Cellular Networking Perspectives

Editor: David Crowe • Phone +1-403-289-6609 • Fax +1-403-289-6658 Vol. 7, No. 12 December, 1998

In This Issue...

Next Issue: January 11, 1999

Alert! Error in IS-41-C

There is an error in Revision C of IS-41 that has caused much confusion. Digits parameters contain the *Nature of Number* field (octet 2, bits A-H). Revision C defines value 0 in bit A to mean *International* and value 1 to mean *National.* TIA/EIA-41 Revision D, on the other hand, defines these values the opposite way round.

Only one version of IS-41 is wrong, and that is Revision C. TIA/EIA-41-D contains the correct encoding, as does TIA/EIA/TSB-41 ("Tech Notes"). The reason why it has to be this way is because IS-41 Rev. B reserved this field, meaning that those systems should fill it with zero. Assuming that digits parameters in IS-41 Rev. B are all of national format, this implicit encoding must be maintained.

In summary, *Nature of Number* bit A should be 0 for nationally formatted digit strings (e.g. 10 digit NANP numbers) and 1 for internationally formatted digit strings (e.g. conforming to the ITU-T E.164 or E.212 recommendations).

Quote of the Month

"Enhanced wireless 9-1-1 access costs which were forecast to be *limited* costs have become limiting ones. Those costs are not insignificant when weighed against the outcome of delayed emergency response. Why? Because wireless ALI specifications [125 meters, 67% of the time] are sufficiently imprecise that emergency response in many cases will not be timely"

Ernest E. Ricci
E9-1-1 Emergency Telephone System
North Providence, RI

Plagiarism: The Sincerest Form of Flattery

www.cnp-wireless.com has been plagiarized three times, to our knowledge. Twice when unsuspecting companies hired unethical web site creators who trolled the web and edited out any evidence of where they hooked the source. Most recently, and most humorously, an innocent engineer (who shall remain nameless, to protect his innocence) emailed the editor an edited version of:

http://www.cnp-wireless.com/acronyms.html

our tongue-in-cheek telecom acronyms page. Edited, of course, to remove any evidence of its source.

We are pleased that our readers have always respected our distribution policies. As we increase our intranet licensing, something that is better for you and for us, the danger of accidental public access increases. So, if *Cellular Networking Perspectives* is stored on your intranet, please ensure that the files are secure from unlicensed access, and that you contact us whenever your distribution needs go above your current limits.

And, feel free to check out our acronyms web-page. You even have our permission to copy it, as long as you leave our name in it. We will be flattered!

Cellular Networking Perspectives (issn 1195-3233) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary AB, T2N 3W1, Canada.
Contact Information: Phone: 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** http://www.cnp-wireless.com/.
Subscriptions: CDN$300 in Canada (incl. GST), US$300 in the USA and US$400 elsewhere. Payment by cheque, bank transfer, American Express, MasterCard or Visa.
Delivery: Email or 1st class mail. **Back Issues:** Available individually for $35 in the US and Canada and $40 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Copies:** Each subscriber is licensed to make up to 10 copies of each issue or back issue. Please call for rates to allow more copies.

FCC Releases Proposed Rulemaking: Status of J-STD-025 Still Uncertain

The FCC released a *Further Notice of Proposed Rulemaking* (NPRM) for CALEA requirements on November 5, 1998. This document indicates the current thoughts of the FCC on this issue, but is certainly *not* a final decision. All that can be said is, that unless the FCC receives persuasive arguments on a topic, the final rulemaking will probably not change.

The FCC has to decide what should be removed from joint TIA/ATIS standard J-STD-025, and what should be added from the FBI 'punch list'. In most cases they have made tentative decisions in the NPRM, and more is being added than removed.

Deadlines specified by this NPRM (all but the first two open to change) are listed in Table 1.

Table 1: US CALEA Implementation Dates

Date	NPRM Requirement
December 14, 1998	Comments due to the FCC.
January 13, 1999	Reply comments due (i.e. comments to comments received by the December 14, 1998 deadline).
June 30, 2000	US carriers must have the capability to support TIA/ATIS J-STD-025, including cellsite location at start and end of the call, but not including packet data capabilities.
180 days after release of FCC Report & Order	TIA/ATIS must complete the ordered revisions to J-STD-025.
Date to be specified in Report & Order	US carriers must implement the J-STD-025 revisions (or equivalent) ordered by the FCC.

