Cellular Networking Perspectives

David Crowe [Editor] • Phone: 1-800-633-5514 • Fax: 403-289-6658 Vol. 5, No. 11, November 1996

In This Issue...

Look forward to your next issue on: December 3, 1996

Introducing the North American Numbering Council (NANC)

The US FCC announced its intention to transfer numbering issues from Bellcore's NANPA (North American Numbering Plan Administration) some time ago (e.g. August, 1993 issue). Now, the North American Numbering Council is taking its first steps. This organization is intended to blunt the criticism of the NANPA, that it was beholden to the large local exchange carriers that owned Bellcore.

The NANC will certainly be part of an impressive bureaucratic structure. While it will advise the FCC and other North American Number Plan member countries (Canada and the Caribbean nations) on numbering issues, it will not directly administer numbers. One of its first jobs is to create a working group (North American Numbering Plan Administration Working Group) to "develop and advise the NANC on an appropriate process for selecting a neutral NANP Administrator." So, some time down the road, the NANPA will be reborn, but working for a different master (or, rather, masters). Other functions for this working group will be to plan a transition from the Bellcore NANPA to the new NANPA, and from the current local code administrators (generally the dominant local exchange carrier). It will also have to define a cost recovery mechanism for NANP administration expenses.

Another working group of the NANC is charged with recommending to the FCC, by May 1997, one or more Local Number Portability administrators.

The concept of the NANC is to allow a wide range of industry interest groups to influence numbering policy decisions, while having day to day issues divested to a neutral administrator. Theoretically, this will allow allocation of numbering resources to be performed efficiently and fairly following rules that have been agreed to by the entire industry.

For more information contact Marian Gordon of the FCC (202) 418-2337. ❑

Intersystem Message Security

Once authentication is universally available, the most vulnerable point for technological fraud will be the networks used to carry IS-41 signaling and IS-124 call detail information between cellular/PCS systems. A new TIA ad-hoc group is being set up to address this issue, with membership drawn from subcommittee TR-45.2 (responsible for developing both the IS-41 and IS-124 standards) and the TIA TR-45 AHAG (ad-hoc Authentication Group, responsible for security issues).

This joint ad hoc group will be responsible for implementing the recommendations of the CTIA Intersystem Messaging Security Forum that convened in July/August 1996, which were:

a. Network Entity Authentication (i.e. don't talk to strangers)

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. 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.

b. Data Confidentiality (i.e. elude eavesdroppers).

c. Message Integrity (i.e. make sure the postman keeps his eye on the mail).

This group will likely develop a method of encryption for IS-41 and IS-124 messages, that minimizes the additional network overhead, key management overhead and compatibility impact. ❒

Wireless Around the World…Again

Updated figures from the US Department of Commerce map the continuing expansion of wireless around the world (about 8% growth in 6 months). Although the figures are, perhaps not surprisingly, somewhat out of date (up to 1 year old, judging by the US figures), they document a more rapid expansion of GSM than AMPS systems, although the number of AMPS subscribers is still almost three times higher than the GSM total. The total number of GSM subscribers has now surpassed that of TACS systems. Growth in TACS and NMT systems (as a percent of the total market) is no longer accelerating.

The observant reader may note that fewer nations are listed for most categories. In our last report (August, 1996), we included nations with systems listed with no subscribers. In this report, we list the more meaningful figure of the number of nations that have systems with paying subscribers (at the time the data was gathered). Even more observant readers may note that the "% of Market" figures add up to more than 100%. This is due to rounding. ❒

Table 1: Global Wireless Penetration

Wireless Technology	Subscribers (millions)	% of Market	# of Nations	Description of Technology
AMPS	45.1M	50%	65	Analog and digital technology based on AMPS, NAMPS, D-AMPS (TDMA) and CDMA (IS-95)
GSM	15.8M	18%	53	Digital in the 900/1800/1900 MHz bands
TACS	14.0M	16%	25	Analog AMPS adapted to the 900 MHz band
Japan	10.0M	11%	1	Several different technologies
NMT	4.4M	5%	40	European analog system (450/900 MHz)
Other	0.9M	1%	11	Various other analog standards
Total	90.2 M			

IS-129: A Standard for GSM to IS-41 Interworking, Part II

We described the purpose of IS-129 as a standard to provide GSM to IS-41 interworking in Part I of this series. In this part, we continue the discussion of the network capabilities that are supported, and those that are not, and conclude with a list of announced products and an assessment of the value of this standard.

