TICOM

TECHNICAL INTELLIGENCE COMMUNICATIONS

Issue #1, February 2005

http://www.iirg.net/~ticom/zine/ - email: ticom@iirg.net

CONTENTS:

Experiments in Spread Spectrum Interception

Having an interest in unusual and "exotic" communications equipment, I recently acquired a Transcrypt SC-1000 frequency hopping spread spectrum (FHSS) transceiver at a local hamfest (It pays to check them out. You never know what you might find.). FHSS is used as a means of combating jamming and signal interception in a few communications systems. The biggest one that comes to mind is SINCGARS (Single Channel Ground/Air Communications System) used by the U.S. Military. I wanted to see just how secure it is against commonly available commercial off-the-shelf equipment. The unit operated in the VHF-high band, and when not in "comsec mode" was a single channel frequency agile transceiver operating in the 163-173 Mhz. Range. The following pieces of equipment were used in evaluating the transceiver:

- Information Security Associates ECR-1 TSCM receiver/spectrum analyzer
- Optoelectronics R-10 Interceptor near field receiver
- Icom R-10 communications receiver
- Aceco FC3002 frequency counter (reaction tune capability with Icom receiver)

The objectives of this exercise were to determine how easily it would be to detect the FHSS signal, and to see if it were possible to actually hear the transmitted audio while in FHSS mode. The first step was to fire the thing up in single channel mode, make sure it worked, and make sure the test equipment worked. The transceiver was attached to a dummy load, and keyed up in single channel mode. It was a stock VHF-high FM transceiver. The ECR-1 showed a nice spike on the screen, the Opto Interceptor locked on the signal, and the Aceco frequency counter registered a hit and tuned the Icom R-10 to the frequency. No problem. Now for things to get interesting.

I flipped the "comsec mode" switch to "on", and keyed the thing up. The first thing I noticed was that the frequency counter and Icom receiver reaction-tune combo did not detect a signal. That was no surprise. The FHSS signal hopped too quickly for the counter to get a lock, yet alone tune a receiver via a 9600 baud TTL serial link. Optoelectronics is currently selling a "Digital Scout" that allegedly has the capability to measure TX frequency on FHSS signals. Since I don't have one handy to evaluate, it remains to be seen how well it would work. Taking the Aceco out of "capture mode" and using it as a regular frequency counter however would result in the frequency display showing a signal within 500 KHz.-1 MHz. The counter had to be within a foot of the transmitter (keying into a dummy load though) to get this reading however.

The next piece of test equipment I checked was the ECR-1. The spectrum display clearly showed a nice FHSS signal. One could even narrow the display down to the 10 MHz. of spectrum the transceiver operated on, and make out individual frequencies in the hopping pattern. The receiver's sweep speed, however was not quick enough to make out the audio of the transmitter while it was in FHSS mode. All one heard was a "popping" sound above the squelch noise. A FHSS signal makes a distinguishable pattern on a spectrum display, provided one is looking at a wide enough chunk of the spectrum. If I went down to too narrow a display, I wound up "missing" parts of the hopping sequence, and an unskilled operator may overlook the signal. Interestingly enough, on a wide enough sweep range, I could make out the second harmonic of the transmitter hopping in time to the fundamental frequency.

Finally there was the surprise of the experiment. The Optoelectronics R-10 Interceptor continually locked on to, and followed the FHSS signal. The sweep speed of the R-10 was quick enough to allow one to hear the transmitted audio! It wasn't perfect. The audio sounded "clipped" as the Interceptor was still playing catch-up. The Interceptor near field receiver would lock onto any strong local signal, and this would result in losing the FHSS signal. Upon hitting the skip button on the Interceptor however, it would shortly reacquire the signal. The evaluation was done in a rural area where there were few "near field" signals, which meant there was little for the Interceptor to lock onto. This technique would probably be less effective in an urban area with more radio traffic. The lack of a delay period before resuming its sweep proved to be a handy feature for tracking the FHSS signal well enough to hear the transmitted audio. The Interceptor is a neat piece of equipment that many clueless hobbyists didn't understand, but the pros knew better. It harks back to the days before the cellular phone companies managed to pay off enough CONgressmen (congress is the opposite of progress) to declare 54 MHz. of spectrum "private" (as if passing a law would do that), and a symbol of eliteness was a 2135 key. (I wonder how many modern "hackers" play around with items that require a 2135 key, or even real-world locks these days?)

