elements with IS-41 interfaces are in **bold** type):

AC Authentication Center. Contains the secret keys and other information required by authenticating mobiles. The AC/MSC interface (physically realized via the HLR and VLR) was first standardized in TSB-51. The AC/HLR interface is currently not being considered for standardization.

BSS Base Station Subsystem. The MSC/BSS interface is not under consideration for standardization in North American cellular.

HLR Home Location Register. The repository for master subscriber records.

MSC Mobile Switching Centre. A system that switches calls involving mobiles.

MSC-G Gateway Switching Centre. A switch that can locate mobiles and route to them directly rather than always through their home system.

PSTN Public Switched Telephone Network. The interface to the PSTN is currently being standardized by TR45.2 WG VII.

VLR Visitor Location Register. The repository for temporary roamer records in the visited system.

Document Structure

All revisions of IS-41 have been divided into the same 5 major sections:

IS-41.1 Functional Overview.

Describes the IS-41 Network Reference Model, defines terms and acronyms and includes a list of references.

IS-41.2 Intersystem Handoff.

Describes intersystem handoff procedures.

IS-41.3. Automatic Roaming.

Describes intersystem call delivery and remote feature control procedures.

IS-41.4. Operations, Administration and Maintenance.

Describes the procedures used to implement common channel signaling for inter-MSC trunks. These trunk management procedures are very similar to SS7 ISUP and are currently required only for intersystem handoff.

IS-41.5. Data Communications.

Describes the usage of the protocol layers beneath IS-41 and defines all IS-41 messages and parameters. Protocols beneath IS-41 are ANSI TCAP for transaction handling and message packaging and either X.25 or ANSI SS7 for reliable data transmission.

Back Issues Available

Back issues are always available. Major topics in recent issues are:

October, 1992
North American Numbering Plan changes, part II.

November, 1992
Inter-System Handoff, part I - Handoff Forward/Back.

December, 1992
Inter-System Handoff, part II - Path Minimization.

January, 1993
Inter-System Handoff, part III - Feature Interactions

February, 1993
Inter-System Handoff, part IV - New Air Interfaces. IS-41 Rev. 0 Field Trials

March, 1993
Wireless '93 in review. IS-41 Rev. A Field Trials

The price of a back issue is:

CDN$25 Canadian fax number
US$25 US fax number
US$30 Other fax numbers

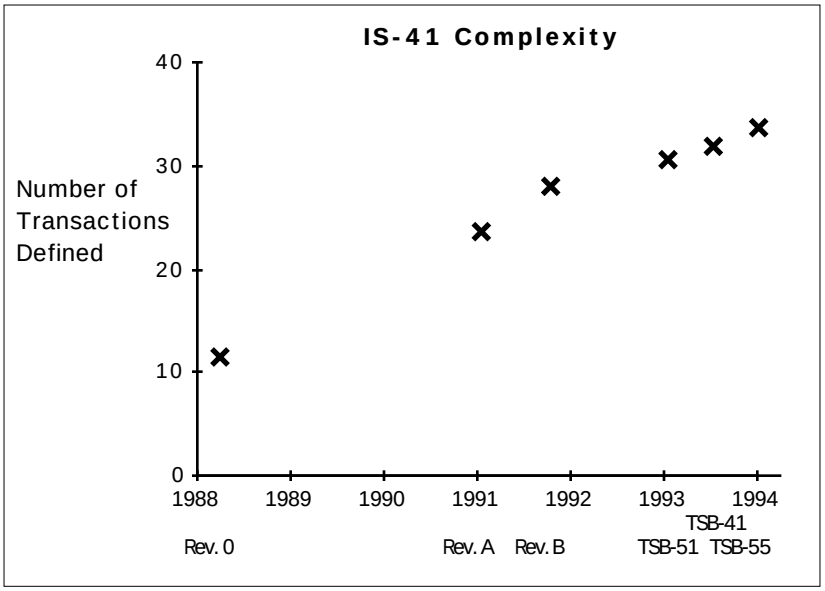
Subscribers may fax requests for back issues and be invoiced later.