Notable Exclusions: Handoff and Short Message Service

Inter-system handoff and short message service interworking are not defined in IS-129. The absence of handoff is not hard to explain. The technologies differ significantly in how they perform handoff, and base station modifications would be required to allow the measurement of signal strength of a mobile operating in a different frequency band using a different technology. There is probably no business case for ever supporting this capability.

Short Message Service is a more surprising omission. AMPS analog cellular has supported short message service since the development of IS-91, as an optional capability. Although IS-91 also defines an NAMPS (Narrowband AMPS) capability, this is also optional, so many analog terminals, NAMPS or not, support at least basic numeric short messaging. Short messaging is also built in the standards for second generation TDMA (IS-136) terminals, all IS-95 CDMA terminals and, of course, in GSM terminals. Only the EIA/TIA-553 analog standard and IS-54 TDMA digital do not support short message service.

Call Delivery

Basic call delivery can be provided through inter-working, by translating the IS-41 RoutingRequest transaction to or from the GSM Provide_Roaming_ Number transaction. Unfortunately, no details of this translation are provided in the standard. Compatibility is possible because both systems deliver calls to roamers using a PSTN routing number, known as a TLDN in IS-41 and Roaming_ Number in GSM.

Seamless interworking is possible for call forwarding diversion that is initiated *instead* of routing to the current serving system (e.g. call forward immediate), although surprisingly this is not shown for the case of call forwarding busy (which can use pre-routing diversion in most cases).

Call forward on no-answer/no-page-response (and some rare call forward busy situations) requires that a call be set up to the serving system. If the mobile does not respond to the page, or is not answered, IS-41 allows the home (i.e. originating) MSC to handle the diversion, tearing down the (probably) long distance call leg to the serv-

ing system. However, as in any interoperability standard, the lowest common denominator has to be used, which for this operation is GSM, and diversion has to occur from the serving system (see Figure 1). In the likely case that the call forward number is in the subscriber's home area, IS-41 would set the call up as a local call, but IS-129 would set up a double long distance call (to the serving system and back again).

Products

One independent vendor that has announced a product that is compliant with IS-129, is Synacom with their RoamFree™ Gateway. According to Randy Snyder, their product manager, the product is currently in beta test with Nokia. This GSM equipment supplier has announced that they will be using RoamFree™. According to Snyder, "RoamFree will allow GSM operators to provide nationwide roaming as soon as they turn on their US PCS systems." Dual-mode DCS1900 (GSM)/AMPS-analog handsets are expected soon from a number of major terminal manufacturers to take advantage of this capability. Nortel and Ericsson, two of the most prominent vendors with both GSM and IS-41 based infrastructure equipment, also have announced the development of products that will support GSM/IS-41 interoperability based on IS-129.