In conclusion, FHSS is readily detectable and even able to be monitored under certain circumstances depending on available equipment and other factors. There are few things a skilled operator with a spectrum analyzer cannot detect; which is probably why it is the number one piece of equipment used for RF sweeps by TSCM pros. The transceiver I used for the evaluation only operated in a small 10 MHz. piece of RF spectrum. SINCGARS transceivers have 58 MHz. of operating space, so I suspect monitoring more modern FHSS equipment would be more difficult. Additionally, encrypting the signal with a good cryptographic system would prevent communications from being monitored (but not detected); which is the case with the latest SINCGARS units. Frequency hopping spread spectrum initself does offer security against the common scanner dweeb and others using less sophisticated monitoring equipment and techniques.

4. Circuit Identification and Interface Code Descriptions

4A. Circuit Identification

New Common Language Circuit Identifiers (CLCI) are provided to allow discrete identity for LATA Access Services. The following example and tables are referenced in BSP 795-402-100 which is currently being revised.

Telephone Number Format

PREFIX		SERVICE CODE		MODIFIER		NPA CODE		
1	2	3	4	5	6	7	8	9

Serial Number Format

PREFIX		SERVICE CODE		MODIFIER		SERIAL NUMBER					
1	2	3	4	5	6	7	8	9	10	11	12

Service Codes
Character Position 3-4

USE	CODE	USE	CODE
Switched		Tele-	TV
Access	SB	vision	TW
	NT		WJ
	NV	Wide	WQ
Narrow	NV	Band	WL
Band	NW	Analog	WR
	NY		WN
	LB		WP
	LC	Dedicated	SE
	LD	Access	SF
	LE	Wide	WB
	LF	Band	WE
Voice	LG	Digital	WF
Band	LH		WH
	LJ		XA
	LK	DDS	XB
	LN		XC
	LP		XH
	LR	Sub	RB
	LU	Rate	RC
Program	PE	Mpx	RC
Audio	PF	Digital	HC-HD
	PJ	High	HE-HF
	PK	Cap	HG

Modifier #1
Character Position 5

INTERLATA INTRASTATE	INTERLATA INTERSTATE	CODE DESCRIPTION
F	G	ALL SVC TYPES DATA AND VOICE

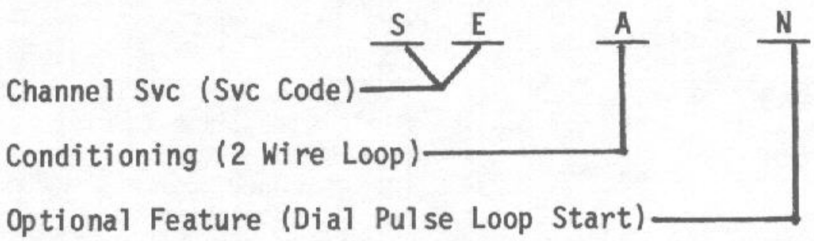
Modifier #2
(Character Position 6)

SPL ACC SVC EXCEPT GOV'T	SPL ACC SVC GOV'T SVC	CODE DESCRIPTION
S	M	All Fax and equip. excluding IC is BOC provided.
S	P	Part of the Fax and equip. excluding IC and equip. is CPE.
S	J	All Fax are BOC provided except IC and equip. is CPE.
S	S	CKT terminates in an interface for connection to an IC or connects to Fax provided to an IC.
V	V	CKT terminates in an Interface for connection to a radio common carrier (RCC)
S	F	CKT directly connects to a channel of CPE communication system within the LATA
S		Official service (refer to tariff.)

4B. Network Channel Codes (NC)

The NC codes describe the conditioning and features related to the LATA Access circuit. The code is 4 characters in length and divided into three fields that represent the parameters of the basic channel (i.e., Service Grade, Conditioning and features). The first two characters of code are actually the new switched or dedicated access service codes.

An example of an NC code is as follows:



The following tables reflect NC code availability.