Revisions of IS-41

IS-41 has been revised twice since Revision 0 was published in 1988. Both Revisions A and B added significant new functionality. Between revisions it has sometimes been necessary to release Telecommunications Systems Bulletins (TSB's) to clarify ambiguities in the standard or to add new functionality without the delays inherent in publication of a standard. The revisions of IS-41 and associated TSB's are summarized below:

Revision / TSB	Published	Description
IS-41 Rev. 0	Feb., 1988	Intersystem Handoff and Validation
TSB-27	unpublished	Clarification of Rev. 0 encoding
IS-41 Rev. A	Jan, 1991	Call Delivery and Enhanced Validation
IS-41 Rev. B	Dec., 1991	Enhanced Networking and Handoff
TSB-51	in press	Authentication and Voice Privacy
TSB-41	later 1993	Clarification of Rev. B
TSB-55	later 1993	Rev. A/B Compatibility
IS-87	later 1993	Border Cell Problems
IS-41 Rev. C	later 1993	New air interfaces (CDMA, etc.)

The increase in complexity of IS-41 over time is illustrated by the following graph showing the number of transactions at each stage in its development:



Compatibility Between Revisions

Ideally systems implementing different revisions of IS-41 should be compatible. While that has become the goal of TR45.2, it has not yet achieved.

IS-41 Rev. 0 started off on the wrong foot by using an unpublished version of TCAP. This made it incompatible with IS-41 Rev. A without custom conversion equipment. IS-41 Rev. A was published using standard ANSI TCAP, but without compatibility guidelines. These guidelines, first introduced into IS-41 Rev. B, guide the processing of IS-41 messages when the revision level of the sending system is not known. They also restrict changes that can be made to IS-41 that might create new compatibility problems. Compatibility considerations call for a great deal of care in designing the processing of incoming IS-41 messages. Unrecognized messages must be rejected but unrecognized parameters must be ignored, as they are probably being sent by a system at a higher revision level. A subset of these guidelines will be published as TSB-55 to allow IS-41 Rev. A systems to ensure compatibility with IS-41 Rev. B.

Even in IS-41 Rev. B there are still a few less serious compatibility problems that may need to be resolved in IS-41 Rev. C. As the experience of the industry with IS-41 upgrades grows, the ease of introduction of new functionality into the network should also grow.

IS-41 Features

IS-41 provides solutions for mobility management problems in the following areas:

- Intersystem Handoff
- Validation
- Call Delivery
- Remote Feature Control
- Authentication
- Voice Privacy
- Border Cell Problems

These features are provided in a fairly general way in IS-41, and can be applied to mobility management in other arenas than cellular, such as PCS.

Intersystem Handoff

Intersystem handoff was the first mobility feature standardized in IS-41, in Rev. 0. This was not because it was the most desired feature, but merely because it could be implemented with direct links between two neighbouring MSC's. The complex technical, business and regulatory issues of networking could be avoided. Intersystem handoff is important, however, as it improves the customer's perception of cellular service by providing fewer dropped or noisy calls in border areas.

IS-41 Rev. B and later TSB's enhanced handoff procedures beyond the basic handoff forward and backward defined in IS-41 Rev. 0. IS-41 Rev. B provided path minimization which, ironically, requires networking to reduce the facility usage of calls after several intersystem handoffs. Rev. B also included support for handing off TDMA mobiles and the capability to support call waiting and 3 way calling following a handoff. TSB-51 will allow voice privacy to be maintained after an intersystem handoff.

Validation

The designers of the first cellular systems, being honest people, gave little thought to one of the few modern industries that is growing as fast as cellular... Fraud. While a supposedly unalterable electronic serial number (ESN) was provided in each phone, no mechanism was provided to exchange MIN and ESN information for roamers, nor to detect falsification of an ESN. In the absence of standard solutions, GTE and Appex (now EDS PCC) were not long in providing kludgy but effective systems to validate the MIN and ESN in mobiles. However, these systems could only validate

after a call disconnected, and even then the delay before validation was very long, hours in some cases. Although IS-41 Rev. 0 specified only validation with a neighbouring system, it did provide it during call setup. GTE and EDS PCC were quick to develop proprietary enhancements to allow networking of Rev. 0 validation. This networking of validation can now be provided in a more standard way through IS–41 Rev. A and B.

IS-41 validation, as it penetrates the network, is gradually eliminating 'tumbling' fraud. This fraud technique provides an endless number of invalid MIN/ESN combinations to the system, relying on the slowness of the validation process to allow at least one call before the ESN is recognized as invalid. Then the tumbler only has to move on to the next MIN/ESN combination. Tumbling can be stopped if each MIN/ESN combination is validated before conversation. Cloning fraud is the only type of air interface fraud that is untouched by IS-41 validation, and remains a serious threat to the industry.