J-STD-025 Endorsed, Well sort of…

The NPRM does (tentatively) find the joint ATIS/TIA standard J–STD–025 deficient in some ways, but this is not really a criticism. The FCC still requires carriers to implement to this standard (or equivalent) before a modified version is ready, less only the provisions for packet data monitoring. And, the FCC has stated that they want any further modifications that they order, to be made by the same joint TIA/ATIS group that created the current version of J-STD-025.

Most importantly, the FCC has referred to J–STD–025 as 'safe harbor', meaning that implementation to the standard is considered (by the FCC at least) as equivalent to compliance with the CALEA legislation, even if deficiencies are later found in the standard.

What's Hot, What's Not?

The NPRM divides capabilities into those that will be mandatory and those that will not be required. This is a useful division, although it is an over-simplification, as there is the possibility that the FCC may be persuaded to move them from one category to another. We have divided capabilities into Hot (mostly included), Warm (included, but with significant limitations) and Cold (not included).

Hot Stuff

The capabilities that the FCC has (tentatively) concluded should be kept in J-STD-025, without major limitations, are listed in Table 2.

Warming on the Threshold

The FCC has decided that some capabilities should only be included with significant limitations, or it is definite about including some portions of these capabilities, but unsure about others. These capabilities are listed in Table 3.

Out in the Cold

Table 4 lists the three capabilities that are (at least for now) not to be included in J-STD-025 support for CALEA at all.

Open Questions

The FCC NPRM on CALEA compliance leaves open a number of technical questions, beyond those unpredictable changes that will be made in the final

Table 2: HOT! Items to be Provided

Name	Description
Existing J-STD-025 Capabilities, except location and packet data.	To be retained. This includes call content (e.g. voice) and call related data (e.g. identity of subject and other parties in the call, the duration of call and the time that the call was initiated, answered and disconnected).
Party Hold, Join, Drop on Multi-party Calls	Law enforcement will be informed every time a party is placed on hold by the subject, added to a multi-party call ('join') or removed ('drop').
Subject-Initiated Dialing and Signaling Information	When a subject *uses* a feature such as call forwarding or call waiting, law enforcement will be informed. Compare with Feature Status (*Cold* list).
Timing Information	Every message sent on the Call Data Channel (e.g. Origination, Termination) will be accurately time-stamped.

rulemaking and beyond all the legal issues that it might raise.

Location

The FCC is going to have to clearly define the privacy issues surrounding location, and in such a way that implementations are straightforward. Unless, of course, they rule that all location information (including E911) should be provided.

Packet Data

The FCC is looking for help in defining technically achievable methods of distinguishing the information part of packets (not covered) from the telecommunications part (covered)…and they will need it! This could prove impossible for a service like TIA/EIA-41 Short Message Service where both types of data are carried transparently by wireless switches.

Multi-Party Calls

The FCC has distinguished between parties added by the subject (covered) and those added by another party (not covered). Yet there are real situations where two multi-party calls merge, and then what is a poor switch supposed to do?

Dialed Digit Extraction

The FCC has not yet realized that it is impossible for switches to distinguish between the three types of post-cut-through digits identified in Table 3. The only device that can interpret these signals is the one that is receiving them (e.g. the inter-exchange carrier). The problem is that tolerances for identifying signals may vary from device to device, that timing (even for the same dialog) may vary from one use to another. This can only be resolved by an intercept at the intermediate switch or by monitoring call content. Neither of these options require changes in J-STD-025, but both require more work from law enforcement, either to obtain a court order that includes call content, so that all audible tones can be monitored, or to obtain an order from the inter-exchange carrier (or carriers) being used by the subject of the order.