Table	I -	Switched Services
	II -	Special Access Service, Dedicated Access Lines
	III -	Narrowband Special Access Service
	IV -	Voicegrade Special Access Service
	V -	Program Audio Special Access Service
	VI -	Television Special Access Service
	VII -	Wideband Analog Special Access Service
	VIII -	Wideband Digital Special Access Service
	IX -	Digital Access Channel
	X -	High Capacity
	XI -	Digital Subrate

NC CODES

TABLE I

SWITCHED ACCESS

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
Transmission Grade B (4W Interface)	SD	-Second Dial Tone	F	FEATURE GROUP A	
		-Foreign Dial Tone	G	TWO WAY	
		-Private Switch Network	H	-Dial Pulse Loop Start	A
Transmission Grade C (2W Interface)	SB			-Dial Pulse Ground Start	E
				-DTMF Loop Start	F
				-DTMF Ground Start	G
				TERMINATE ONLY	
				-Dial Pulse Loop Start	N
				-Dial Pulse Ground Start	P
				-DTMF Loop Start	R
				-DTMF Ground Start	S
				ORIGINATE ONLY	
				-Loop Start	U
				-Ground Start	V
		None	-	FEATURE GROUP B	
				-Multi Frequency	B
				-Rotary Dial Station Signalling	H
				FEATURE GROUP C	
				-Multi Frequency	C
				-Dial Pulse	M
				FEATURE GROUP D	
				-Multi Frequency	D
				FEATURE GROUP E	
				-Multi Frequency	K
				-Dial Pulse	L
				DIRECTORY ASSISTANCE	J
* Transmission Grade A	SH	None	-	FEATURE GROUP D	
				-Multi Frequency	D
				DIRECTORY ASSISTANCE	J

*Transmission Grade A is not applicable for Embedded Circuits.
Transmission Grade A is only available with Feature Group D and Directory Assistance.

TABLE II

SPECIAL ACCESS SERVICE - DEDICATED ACCESS LINES (DIAL)

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
Standard DAL	SE	- 2W Loop	A	OUTWATS	
		- 4W Loop	B	-Dial Pulse Loop Start	N
				-Dial Pulse Ground Start	P
Improved DAL	SF			-DTMF Loop Start	R
				-DTMF Ground Start	S
				800 SERVICE:	
				-DNIS	T
				-Loop Start	U
				-Ground Start	V
				TWO WAY	-
				NONSTANDARD	Z

TABLE III

NARROWBAND SPECIAL ACCESS SERVICE

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
NB1	NT	NONE	-	BRIDGING	B
				NONSTANDARD	Z
				NONE	
NB2	NU				
NB3	NV				
NB4	NW				
NB5	NY				

TABLE IV

VOICE GRADE SPECIAL ACCESS SERVICE

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
VG1	LB	NONE	-	Effective 4W Imp. 4W R.L. @ POI + EFF. 4W Nonstandard None	A D Z -
VG2	LC	NONE	-	Effective 4W CO Bridging Imp. R.L. for EFF 2W Imp. 4W R.L. @ POI + EFF. 4W A + B B + C B + D Nonstandard None	A B C D F G E Z -
VG3	LD	None	-	Effective 4W Imp. R.L. for EFF 2W Imp. 4W R.L. @ POI + EFF. 4W Nonstandard None	A C D Z -
VG4	LE	None	-	Imp. 4W R.L. @ POI for EFF. 4W Nonstandard None	D Z -
VG5	LF	BRIDGING MODIFIERS *DSAS -2 Wire .Addressable .A + C .Sequential .S + C -4 Wire .Addressable .X + C .Sequential .Y + C #TABS -Split Band Active .F + C -Passive Bridging .P + C -Summation Active .B +,C C Conditioning None	 A G S H X J Y K F L P M B N C -	Effective 4W CO Bridging Imp. 4W R.L. @ POI + EFF. 4W A + B B + D Nonstandard None	A B D F E Z -

*DataPhone Select-A-Station
#Telemetry and Alarm Bridging

TABLE IV (cont'd)

