Cellular Networking Perspectives

David Crowe [Editor] • Phone: 1-800-633-5514 • Fax: 403-289-6658 Vol. 5, No. 2 February, 1996

In This Issue...

Surfing The NET??

Visit *Cellular Networking Perspectives* at our EXCITING NEW web page at:
http://www.cadvision.com/cnp-wireless

Check out the story about the mosquitoes of Thunder Bay...

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

Subsystem No. = Headache TSB-55 = Aspirin™

The biggest outstanding source of incompatibility between IS-41 Rev. A and B systems is the SS7 subsystem number (SSN). IS-41 Revision A insists that this should always have the value 5, whereas IS-41 Rev. B defines it as 6 for a message transmitted by an HLR, 7 for a VLR and 8 for an MSC. Some IS-41 Rev. A system consequently reject any message from an IS-41 Rev. B system, based on a strict interpretation of the standard. In reality, both versions of IS-41 were wrong, the SSN is part of the full SS7 address and should no more be specified in a standard than should the point codes.

To solve this problem, all MSCs that are connected to an IS-41 network should be upgraded to implement the recommendation of TIA TSB-55 that:

> "IS-41-A [systems] shall permit the receipt of any Calling Party Subsystem Number. IS-41-A [systems] shall populate the Called Party Subsystem Number in the response message with the value received in the Calling Party Subsystem Number of the Query."

IS-41 Rev. B systems should also implement the recommendations of TSB-55 to ensure that they can accept SSN 5 from IS-41 Rev. A systems and that they can accept any SSN from IS-41 Rev. C and higher systems.

Our thanks to Jim McGarrah of BellSouth for pointing out the importance of this problem, based on extensive field experience with a mixture of IS-41 Rev. A and B systems.❑

More on Authentication...

Export Controls on CAVE Algorithm

Exporting equipment containing the TIA CAVE algorithm for authentication and voice encryption requires an export license, but not necessarily from the US Dept. of State, as was reported in our December, 1995 issue. When the algorithm is embedded in a piece of equipment (i.e. binary software code, in a read-only memory), only a Dept. of Commerce license may be required. These licenses are generally easier to get, are valid for a longer time and require less administration.

More A-Key Requirements

Both the A-Key and the random number (RANDSSD) used to generate Shared Secret Data should be randomly selected. If a carrier was to take a simple approach and assign A-Keys (or random numbers) starting at 0 and incremented by one for each subscriber, it would be easier for a cloner to guess the value of the A-Key (or the random number). This approach would make a brute force approach to determining an A-Key or SSD significantly easier.

For a similar reason, the A-Key should be selected from the full range available. Attempts to reduce the number of digits that have to be entered in a cellular phone below 26 would again make a brute force attack much easier.

Thanks to Allan Angus of JRC International for bringing this additional information to our attention.❑

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 1-403-289-6609. Fax: 403-289-6658. Subscriptions: CDN$250 in Canada (incl. GST), US$250 in the USA and US$300 elsewhere. Payment by cheque, money order or American Express Card. Issues are faxed or mailed 1st class. Copies: Each subscriber may make up to 10 copies of each issue. Rates are available for more copies.
Discounts: Educational and small business rates: CDN$150 (incl. GST), US$150 and US$200, by mail only. Back Issues: Phone for price list and table of contents.

The IS-95 Standard for CDMA Digital Wireless Communication: Part I

CDMA is one of the two branches of digital cellular technology, preferred by carriers representing over half of the US market. The other branch of digital cellular, TDMA, is described (as exemplified by the TIA IS-136 standard) in the August and September issues. CDMA is also battling TDMA for supremacy in the PCS arena, with carriers divided (so far) between CDMA and the TDMA standards PCS1900 (based on GSM) and IS-136.

CDMA is an attempt to apply the benefits of digital technology to cellular communications; higher capacity, better quality, more features and greater privacy. The delays in the progress of CDMA have been a reflection of the immense technical challenges to overcome to bring this technology to market, and the better than expected ability of analog systems to handle the dramatic increases in capacity. However, it is inevitable that digital technology will displace analog, the questions are: When? and; Which technologies will survive?