Table 3: WARM! Questionable Items & Partial Requirements

Name	Description (and Limitations)
Content of subject-initiated multi-party calls	The subject, and any parties that they add during a multi-party call, will be monitored. This includes 3-way calls, call-waiting, conference calls (more than 3 parties) and call transfer (even after the subject has disconnected). Parties added by people other than the subject should not be monitored. This would result in a party on hold being monitored, but a party receiving an incoming call-waiting call would not be monitored while in conversation with the add-on party instead of the subject.
Dialed Digit Extraction	Digits (e.g. DTMF tones) dialed by a subject during a call ('post cut-through') can be classified as • Call Identifying Information (e.g. a destination number being provided to an inter-exchange carrier), • Information Services (e.g. digits dialed to access a bank account), or • Chaff (digits dialed when there is no digit receiver monitoring the line).
In-Band and Out-of-Band Signaling	Audible or visual signals to a phone that indicate a change in status or an event (e.g. voice mail notification).
Location	The cell or sector where a subject's call is initiated and disconnected will be provided, but the FCC has not decided whether location provided by billing systems, handoff or (most importantly) the more precise E911 requirements, will be made available under CALEA. Even if provided, the court order authorization requirements for law enforcement will likely be greater than for basic call identifying information.
Packet Data	Packet data is a combination of call identifying information (covered by CALEA) and information services (excluded by CALEA). The FCC is asking for help deciding whether these functions can easily be separated by carriers.
Voice Mail	Retrieval of voice mail is considered an 'information service', and is not covered. Notification of callers, and the number of messages waiting is considered call identifying information and is covered by CALEA.

Table 4: COLD! Items *Not* to be Provided by Carriers

Name	Description
Surveillance Status	If mandated, carriers would regularly inform law enforcement of each surveillance that is active (whether actively monitoring a call or not).
Continuity Check	If mandated, a tone would be generated on idle call content circuits to allow law enforcement to verify that voice can be carried.
Feature Status	If mandated, whenever a subject *activated* or *deactivated* or otherwise controlled a feature such as call forwarding or call waiting, law enforcement would be informed.

Digital Circuit Switched Data, Part III: Intersystem Messaging & Standards Deconfusion

The November 1998 issue of *Cellular Networking Perspectives* illustrated some of the basic circuit-switched data scenarios involving roaming that are provided by IS-737. Table 5 lists the existing operations that have been modified to support data and Table 6 lists the two new TIA/EIA-41 operations (also loosely known as transactions, or simply messages) that have been added to support circuit data services in a roaming or other multi-vendor environment.

For further background on the voice-oriented inter-system capabilities that have been modified to support data, consult our back issues. November 1992–February 1993 cover inter-system handoff, March–August 1994 cover inter-system call delivery (using the LocationRequest, RoutingRequest operations, among others), and May–July 1996 cover border cell problems (including inter-system paging).

TIA/EIA-41 Parameters

To support inter-system operations for data mobiles (e.g. call delivery and handoff) IS-737 supports a variety of new types of information, implemented either

Table 5: Modified TIA/EIA-41 Operations

Operation	Modification
AuthenticationRequest	Addition of DataKey parameter to support data encryption.
FacilitiesDirective2	Carries information about a data call from the current Serving MSC to the Target MSC for inter-MSC handoff setup. This includes technology specific (i.e. CDMA or TDMA) radio link parameters, the data key and IS-728 ISLP information.
HandoffBack2	Carries information about a data call from the current Serving MSC back to a previous Serving MSC, that is acting as the Target MSC for a handoff back scenario. The information is the same as for FacilitiesDirective2, except that the Target MSC does not need to be informed about post-handoff ISLP information.
HandoffMeasurement-Request2	Carries information about a data call to a neighboring MSC, to assist in determining which cell would be the best to handoff to.
HandoffToThird2	Carries information about a data call to a Target MSC for situations when an inter-MSC handoff requires a path minimization scenario. The parameters included are similar to FacilitiesDirective2.
InterSystemPage, InterSystemPage2	Carries technology-specific radio link parameters between two neighboring MSC's when border cell problems demand that paging occur in multiple MSC's.
InterSystemSetup	Carries data encryption and ISLP information to configure an inter-MSC circuit when call setup terminates in one MSC, but paging was successful in a neighbor.
LocationRequest	The INVOKE carries data service subscription information, along with call-related data service information (e.g. bit rate) if the Originating MSC has recognized an incoming call as data (see the *Shared Directory Number* solution to *The Termination Problem* on page 4 of the October, 1998 issue). The response (i.e. RETURN RESULT) will carry data service information back to the Originating MSC, except when a call is initiated in voice mode, and changes to data later.
OriginationRequest	When an IS-41 trigger is encountered on a mobile origination (e.g. 4 digit dialing trigger), the HLR is informed of the data service being requested, to assist with its processing of the call origination information.
RedirectionRequest, TransferToNumberRequest	When a call has been terminated, is in a data mode, and needs to be redirected (e.g. call forward no-answer), the Originating MSC must be informed of the data service that had been negotiated. This MSC usually obtains the redirection number from the HLR using TransferToNumberRequest, which therefore needs the same modifications.
RoutingRequest	The INVOKE carries data service subscription information, along with call-related data service information (e.g. bit rate if either the Originating MSC has recognized an incoming call as data (using the *Shared Directory Number* method) or if the HLR has (using the *Separate Directory Number* method). The response (i.e. RETURN RESULT) will carry data service information under exactly the same situations as the LocationRequest RETURN RESULT (see above).
TransferToNumberRequest	*see RedirectionRequest above.*
UnsolicitedResponse	When an MSC receives an unexpected page response from a mobile, it may send the UnsolicitedResponse transaction to neighboring MSC's to try to find the MSC which initiated the page. If the page response requests a data service, then this information must also be included (particularly applicable in the *Page Response in Data Mode* method, described on page 4 in the October, 1998 issue).