VOICE GRADE SPECIAL ACCESS SERVICE

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
VG6	LG	C Cond	C	CO Bridging	B
		D Cond	D	Imp. 4W R.L. @ POI + EFF. 4W	D
		C + D Cond	E	CO Multiplexing Voice to Narrowband	M
		None	-	B + D	E
				D + M	J
				Nonstandard	Z
				None	-
VG7	LH	C Cond	C	Effective 4W	A
		D Cond	D	Imp. R.L. for EFF. 2W	C
		C + D Cond	E	Imp. 4W R.L. @ POI + EFF. 4W	D
		None	-	Nonstandard	Z
				None	-
VG8	LJ	C Cond	C	Imp. 4W R.L. @ POI for EFF. 4W	D
		None	-	Nonstandard	Z
				None	-
VG9	LK	C Cond	C	Imp. 4W R.L. @ POI for EFF. 4W	D
		None	-	Nonstandard	Z
				None	-
VG10	LN	C Cond	C	CO Bridging	B
		D Cond	D	Imp. 4W R.L. @ POI for EFF. 4W	D
		C + D Cond	E	B + D	E
		None	-	Nonstandard	Z
				None	-
VG11	LP	TA (Telephoto)	Z	Effective 4W	A
		None	-	CO Bridging	B
				Imp. 4W R.L. @ POI with EFF. 4W	D
				A + B	F
				B + D	E
				Nonstandard	Z
				None	-

TABLE IV (Cont'd)

VOICE GRADE SPECIAL ACCESS SERVICE

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
VG12	LR	None	-	Effective 4W CO Bridging Imp. 4W R.L. @ POI with EFF. 4W A + B B + D Nonstandard None	A B D F E Z -
VG13	LU	None	-	Nonstandard None	Z -

TABLE V

PROGRAM AUDIO SPECIAL ACCESS SERVICE

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
AP1	PE	Gain Conditioning None	P -	Bridging Nonstandard None	B Z -
AP2	PF				
AP3	PJ				
AP4	PK	Gain Conditioning None	P -	Bridging Stereo B + S Nonstandard None	B S K Z -

TABLE VI

TELEVISION SPECIAL ACCESS SERVICE

TV1	TV	None	-	Nonstandard None	Z -
TV2	TW				

NOTICE
Not for use or disclosure outside the sponsoring Regional Bell Operating Companies except under written agreement.

TABLE VII

WIDEBAND ANALOG SPECIAL ACCESS SERVICE

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
WA1	WJ	None	-	CO Multiplexing Nonstandard None	M Z -
WA1T	WO				
WA2	WL				
WA2A	WR				
WA3	WN	None	-	Nonstandard None	Z -
WA4	WP				

TABLE VIII

WIDEBAND DIGITAL SPECIAL ACCESS SERVICE

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
WD1	WB	None	-	Nonstandard None	Z -
WD2	WE				
WD3	WF				
WD4	WH				

TABLE IX

DIGITAL ACCESS CHANNEL SPECIAL ACCESS SERVICE

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
DA1	XA	None	-	Bridging Transfer Arrangement CO Multiplexing B + T B + M B + M + T Nonstandard None	B T M U X V Z -
DA2	XB				
DA3	XG				
DA4	XH				

TABLE X

HIGH CAPACITY SPECIAL ACCESS SERVICE

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
HC1	HC	None	-	Auto Protection Switching	P
				CO DS1 to Voice Multiplexing	M
				P + M	N
				CO DS1 to DS0 Multiplexing	L
				P + L	H
				Nonstandard	Z
				None	-
HC1C	HD	None	-	CO Multiplexing	M
				Nonstandard	Z
				None	-
HC2	HE				
HC3	HF				
HC4	HG				

TABLE XI

DIGITAL SUBRATE SPECIAL ACCESS SERVICE

CHANNEL SERVICE	CODE	CONDITIONING	CODE	OPTIONAL FEATURE	CODE
SR1	RB	None	-	Multiplexing	M
SR2	RC				
SR3	RD				

4C. Network Channel Interface (NCI) Codes

The NCI describes the electrical conditions, on the access circuit, at the POP interface and at the customer premise interface. An NCI code is not provided on switched access at the switched (open) end of the circuit.

LATA access service WORD documents list the NCI at the POI and NI. The following describes NCI make-up and codes.