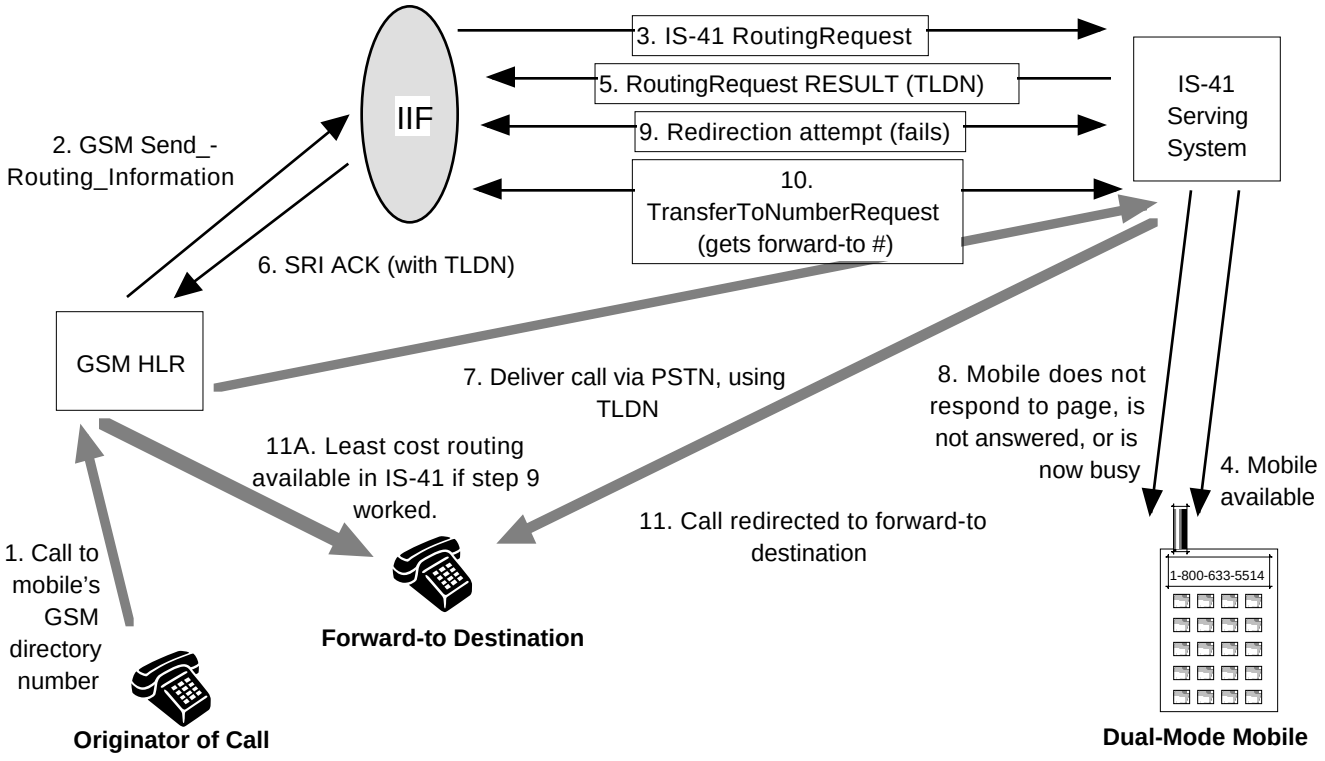
GTE (with their GlobalRoam™ product) and AT&T Wireless Services both provide a GSM/IS-41 roaming service, but one that is oriented to North American AMPS and European GSM operation. There is no indication that they plan to adapt their services for use within North America between different technologies.

Summary

IS-129 is a good start on a standard for GSM/IS-41 interworking. It provides a useful description of interworking requirements. However, the description of network flows is inadequate, as the GSM HLR/IIF/IS-41 HLR message flows are inexplicably omitted. The Stage III description of parameter mapping is omitted entirely. The standard is a good indication that interworking for a few basic features is possible, but it leaves a lot to the imagination.

It is questionable whether IS-129 is required at all. Since the IIF must be built using unmodified standard interfaces, there are no interfaces to standardize or modify. The inner workings of the IIF essentially define the interworking, and to standardize the internal operations of a network element would be outside the normal realm of standardization (and is certainly not tackled by IS-129). IS-129 basically provides a high level introduction to interworking, that probably has more educational than technical value. ❒

Figure 1: Interoperability Inefficiencies in IS-41/GSM Call Forwarding



RF Fingerprinting Carves a Niche Out of Fraud, Part I

RF Fingerprinting appears to be successfully finding a place for itself as a mechanism for reducing cloning fraud. Its manufacturers, and carriers that have purchased the equipment, claim that each cellular phone can be recognized by stable features of each radio transmission that are unique to each phone, just like a human fingerprint. They claim that this technique can reduce cloning fraud by 75%-85%. RF Fingerprinting will coexist with authentication and profiling, until authentication achieves enough penetration to stand alone (which could be 5 to 10 years, according to estimates published in the August, 1996 issue). This anti-fraud technique is based on recently declassified military technology that examines several parameters of a radio signal to attempt to distinguish known radios from clones.