Introduction to CDMA

CDMA is a multiple access technology using spreading codes to allow several users to share one block of spectrum. CDMA systems digitize all voice and data traffic and overlap all calls over the entire width of the RF channel, and in every time interval. The transmitted signal looks like noise to an outsider:

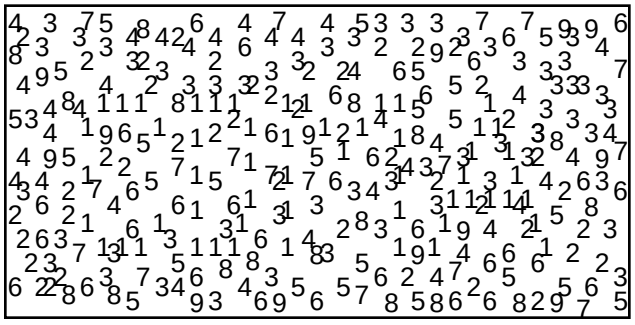

Figure 1: CDMA transmissions look like noise...

However, if the unique spreading code of an individual caller is applied to the broadband signal, their voice or data pops out, leaving the remaining signals just as background noise.

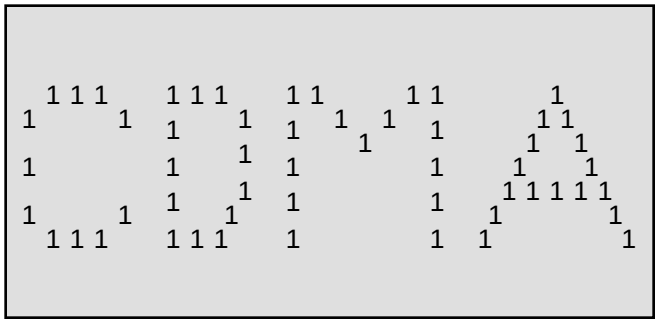

Figure 2: ...unless you know the secret code

CDMA technology is distinguished from FDMA (Frequency division multiple access) that uses frequency to separate calls and TDMA (Time division multiple access) that uses time to separate calls (see August, 1995 and September, 1995 issues for a discussion of the IS-136 TDMA digital cellular standard). CDMA, as defined in the TIA IS-95 standard, also differs from FDMA and TDMA cellular in using 1.25 MHz of spectrum per RF channel, rather than 30 KHz. Qualcomm claims that CDMA systems can support, in commercial systems, more than 10 times the number of users than analog systems can.

A Little History

The cellular industry recognized the need for higher capacity systems in 1988 when the CTIA released a set of requirements ("UPR") for a higher performance cellular system. The UPR had the requirements listed in Table 1:

The solution chosen was to move to digital technology. First the industry battled over FDMA versus TDMA, with TDMA winning out. However, just as the TIA started developing the IS-54 TDMA digital cellular standard, interest started to grow in a new, CDMA, alternative proposed by Qualcomm. While some felt that only one standard for digital cellular should be supported (and that the decision had already been made), others strongly felt that CDMA was better and that the standards committees should support both technologies. The proponents of CDMA won approval from the CTIA early in 1992 to proceed with a parallel standardization effort. Much has changed since then, but TDMA and CDMA proponents are still embroiled in a battle for technical supremacy. As an ironic footnote, FDMA proponents can even claim a victory, with Motorola's FDMA based NAMPS technology being standardized in IS-88 and IS-91.

Table 1: CTIA Users' Performance Requirements for Second Generation Cellular Systems (1988)

#	Requirement	TDMA	CDMA
1	10x capacity increase	✔	✔✔
2	Long lifespan	✔	✔✔
3	New Features	✔	✔
4	Quality Improvements	✔	✔
5	Privacy	✔	✔✔
6	Ease of transition and compatibility with analog	✔✔	✔
7	Early availability and reasonable cost	✔✔	✔
8	IS-41 compatibility	✔	✔

Commercial status

TDMA systems have been in commercial service since 1992, although not without their critics, particularly in terms of voice quality. CDMA systems entered commercial service with Hutchinson in Hong Kong in 1995, now with several thousand CDMA users. Strong promises are being made for US and Canadian commercial service this year. Trial PCS systems are being built and undergoing testing. Some carriers and equipment suppliers are strongly committed to TDMA (e.g. Southwestern Bell and Ericsson), some to CDMA (e.g. AirTouch, US West and Qualcomm) while others have a foot in both camps. We will not dwell on the merits of one technology or the other, but

merely say that the proof of the pudding is in the eating. Until CDMA systems are running side by side with TDMA systems in dense urban environments, it will be impossible to say which technology is truly better. Whether both systems will coexist (leading to the eventual development of tri-mode phones) or whether one will eliminate the other is not possible to predict.