The NCI is made up of five elements;

1. Physical conductors (2 numeric characters)
   - describes the number of wires that transverse the interface (See Table 1 for codes)
2. Protocol (2 alpha characters)
   - identifies the signaling and/or transmission characteristics at the interface (See Table 2) for codes
3. Impedance (1 numeric character)
   - identifies the nominal reference impedance termination of the channel (See Table 3 for codes)
4. Protocol Options (3 alphanumeric characters)
   - describes options applicable to protocol codes (Not all protocols have options) (See Table 2 for codes)
5. Transmission Level Point (TLP) (2 alpha characters)
   - the TLP at the interface one for transmit level, one for receive level (See Table 4 for codes)

An example of an NCI code is as follows:

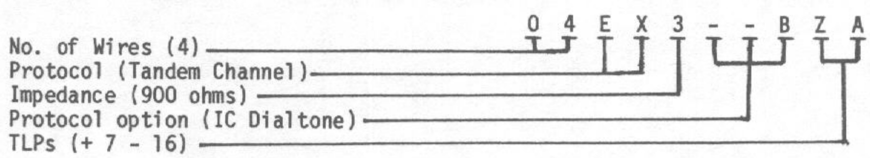


TABLE 1

TOTAL WIRES

NUMBER OF WIRES	CODE
2	02
4	04
6	06
7	07
8	08
9	09
10	10
12	12

TABLE 2

PROTOCOL CODES AND OPTIONS

Code	Option	Definition
AB -		accepts 20 Hz ringing signal at IC point of interface
AC -		accepts 20 Hz ringing signal at end user network interface
AH -		analog high capacity interface
- B		60 kHz to 108 kHz (12 channels)
- C		312 kHz to 552 kHz (60 channels)
- D		564 kHz to 3084 kHz (600 channels)
DA -		data stream in VF frequency band at end user network interface
DB -		data stream in VF frequency band at IC point of interface
-	10	VF for NW and NY service codes
-	43	VF for 43 Telegraph Carrier type signals, NW and NY svc. codes
DC -		direct current or voltage
-	1	monitoring interface with series RC combination (McCulloh format)
-	2	Telephone Company energized alarm channel
-	3	Metallic facilities (DC continuity) for direct current/low frequency control signals or slow speed data (30 baud)
DD -		DATAPHONE Select-A-Station (and TABS) interface at IC point of interface
DE -		DATAPHONE Select-A-Station (and TABS) interface at the user NI
DO -		digital interface at IC terminal location at the digital signal level zero A (DS-0A)
DS -		digital hierarchy interface
-	15	1.544 Mbps (DS1) format per PUB41451 plus D4
-	15E	8-bit PCM encoded in one 64 kbps of the DS1 signal
-	15F	8-bit PCM encoded in tow 64 kbps of the DS1 signal
-	15G	8-bit PCM encoded in three 64 kbps of the DS1 signal
-	15H	14/11-bit PCM encoded in six 64 kbps of the DS1 signal
-	15J	1.544 Mbps format per PUB 41451
-	15K	1.544 Mbps format per PUB 41451 plus extended framing format
-	15L	1.544 Mbps (DS1) with SF signaling
-	27	274.176 Mbps (DS4)
-	27L	274.176 Mbps (DS4) with SF signaling
-	31	3.152 Mbps (DS1C)
-	31L	3.152 Mbps (DS1C) with SF signaling
-	44	44.736 Mbps (DS3)
-	44L	44.736 Mbps (DS3) with SF signaling
-	63	6.312 Mbps (DS2)
-	63L	6.312 Mbps (DS2) with SF signaling