Table 6: New TIA/EIA-41 Operations

Operation	Purpose
ChangeFacilities	Used by one MSC to request a service on behalf of a mobile data user that requires changing the call from one inter-MSC circuit to another.
ChangeService	Used by one MSC to request a service on behalf of a mobile data user that can be serviced using the currently allocated inter-MSC circuit.

new parameters, or new values for existing parameters, that are related to the radio link, to data privacy, to the ISLP circuit, to call processing events and to subscription capabilities.

We discuss some of the major parameters below. For a complete description of all parameters, consult TIA/EIA-737.

TDMA Radio Link Parameters

The data rate provided to TDMA mobiles is dependent on the number of time slots in use for each cycle of six. Voice users normally use two, providing about 9.6 kbps of data. However, as few as one time slot per cycle can be used (half rate) or as many as two (double full-rate) or three (triple full-rate). This information is encoded in the TDMABandwidth parameter and is used to control the bandwidth allocated to a mobile during a call.

Other parameters (all beginning with the prefix *TDMA* control radio interface parameters, such as error checking, describe the built in capabilities of a mobile (versus the Subscription Capabilities) and which voice coder should be used (obviously none, for data).

CDMA Radio Link Parameters

A number of parameters are provided that identify data characteristics of the CDMA radio interface. All these parameters start with the prefix *CDMA*. Unlike the TDMA parameters, their definitions are not documented in IS-737, but in the CDMA standard (IS-95 Rev. A, soon to be updated to ANSI standard TIA/EIA-95 Rev. B).

Data Privacy Parameters

The DataKey parameter, based on the Shared Secret Data (see December 1995 issue for an overview of authentication) is used to provide encryption (privacy) of user data. The older voice encryption algorithm could not be used because it is based on a fixed mask. While providing a modest level of voice privacy, it is of no use for data, where long strings of 0 bits would reveal the mask. Data privacy is, instead, based upon the ORYX algorithm, using a rotating mask. A new algorithm, known as E-ORYX will soon be available. While considerably stronger than ORYX, it will not require any TIA/EIA-41 modifications. Further in the future, the TIA TR-45 AHAG (*ad hoc* Authentication Group) will be developing, through a public process, a completely new set of algorithms, including data privacy. It is likely that some TIA/EIA-41 modifications will be required at that time.

An existing parameter, ConfidentialityModes has been extended to transmit the desired or actual state (depending upon the specific usage) of data privacy during inter-system handoff. SystemCapabilities has been modified to allow an MSC to inform the Authentication Center (AC) that it supports data privacy.

Table 7: TIA TR-45 Data Standards

Technology	TIA TR-45 Subcommittee	Std.	Description	Pub.
Network	TR-45.2	IS-728	Inter-system link protocol (ISLP)	04/98
		IS-737	Inter-System circuit switched data	05/98
TDMA	TR-45.3	IS-130-A	Data services radio link protocol (RLP)	07/97
		IS-135	Circuit switched data and fax	04/95
		IS-684	STU-III radio link protocol (encrypted voice)	07/96
		TIA/EIA-136-3XX	ANSI version of data services standards IS-130 and IS-135	devel.
CDMA	TR-45.5	IS-99	Circuit-switched data services (9.6 kbps)	07/95
		IS-657	Packet data services	07/96
		IS-658	Data services inter-working function (‘modem pool’)	07/96
		IS-707-A	Circuit-switched data services (14.4 kbps)	ballot
CDPD	TR-45.6	IS-732	Packet data using ‘analog’ 30 kHz channels	02/98
		TSB-87	Implementor guidelines for IS-732	02/98