Spectral Efficiency

The initial push toward digital, and toward CDMA in particular, is based on increased spectral efficiency, defined as the number of simultaneous calls in the spectrum available to a user. Spectral efficiency in the competing cellular technologies is based upon the number of carriers in the available frequency, multiplied by the number of simultaneous calls possible in one carrier and divided by the frequency reuse pattern. CDMA gains by reusing the same frequency in every cell. If this was not the case, its spectral efficiency would be little more than analog cellular. The following table estimates the capacity of various cellular technologies (numbers for PCS will be similar). Constraints not listed in this table may decrease the number of simultaneous calls in each cell:

harder to sell to consumers of cellular service. The one benefit of digital that should appeal to all consumers (lower price) was not passed on by the carriers for a long time, leaving the consumer to pay more for a digital terminal and receive only minor (if any) reductions in air time charges.

Move Over Analog

One of the problems with CDMA is that, although the spectral efficiency of a pure CDMA system is great, it still has to coexist with analog. This means that spectrum has to be assigned from analog use to CDMA in a carefully coordinated fashion. Unlike TDMA that can start with a single 30 khz channel being removed from a cell (with the loss of usually one more channel for a guard band), CDMA requires an initial investment of 1.25 MHz (plus a large guard band) throughout the network. If sufficient CDMA terminals are on the system, this will double the capacity. However, if the system is heavily loaded, and most terminals are still analog, the transition will cause a capacity crunch. CDMA carriers can avoid this problem by selling CDMA terminals in advance of the turnup of CDMA, or by committing to NAMPS, which makes more efficient use of the existing spectrum. It is unlikely that analog phones will ever totally disappear, so the full efficiency of CDMA (and TDMA for that matter) will never be achieved in cellular. PCS is a different matter, as a carrier can choose to use only digital technology on their network.

Power Control

Power control is more important in CDMA than in TDMA or analog. If it is not monitored and adjusted regularly, phones close to a cell site will drown out those further away. The aim of CDMA power control is to keep the power as low as possible while keeping the frame error rate above a minimum level. In the case of soft handoff (when a mobile is communicating with more than one cell), power levels are controlled by the cellsite receiving the best signal from the mobile. Power control is implemented by monitoring the long term frame error rate, and using it to occasionally update a signal-to-noise ratio (Eb/No) threshold that provides real-time power control. Additional advantages of power control are that it significantly increases the battery life of phones and maintains a consistently high voice quality.

Raw Data Rates

The original IS-95 standard supported a maximum raw bit rate of 9600 bps for each traffic channel. Due to overhead, the actual throughput is lower (i.e. 8550 bps). That rate was increased to 14,400 bps in J-STD-008 (the PCS version of IS-95) and in TIA TSB-74 (an add-on to IS-95-A for cellular systems). A proposal has been made by Qualcomm to support a bit rate of 64,000 bps, presumably to support data applications.

Table 2: Spectral Efficiency of AMPS based Wireless Standards

	Analog	NAMPS	TDMA	*…future*	*CDMA*	*…future*
TIA Standards	EIA/TIA-553, IS-91	IS-88, IS-91	IS-54, IS-136	IS-54, IS-136	IS-95	IS-95
Spectrum available (per cellular carrier)			12500 KHz			
Carrier size	30 KHz	30 KHz	30 KHz	30 KHz	1250 KHz	1250 KHz
# carriers (N)	417	417	417	417	10	10
Calls per carrier (C)	1	3	3	6	60	120
Voice coder efficiency (V)	1	1	1	2	2	2
Cell Reuse Pattern (R)	7	7	7	7	1	1
Calls/cell (theoretical): (N x C x V) / R	60	179	179	715	1200	2400
Calls/cell (actual)	60	179	179		600	

Spectrum efficiency was the biggest motivation for moving to digital, but the feared spectrum shortage has not materialized in a drastic way. This has slowed the drive to digital, because, outside of spectrum efficiency, the merits of digital are

Variable Rate Voice Coder

CDMA uses a variable rate voice coder to increase the capacity of the system by about 2 times, and to reduce the power requirements. These gains are based on the observation that each talker in a conversation speaks on average only 35% of the time. Also, in data applications, transmission is usually heavily skewed towards one direction at a time.