How it Works

Every radio has a transmission pattern with some unique, and relatively stable, features that change only slowly over time. The set of features used by a vendor are known as the radio's RF Fingerprint. The military applications of this technology were first exploited, both for authentication of 'friendly' radios, and also to try to recognize which radio enemy transmissions were coming from. This technology has been civilianized by three companies; Corsair (previously TRW/ESL), Cellular Technical Services and Signal Sciences.

RF Fingerprinting systems tap into the antenna system, monitoring the analog control channel for each cellsite that it operates in. The cell-site equipment passively monitors each origination, page response and registration extracting not only the RF features required for the proprietary algorithm, but also the MIN and ESN from the transmitted access attempt. Usually, monitors for several cellsites are networked to a single central processor, containing the database of valid fingerprints. Applying a complex algorithm, it matches the received signal with the one stored for that MIN and determines the 'distance' from the legitimate mobile's signal. If the caller is determined to be a cloner (i.e. the signal is too 'far' away from the legitimate, stored pattern), the call will be disconnected.

There are several ways that a cloner can be disconnected:

i. waiting for the mobile to appear on the voice channel, and then simulating a disconnect.

ii. sending a message to the MSC to initiate a disconnect (an MSC dependent method).

iii. Using the control channel to obscure the IVCD (Initial Voice Channel Designation) message to the switch, or to simulate a second origination from the same mobile (which may cause a disconnect through the MSC's own fraud detection software).

The actual method used will vary depending on the type of RF Fingerprint system, the type of MSC and individual carrier, or even market, requirements. In any case, all the cloner will hear is a click and possibly a brief burst of static. Calls will be disconnected within a few seconds of pressing the SEND key.

Other Methods

Commercial implementation of fingerprinting is ahead of authentication, although behind PIN and Profiling (see the November, 1995 issue for an overview of a number of anti-cloning methods). RF Fingerprinting is not superior to other methods in all ways, but it has a unique combination of strengths that will allow it to co-exist with other methods.

Reducing Roamer Service

Not really an anti-fraud method, refusing to service roamers is a last resort, whether by totally refusing service or by reducing service to local calls only. RF fingerprinting should reduce the necessity to do this, although the inter-operability problem needs to be solved to allow fingerprinting to be used on all mobiles. This will enable significant quantities of lost roamer revenue to be recovered.

Profiling

Profiling, which compares each call to an individual subscriber's historical calling patterns is, like RF Fingerprinting, a probabilistic method. Consequently, there is some synergy between the two technologies. Corsair allows RF Fingerprinting information to be exported to a profiling system to improve the performance of profilers. CTS allows profiling data to be imported to reduce the probability of disconnecting legitimate calls. Signal Sciences uses profiling information to raise the probability of detecting a clone from the high 80% range to the high 90% range.

Authentication

Authentication is the ultimate clone fighting method … for phones that support authentication. Even if all phones manufactured in 1997 and beyond are authentication capable (and there is certainly no reason why they should not be), it will be several years before a large enough majority of phones are authenticateable to make the life of a cloner truly difficult. This time period is the period of opportunity for RF fingerprinting, which is not as strong a method, but does work with all phones.

Law Enforcement

Catching and prosecuting cloners is much more expensive and less effective than preventing them from operating. However, some resources will always be necessary to catch people attempting to defraud systems. RF Fingerprinting will not eliminate fraud, and therefore will not eliminate the need for resources to be applied to catching and prosecuting cloners. There may be some synergy between these two methodologies, if the RF platform can be adapted to tracking down the location of cloner phones.

To be continued...