Code	Option	Definition
DU -		digital access interface at end user premises
-	24	2.4 kbps
-	48	4.8 kbps
-	56	56.0 kbps
-	96	9.6 kbps
-	A	1.544 Mbps format per PUB 41451
-	B	1.544 Mbps format per PUB 41451 plus D4
-	C	1.544 Mbps format per PUB 41451 plus extended framing format
DX -		duplex signaling interface at IC POI
DY -		duplex signaling interface at end user NI
EA -	E	Type I E&M Lead Signaling. IC at POI or end user at NI originates on E Lead.
EA -	M	Type I E&M Lead Signaling. IC at POI or end user at NI originates on M Lead.
EB -	E	Type II E&M Lead Signaling. IC at POI or end user at NI originates on E Lead.
EB -	M	Type II E&M Lead Signling. IC at POI or end user at NI originates or M Lead.
EC -		Type III E&M signaling at IC terminal POI
EX -	A	tandem channel units signaling for loop start or ground start and IC supplies open end (dial tone, etc.) functions.
EX -	B	tandem channel unit signaling for loop start or ground start and IC supplies closed end (dial pulsing, etc.) functions.
GO -		ground start loop signaling - open end function by IC or end user
GS -		ground start loop signaling - closed and function by IC or end user.
LA -		E.I.A. (25 pin RS-232)
LA -		end user loop start loop signaling - Type A OPS registered port open end
LB -		end user loop start loop signaling - Type B OPS registered port open end
LC -		end user loop start loop signaling - Type C OPS registered port open end
LO -		loop start loop signaling - open end function by IC or end user
LR -		20 Hz automatic ringdown interface at IC with Telephone Company provided PLAR
LS -		loop start loop signaling - closed end function by IC or end user
NO -		no signaling interface, transmission only
PG -		program transmission - no dc signaling
-	1	nominal frequency from 50 to 15000 Hz
-	3	nominal frequency from 200 to 3500 Hz
-	5	nominal frequency from 100 to 5000 Hz
-	8	nominal frequency from 50 to 8000 Hz

Code	Option	Definition
RV -	0	reverse battery signaling, one way operation, originate by IC
-	T	reverse battery signaling, one way operation, terminate function by IC or end user
SF -		single frequency signaling with VF band at either IC POI or end user NI
TF -		telephotograph interface
TT -		telegraph/teletypewriter interface at the IC POI or end user NI
-		20.0 milliamperes
-		3.0 millamperes
-		62.5 milliamperes
TV -		television interface
-		combined (diplexed) video and one audio signal
-		combined (diplexed) video and two audio signals
-		video plus one (or two) audio 5 kHz signal(s) or one (or two) two wire
-	15	video plus one (or two) audio 15 kHz signal(s)
WA -		wideband bandwidth interface at end user NI
-	1	limited bandwidth
-	2	nominal passband from 29000 to 44000 Hz
WB -		wideband data interface at IC POI
-	18S	18.75 kbps, synchronous
-	19A	up to 19.2 kbps asynchronous
-	19S	19.2 kpbs synchronous
-	23A	up to 230.4 kbps, asynchronous
-	23S	230.4 kbps, synchronous
-	40S	40.8 kbps, synchronous
-	50A	up to 50.0 kbps, asynchronous
-	50S	50.0 kpbs, synchronous
-	64	64.0 kbps, restored polar
WC -		wideband data interface at end user NI
-	18.75	kbps, synchronous
-	19	for 12-wire interface: 19.2 kbps, synchronous for 10-wire interface: up to 19.2 kbps, asynchronous
-	23	up to 230.4 kbps, asynchronous
-	23S	230.4 kbps, synchronous
-	40	40.8 kbps, synchronous
-	for	12-wire interface: 50.0 kbps, synchronous for 10-wire interface: up to 50.0 kbps, asynchronous
WD -		wideband bandwidth interface at IC POI
-	1	nominal passband from 300 to 16000 Hz
-	2	nominal passband from 28000 to 44000 Hz
-	3	nominal passband from 29000 to 44000 Hz

TABLE 3

IMPEDANCE

The nominal reference impedance with which the IC or end user will terminate the channel for the purpose of evaluating transmission performance:

Value (ohms)	Code(s)
110	0
150	1
600	2
900	3+
1200	4
135	5
75	6
124	7
Variable	8
100	9

\+ For those interface codes with a 4-wire transmission path at the POI at the IC's terminal location, rather than a standard 900 ohm impedance the code (3) denotes an IC provided transmission equipment termination. Such terminations were provided to ICs in accordance with the F.C.C. Docket No. 20099 Settlement Agreement.

TABLE 4

TRANSMISSION LEVEL POINT CODE FOR INTERFACE LEVELS

TLP	CODE(S)
-16.0	A
-15.0	B
-14.0	C
-13.0	D
-12.0	E
-11.0	F
-10.0	G
- 9.0	H
Refer to TLV (S&E section)	(I)
- 8.0	J
- 7.0	K
- 6.0	L
- 5.0	M
- 4.0	N
- 3.0	P
- 2.0	Q
- 1.0	R
0.0	S
+ 1.0	T
+ 2.0	U
+ 3.0	V
+ 4.0	W
+ 5.0	X
+ 6.0	Y
+ 7.0	Z