Each voice coder supports four data rates, with the highest rate normally being used to transmit voice or data. The lowest bit rate is used when one direction of the conversation is silent (or, for data, when the transmission is unidirectional for some time), transmitting background noise (although without the greatest fidelity!). The second highest bit rate is most commonly used to transmit signaling messages in parallel with voice, a method known as "dim and burst", as opposed to "blank and burst" (used in analog cellular) that interrupts the transmission of traffic for the duration of signaling message transmission..

The first CDMA voice coder, defined in TIA IS-96, runs at a maximum raw rate of 9600 bps (8550 data bits), with other possible rates being 4800 bps, 2400 bps and 1200 bps.

IS-127 Enhancement: An improved voice coder that runs at the same speed as IS-96 is under development as TIA IS-127, known as the Enhanced Variable Rate Voice Coder (EVRC). This voice coder takes advantage of advances in voice coder technology since the development of IS-96.

TSB-74 and J-STD-008 Enhancement: A new voice coder that will run at a maximum rate of 14,400 bps has been developed by the CDG (CDMA Development Group), with the ability to step down to rates of 7200 bps, 3600 bps and 1800 bps. It is expected that this voice coder will be used extensively in PCS systems, where capacity is less of a concern than in cellular systems. This voice coder will also be incorporated into IS-95 Rev. B.

Frequency Use

One of the distinct differences between CDMA systems and others is the use of the same frequency in multiple cells. Analog and TDMA cellular systems are carefully coordinated to avoid the use of the same frequency in neighbouring cells. CDMA, however, uses the same frequency in all cells, and allows mobiles to concurrently communicate with multiple cells in a mode known as soft handoff. The absence of frequency reuse multiplies the available spectrum by the current reuse factor (often 7 for analog and TDMA, meaning at most 1/7th of available frequencies can be used in any one cell).

CDMA Channel Structure

All CDMA channels are encoded in some way in order to distinguish one from another (hence the name Code Division), as they are not separated by frequency or time. In the forward direction, channels are covered by one of 64 orthogonal Walsh codes (leading to a maximum of 64 channels). In the reverse direction, the access channel is spread by a long code which is a concatenation of system parameters and the traffic channels are spread by a public long code mask derived from the ESN of the mobile or a more secure private long code, based on the output of the TIA CAVE ("Cellular And Voice Encryption") algorithm.

Forward Channel (Base to Mobile)

A CDMA mobile has to lock onto a system gradually. At first, everything looks like noise. The MS searches for the strongest pilot channel, which is unmodulated by data but spread by a known sequence. Then a Sync channel can be acquired to obtain basic system parameters, then the mobile can move on to a paging channel to wait for a command from the user or the network before finally reaching a traffic channel to transmit voice or data. This process is illustrated in Figure 3.

Pilot Channel

Each cell broadcasts one pilot channel. The pilot channel is unmodulated allowing the signal strength of the cell to be determined, and compared with others. Each pilot transmits the same spreading sequence at a different time offset. This offset can be used to distinguish the signals of different pilots. The basic uses of a pilot channel are:

1. Acquiring the system.
2. Identifying handoff candidates.
3. Rescanning (i.e. checking for a better cell every so often).
4. Identifying multi-path components.
5. Time and Phase tracking, maintaining the best communication on the paging or traffic channel.