Call Delivery

Call delivery to roamers both solves a problem and creates a problem. It solves the problem of reaching someone whose exact location is unknown, but creates a financial burden for the subscriber who has to pay both airtime and long distance charges even for calls that they do not want to receive. But the problem solved is a problem solved, and the problem unsolved is an opportunity. Once new services are introduced that make the caller pay at least some of the costs, every roamer who wants to stay in touch will want the call delivery feature.

IS-41 intersystem call delivery occurs in three main phases:

- Tracking the roamer.
- Obtaining routing information.
- Routing the call.

Tracking a roamer requires the HLR subscriber record whenever a roamer appears in an MSC in a new VLR. The stimulus for this update is usually autonomous mobile registration, defined in all the cellular air interface standards, but may also be an origination or a termination through a roamer port.

Whenever an attempt is made to terminate a call to a mobile, the originating system has to obtain, via the HLR, a routing number from the visited system (VLR/MSC). This number, known as a TLDN (Temporary Local Directory Number) is just a phone number set aside from the visited system's stock, which will allow the PSTN to route the call correctly. If the mobile is currently busy, IS-41 allows the visited system to inform the HLR which can take an alternate action, such as forwarding to voice mail.

The last phase of call delivery does not involve IS-41. The TLDN is pulsed out to the PSTN, resulting in a call to the visited system. The visited system correlates the TLDN to the MIN of the roamer and completes the connection.

The TLDN method of call delivery is not the only method that could be used, but it is the most general. It also works within the equal access restrictions of most of the large cellular carriers.

Remote Feature Control

A little known feature of IS-41 is the ability for subscribers to activate and deactivate features such as call forwarding while roaming. Recognizing that feature control digit strings vary from system to system, IS-41 contains procedures to send feature digit strings back to the HLR for interpretation. This is known as ‘reachback’ feature control. The visited system, based on the response from the HLR, will either indicate success or failure to the subscriber, usually by a tone.

A large unresolved problem is that the TIA IS-53 feature specification recommends that any digit string starting with a single asterisk be treated as a feature control string. Yet these are the very patterns that are popular with radio stations and public service organizations for speed dial codes (e.g. *CG for the Coast Guard). Unless this problem is resolved some subscribers that try to activate call forwarding remotely will get the hit line at a radio station instead.

Authentication

The TDMA digital standard, IS-54, was not only intended to address the issue of greater capacity, but was also intended to provide greater protection against fraud. Its designers used encryption as the technology to up the ante on wannabe clone makers.

Authentication cannot be used without intersystem operations. IS-41 support (included in TSB-51) is required to pass encryption keys from the AC to the visited system or authentication responses from the visited system to the AC for validation. Authentication is more sophisticated than validation because terminals do not actually transmit their identification information, but use a sophisticated algorithm to respond to a numerical challenge in a way that shows indirectly that they possess the secret authentication keys. Clones are still possible, but the information they require is much harder to obtain and much more easily invalidated.

Authentication is not only supported in TDMA digital cellular (IS-54 Rev. B) but also in the upcoming CDMA and revised Analog specification (EIA/TIA-553 Rev. A).

Voice Privacy

Eavesdropping is fast becoming a concern of many cellular subscribers; not just Prince Charles and Lady Di. Digital cellular technology makes voice encryption possible using same algorithms as authentication. Again intersystem operations are required. Voice encryption masks have to be passed from the AC to the visited system by IS-41. Unlike authentication, which is completed during call setup, voice encryption has to be maintained during an entire call, necessitating that MSC’s exchange voice mask and other encryption data in IS-41 transactions during a handoff.

The TIA digital cellular standards, both TDMA and CDMA, not only allow voice encryption, but also the encryption of subscriber data, such as DTMF tones. This protects sensitive subscriber information such as voice mail passwords and telephone calling card numbers.

For a Subscription to Cellular Networking Perspectives, send your name, company, address and fax number, along with a cheque or money-order to:

Cellular Networking Perspectives
2636 Toronto Crescent NW
Calgary, AB T2N 3W1 Canada

1 year subscription (12 issues):

Canada	CDN$250.00
USA	US$250.00
Other	US$300.00

Subscribers are licensed to copy within their company or organization as long as credit is given.

Voice and subscriber data encryption for roamers are supported in TIA TSB-51 along with authentication.

Border Cell Problems

Intersystem handoff can be considered as the most obvious example of a border cell problem, a problem that only occurs on the boundary between two cellular systems. Although handoff is accepted as a basic characteristic of cellular, a number of more obscure problems have been discovered in some border areas. Most are due to flaws in the analog air interface standard (EIA/TIA-553), several of which have unfortunately been carried across to its TDMA and CDMA successors.