ISLP Parameters

The only information currently required regarding ISLP is whether it is on or off. However, provision has been made (in the ISLPInformation parameter) to allow new protocols in the future. For example, it would be possible to transmit several 9.6kbps or 14.4kbps data calls over the same inter-MSC circuit, but this would go beyond the capabilities of IS-728 ISLP, requiring independent addressing of each frame.

Call Processing

The AccessDeniedReason parameter has been modified to identify the inability to provide a specific data service (e.g. due to a refusal or inability to provide a requested bit rate). ReasonList has been added to provide a detailed description of the reason why a service change (e.g. change in bit rate) cannot be supported.

Subscription Capabilities

The CallingFeaturesIndicator parameter has been modified to add a new subscription option, allowing the HLR to control whether data services are provided to a mobile or not. A CDMAServiceOptionList parameter has been added to the profile, to allow the HLR to identify, in more detail, the specific services to which each CDMA data user is entitled. Similarly, TDMADataFeaturesIndicator lists the data features (such as Group III fax or triple full-rate data) to which each subscriber is entitled.

Summary of Standards

Table 7 provides a summary of TIA standards for data. Although this series of articles just focused on circuit-switched data, packet data standards are also included for completeness.

Inter-System Link Protocol (ISLP): IS-728

The necessity for a special inter-MSC carriage protocol was mentioned under *The Handoff Problem* in the October, 1998 issue (pages 4-5). ISLP is a very simple protocol that allows asynchronous data to be carried on a synchronous facility, performing basically a rate adaption function. Data being transmitted over a radio interface, even at the highest allowable speeds (currently about 30 kbps for TDMA, and 14.4kbps for CDMA, with 64 kbps possible in the future) poses no capacity problems for an inter-system circuit, which usually runs at 56kbps or 64 kbps or faster. However, these facilities provide no distinction between the mobile's data, and the remainder, that must be discarded, nor any separation of frames that come over the radio interface. Some method is needed to separate the bits coming out of the end of the pipe into wheat (user data) and chaff (framing overhead and filler).

ISLP solves this problem in a simple way, using flag framing and bit stuffing (zero bit insertion, to be precise). A flag is a sequence containing 6 consecutive "1" bits that indicates that user data is not being transmitted, acting as both the beginning and end of frames, as well as additional filler between frames (providing the rate adaption capabilities). Since the flag bit pattern (01111110) can occur in user data, whenever 5 "1" bits are encountered a "0" is inserted by the transmitter and removed by the receiver.

Figure 1 illustrates the intermingling of data and flags on an ISLP transmission.

IFAST Update: "Save the IRM's"

At the rate IRM codes are being assigned, we may soon need Greenpeace to save them before they go extinct. The IRM code, a 10 digit MIN starting with 0 or 1 so it will not conflict with NANP directory number-based MIN's, is essential to allow carriers outside North America to provide international roaming. It is also needed by data service providers (e.g. Cellemetry and Aeris) to distinguish their mobiles from regular voice mobiles.

At the IFAST meeting on October 27th and 28th, 1998, another large batch of IRM codes were assigned. It has only been two years since IFAST began assigning IRM codes, and already one-third of them are gone.

It is becoming apparent that carriers in many regions, not just North America, are forced to align their MIN and Directory Numbers. Doing so makes IRM allocation very inefficient. Brazil, for example, was allocated 58 IRM codes, equivalent to 58 million unique mobile identifiers, far more than they need for the foreseeable future. However, because of various constraints, including their national billing standards combined with privatization, each carrier in each region needs a unique IRM code.

The solution? As we have stated many times, is IMSI. The international allocation of Mobile Country Codes has already been performed by the ITU, and each of the 1 million available carrier blocks can identify 1 billion mobiles. Farsighted vendors and carriers are surely starting to plan. The industry is travelling fast, and the end of the yellow MIN road is approaching.

Figure 1: ISLP Protocol Transmission