Mobiles continually monitor pilot channels while on a paging or traffic channel. This enables a mobile to remain on one channel while simultaneously checking when it would be a good idea to move to a different cell. A mobile in a call monitors several pilot channels continuously, in

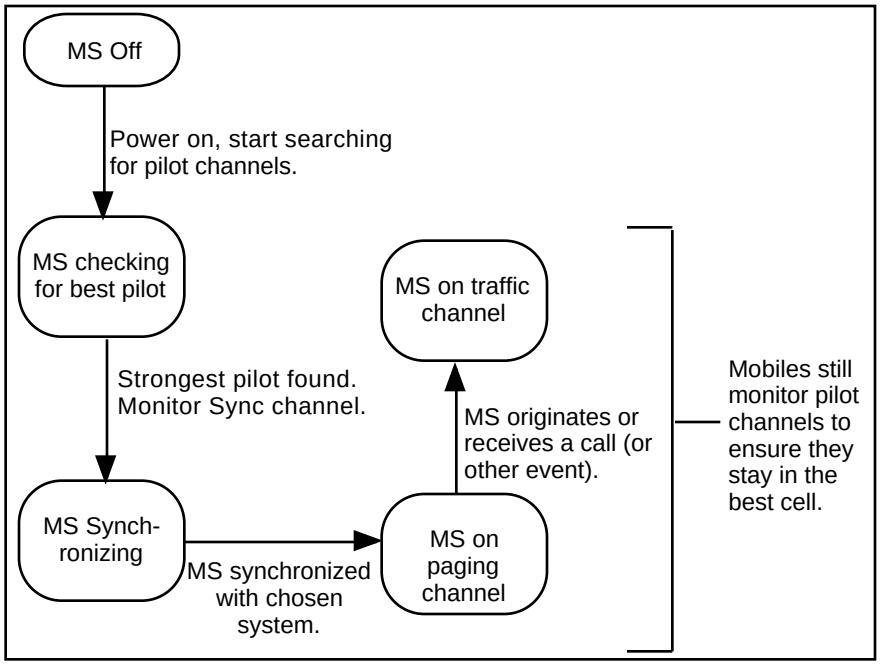

Figure 3: The path to enlightenment for a CDMA mobile

three different sets, while also transmitting and receiving on a traffic channel:

- Active Set
  These are the cells and sectors that a mobile is currently communicating with on a traffic channel. A mobile with an active set of more than one pilot is in "soft handoff". The maximum number of active sectors is 6.
- Candidate Set
  These are the cells that a mobile is thinking of handing off to, if they get stronger than those currently in its active set.
- Neighbour Set
  These are the cells that are potential future handoff candidates. They are monitored less often than pilots in the candidate set. If the signal strength increases enough, they can be moved to the candidate set.

A mobile on a paging channel also monitors pilot channels, performing an "idle handoff" to another pilot when necessary to stay in the cell with the best signal.

Sync Channel

The Sync channel provides a mobile with basic system parameters required to synchronize with the cell and obtain a paging channel: the system time, revision level of the radio interface, the SID (System ID code), the NID (Network ID code) and the paging rate. It also contains the PN ("Pseudo-Random Noise Code") offset of the associated pilot channel, which is used to associate the timing information received on the pilot channel with the system clock. Once a mobile has received a full set of information from the sync channel it will move to a paging channel.

Paging Channel

Messages to a specific mobile and most system parameters are transmitted on a paging channel, of which there may be up to 7 in a sector in any RF channel. Mobiles are assigned to paging channels by a hash function based on the MIN (i.e. pseudo-randomly). Typical messages on the paging channel include pages, traffic channel assignments and short messages.

Forward Traffic Channel

The forward traffic channels are used to transmit voice or data at a rate up to 9600 bps (with a new option of up to 14.4 kbps) to a mobile that is in a call. There may be up to 63 in each cell (depending on the number of paging channels and the presence of a sync channel).

Sometimes it is necessary for a BS to transmit signaling information to a MS during a call. In this case, it can be transmitted using "blank and burst" (interrupting the voice) or "dim and burst" (reducing the voice quality, at the expense of a longer transmit time).

Reverse Channel (Mobile to Base)

Access Channel

The access channel allows a mobile to communicate with the system when it is not in a call. This is required for a mobile to initiate an autonomous action (e.g. register or originate a call) and to respond to messages received on a paging channel (e.g. a response to a page or an acknowledgement of a short message). The access channel implements a contention management system, as multiple terminals may attempt to access at the same time. The access channels run at 4800 bps. The number in each cell is configurable. There will usually be one or two access channels associated with each paging channel. They are spread by a long code based on several parameters forming an identity unique to the access channel. This eliminates a number of "border cell" problems as messages received by the wrong access channel cannot be decoded.