As an example of a border cell problem, mobiles normally register in a system before originating a call, but in a border area may actually originate in a neighbouring system. At the end of the call the mobile will not register again if it rescans back to the system it is registered in. This is because mobiles do not consider an origination a registration event. This creates uncertainty in the location of the mobile, an uncertainty that can more accommodated more easily by allowing paging in more than one system at a time than by recalling 11 million mobiles. IS-41 solutions for this and other border cell problems are described in IS–87, currently under development by TR45.2 WG I.

Protocol Layers

IS-41 is built on top of several other protocol layers, each with a distinct function. Directly below IS-41 is TCAP, an ANSI transaction control and message packaging standard. For the bottom layer there is a choice of either X.25 or SS7. X.25 was used for all Rev. 0 trials, but SS7 is more suitable for the networking environment of IS-41 Rev. A and particularly Rev. B and beyond.

TCAP is used create transactions and package IS-41 messages. Messages can either be an *Invoke* to initiate a transaction, a *Return-Result* to report successful completion, an *ErrorResult* to report unsuccessful completion or a *Reject* to indicate an unusable message. Within each message TCAP provides separate identification and packaging for each parameter included. TCAP allows for simple handling of optional parameters (just by omitting them) and, if used carefully, for compatibility with future revisions of IS-41 that might define new parameters.

The choice of X.25 or SS7 is a tradeoff between cost and complexity on one hand and capacity and functionality on the other. X.25 can run on cheap, low speed links but, because X.25 level 2 is used with IS-41, it can only directly connect two points, such as is required for intersystem handoff. SS7 is more useful, however, to connect the large number of cellular network elements required for validation and call delivery. Although the future IS-41 network may be based on SS7, access to the network will be either by SS7 directly or by X.25 through an intelligent gateway. This intelligence is to extract addressing information from the IS-41 application layer.

Field Trials and Testing

New revisions of IS-41 have traditionally been introduced into the field by testing,first in a lab environment and then in the field, every combination of vendor equipment that will be connected together.

These implementation procedures may change as the IS-41 network grows and the number of possible vendor to vendor connections increases. Emphasis in the future may be on individual vendor testing, a field trial with a limited number of other vendors and then use of the TSB-56 test plan by carriers and service providers to assure themselves that the IS-41 implementation works correctly.

Summary

IS-41 has become established as the only practical standard for mobility management with TIA cellular air interfaces. It is likely that, political considerations aside, it will become the mobility management protocol for PCS services as well. In future more services will involve terminal or personal mobility, or both. New services may well have to start by providing full roaming capabilities, because of the expectations developed by the cellular industry, and its provision of IS-41 technology to continually enhance roaming capabilities.◊

TR45.2 International Working Group VI

TR45.2 Working Group VI studies the international application of TIA cellular. Many countries around the world, particularly in South and Central America, have adopted the TIA analog cellular standard in preference to GSM. Several of these countries are now experimenting with the TDMA and CDMA digital cellular standards. However, since AMPS was originally developed for the US market some unique problems arise when used outside North America, especially when international roaming is attempted. The major problems facing these systems and subscribers are:

- Encoding international mobile identifications in a 10 digit MIN.
- Use of CCITT standards such as R2 and CCITT Signaling System 7.
- Language barrier for roamers.
- Different dialing procedure.

Of all these problems, the restriction of a mobile identification to a 10 digits is potentially the most serious. It is very difficult for cellular operators outside North American, even with the publication of TSB-29, to ensure that they allocate MINs that do not conflict with those used in the USA or in other countries. Discussions have recently started on ways to solve this problem. The most likely solution appears to be the addition of 5 more digits, including the 3 digit CCITT E.212 mobile country code, to the MIN of new analog and digital terminals. This will allow independent national allocation of MIN's, without conflict. It is too early to say which revisions of the air interface standards will incorporate these changes.

WG VI was almost dormant for several years. This should change with the recent appointment of Kimberly Harris of Ericsson to this position. This revitalization is particularly timely given the increasing interest in international roaming problems.

WG VI has published one document, TSB-29-A, that allocates System Identification codes (SID's) to each country, and defines a method for allocating MINs. Unfortunately, recent political changes are ahead of the list of SID blocks and, more importantly, the North American numbering plan administration is studying changes that would invalidate the TSB-29 MIN allocation method.◊