Part II will examine the pros and cons of fingerprinting, and list the market penetration of the two vendors who currently have equipment installed. ❐

Status of IS-41 Rev. B Implementation

Cellular Networking Perspectives

Editor David Crowe • Phone: 1-800-633-5514 • Fax: 403-289-6658 *Last Published 07/96*

Vendor1	Vendor2	Status	Date	Type				Location
Alcatel SEL	EDS PC	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	*connectivity using IS-41 Rev. A plus TSB-55 only*							
Celcore	Alcatel SEL	Commercial	05/96		V	D	S	Yorkville, TN
	Ericsson	Commercial	06/96		V	D	S	Chicago (Cellular One)
	Lucent	Field Trial	09/95	H	V	DX		Cleveland, Ohio (GTE Mobilnet)
	Motorola	Commercial	12/95		V	DX		Little Rock, AR (Alltel)
	Nortel	Field Trial	05/96		V	D	S	Seattle (Western Wireless)
	Tandem (HLR)	Field 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	Commercial	n/a		V	D	S	Several Locations
	Lucent	Commercial	n/a	H	V	D	S	Several Locations
	Motorola	Commercial	n/a	H	V	D	S	Several Locations
	NEC	Commercial	n/a		V	D	S	Several Locations
	Nortel	Commercial	n/a	H	V	D	S	Several Locations
	Tandem	Commercial	n/a		V+	D	S	Several Locations
GTE TSI	*connectivity using IS-41 Rev. A plus TSB-55 only*							
Harris	NACN	Field Trial	08/96		V	DX		NACN testing
Lucent	*Up to date information not available*							
Motorola	Alcatel SEL	Commercial	2Q'95	H	V	D	S	*Multiple locations*
	EDS	Commercial		H	V	D	S	Multiple locations
	Ericsson	Commercial		H	V	D	S	NACN
	Lucent	Commercial		H	V	D	S	Multiple locations
	NEC	Commercial			V	D	S	Brazil
	Nortel	Commercial		H	V	D	S	NACN
	Plexsys	Commercial			V	D	S	Multiple locations
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:		
	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.

TIA TR-46 Committee Public 1800 MHz PCS Project Status Report

Cellular Networking Perspectives

Editor David Crowe • Phone: 1-800-633-5514 • Fax: 403-289-6658 *Last Published 11/95*

Published Interim Standards

IS- Number	Description	Status
IS-104-A	PCS Service Descriptions	Published
IS-129	Interworking/interoperability between DCS1900 and IS-41 MAPs	Published 07/96
IS-651-0	SS7/GSM "A" Interface (RS/PCSC)	Published 07/95
IS-652-0	Intersystem Operations - DCS1900 (GSM) MAP based	Published 05/96

Published Telecommunications Systems Bulletins (TSBs)

TSB- Number	Description	Status
TSB-68	Intersystem Operations - IS-41 MAP based	in press

Projects in Ballot Process (SP=Standards Proposal Number)

ISP	Description	Status
SP-3344	ISDN "A" Interface (RS/PCSC). Includes SS7 as a transport option	Second ballot

Active TR-46 Projects (PN=TIA Project Number)

PN	IS/TSB	Description	Status
3167	internal	System requirements, revised (was PN-3368)	
3436	*internal*	Advanced network reference model, including IN, OA&M, 911 and lawful intercept network elements	Completed
3513	TSB-xxx	SS7 signaling and network routing. Resulting in translation type 10 being reserved for SS7 network routing using an E.164 directory number	Completed
3567	IS-652-A	Intersystem operations for DCS1900 MAP, revised to add call barring, intercept, multi-way calling, data, fax, 911, equal access, ITU-T TCAP and E.164 GTT (see PN-3513)	ballot 4Q'96
3568	*see IS-634-A*	Frame relay A interface (RS/PCSC)	Moved to TR-45.4
3596	IS-651-A	SS7 A-Interface, supporting DCS-1900 (GSM) interface.	TIA review
3808	*tbd*	Lawfully authorized electronic surveillance. A joint project with TR-45.2	Development
3809	*tbd*	Enhanced wireless emergency services. A joint project with TR-45.2	Development
n/a	*internal*	Privacy and authentication requirements (P&A)	Development

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

2. Bold Type indicates modification since the previous publication of this report.