Reverse Traffic Channel

Reverse traffic channels are used to transmit voice or data from a mobile to a base station. Each one is paired with a corresponding forward traffic channel. Signaling information can be transmitted in the same way as on the forward traffic channel (i.e. using "blank and burst" or "dim and burst").

Acknowledgements

I would like to acknowledge the assistance of Dr. Edward Tiedemann, Alejandro Holcman and Sam Broyles, all of Qualcomm.

In our next issue, we will be continuing our discussion of CDMA standards and technology with a description of the basic capabilities of IS-95 and related CDMA systems for handoff, location management and mobile identification. We will describe the basic services available in current standards, and those currently planned for inclusion in IS-95 Rev. B. We will also provide a tabular report of the suite of cellular and PCS CDMA standards that have been developed by the TIA and the TIA/ATIS Joint Technical Committee.❑

Table 3: IS-95 Channel Structure

Forward Channel	Channel Purpose	Number per Cell	Maximum Rate/bps	Modulation Code
Pilot	System Monitoring	1	n/a	Walsh code 0
Sync	System Synchronization	0 or 1	1200	Walsh code 32
Paging	BS-> Idle MS Signaling	up to 7	9600	Walsh code
Traffic	BS->MS Voice or Data	up to 63	9600/ 14400	Walsh code
Reverse Channel				
Access	Idle MS->BS Signaling	up to 14 (usually)	4800	System parameters
Traffic	MS->BS Voice or Data	up to 63	9600/ 14400	Long code mask (private or public)

Status of IS-41 Rev. B Implementation

Cellular Networking Perspectives

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

Vendor1	Vendor2	Status	Date	Type	Location
Alcatel SEL	Astronet*	Commercial	08/94	H V D S	Mobile, Alabama (BellSouth)
	AT&T	Commercial	2Q'95	H V D S	Orlando, Florida (BellSouth)
	EDS PC	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
	GTE TSI	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
	Motorola	Commercial	2Q'95	H V D S	Richmond, Virginia (BellSouth)
	Nortel	Commercial	2Q'95	H V D S	Mobile, Alabama (BellSouth)
Astronet*	AT&T	Field Trial		V DX	Hoffman Estates, IL (Ameritech)
AT&T	Alcatel SEL	Field Trial	03/95	H+ V D S	South Florida (BellSouth)
	GTE TSI*	Planning		V DX S	*Location not announced (BAM)*
	NEC	Commercial		H V D S	Brazil
	Nortel	Planning		H+ V DX T	*Location not announced*
Celcore	Alcatel SEL	Field Trial	01/96	H V D S	Yorkville, TN RSA
	AT&T	Field Trial	09/95	H V DX	Cleveland, Ohio (GTE Mobilnet)
	Ericsson	Field Trial	09/95	V D S	Chicago (Cellular One)
	GTE TSI*	Commercial	10/95	V DX	Yorkville, TN RSA
	Motorola	Field Trial	12/95	V DX	Little Rock, AR (Alltel)
	Nortel	Lab Trial	12/95	V D S	Toronto (Bell Mobility)
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/NovAtel		Development	01/96	V DX	*Location not announced*
Motorola	Alcatel SEL	Commercial	2Q'95	H V D S	*Multiple locations*
	Astronet*	Commercial	4Q'94	V DX	*Multiple locations*
	AT&T*	Commercial		V D S	*Multiple locations*
	EDS PC*	Commercial		V X	Dedham, MA
	Ericsson*	Commercial		V D S	*Multiple locations*
	GTE TSI*	Commercial		V DX	*Multiple locations*
	NEC	Commercial		V D S	Brazil
	Nortel (MTX)*	Commercial		H V DX	Denver, CO
	Nortel(800CM)*	Commercial		V DX	Raleigh, NC
NEC	AT&T	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
	AT&T	Lab Trial	TBD	H V DX	Windsor (Bell Mobility)
	NEC	Commercial	2Q'94	H V D S	Brazil
Plexsys	AT&T	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
	Ericsson	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
	GTE TSI*	Commercial	2Q'95	V DX	San Maarten(V) / Tennessee(D)
	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	GTE TSI*	Field Trial	1Q'96	V D X	Vancouver, BC (BC Tel)
	Nortel	Lab Trial	1Q'96	V D X	Vancouver, BC (BC Tel)

Explanation:

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