Technical Note



Getting Started with Message Coder

How to analyze L3 Messages

MD8480C W-CDMA Signalling Tester







What is Message Coder?

Message Coder^{*1} is a software tool for creating and analyzing higher-layer messages exchanged between GSM/WCDMA base stations and mobile terminals.

^{*1}: The MD8480C includes this message encode/decode tool for scenario creation and analysis.



Category	Message	Reference Spec. *1
RRC	RRC Layer	3GPP TS25.331
NAS	NAS Layer	3GPP TS24.007, TS24.008
Config	Layer 1, Layer 2 Control	
RLC/MAC Control	RLC/MAC Control	3GPP TS04.60
SS	Supplementary Service	3GPP TS24.080
SMS	SMS (SM-RL/SM-TL)	3GPP TS23.040
CBS	CBS	3GPP TS23.041, TS25.324
Layer 3 Me	ssages *2	Reference Spec. *1
сс	Messages for Circuit-switched Call Control (35)	3GPP TS24.008, 9.3
MM	Messages for Mobility Management (22)	3GPP TS24.008, 9.2
GMM	GPRS Mobility Management Messages (23)	3GPP TS24.008, 9.4
SM	GPRS Session Management Messages (16)	3GPP TS24.008, 9.5
SMS	Messages for Short Message or Notification Transfer on CM (3)	3GPP TS24.001, 7.2
RR	Messages for Radio Resource Management (82)	3GPP TS04.18, 9.1
SS	Messages for Supplementary Services Control (3)	3GPP TS24.080, 2.2

*1: Bunoled RKC and NAS definition files are standardized by 3GPP in June 2001 (R99), March 2002 (R99), March 2002 (R99), and December 2005 (Rel. 5), RRC definition files standardized in June 2006 (Rel. 6) are also bundled.
*2: High-layer protocols in messages are not supported.

MD8480C-E-E-5

Slide 4





Analyzing RRC Messages from Trace W	Vindow
Message Coder decodes RRC Messages from the fol messages on the Trace window.	llowing
Uplink CCCH (U_CCCH-U_RACH): rrcConnectinR Downlink CCCH (D_CCCH-D_FACH): rrcConnectinS Uplink DCCH (U_DCCH-U_DCH): rrcConnectinSe Downlink DCCH (D_DCCH-D_DCH): rrcConnectinRe	Request Setup etupComplete elease
 Procedure Select the target message in the Trace window. Copy message data from the primitive details parti window. Paste the data to the Message View Area in Message Press the Decode button in Message Coder. View the message details in the Tree View Area in I 	ition in the Trace ge Coder. Message Coder.
Discover What's Possible™ MD8480C-E-E-5 Slide 6	/inritsu

TIOBLOSS TIME SIGVE			eLoguon	rile(I) macerinter(I) mace
Message Progress Time	Channel	Primitive	BTS	PHY MAC RLC TE RRC NAS
000000383 000000385 000000385 000002852 000002852 000002855 0000002855 000002855 0000002855 000002855 0000002855 0000002855 000002855 0000002855 0000002855 0000002855 0000002855 0000002855 0000002855 0000002855 0000002855 000000285 000000285 000000285 000000285 000000285 000000285 000000285 000000285 000000285 0000000000	D BCH 0 D BCH 0 D BCH 0 U RACH 0 U CCCH 0 D CCCH 0 D CCCH 0 D DCCH 0 D DPCH 0 D DPCH 0 D DPCH 0 D DPCH 0 D DPCH 0 D DPCH 0 0 DPCH 0 0 DPCH 0 0 DPCH 0	PHY_DATA_REQ PHY_DATA_REQ PHY_DATA_REQ PHY_DATA_REQ PHY_DATA_IND MAC_DATA_IND REC_TR_DATA_IND CRLC_CONFIG_REQ CRLC_CONFIG_REQ CPHY_RLSETUP_REO CPHY_RLSETUP_CNF CMAC_CONFIG_REQ CPHY_RLSETUP_CNF CMAC_CONFIG_REQ COMPCIONFIG_REQ COMAC_CONFIG_REQ COMAC_CONFIG_REQ COMAC_CONFIG_REQ COMAC_CONFIG_REQ COMAC_CONFIG_NF CMAC_	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Message Data [Length=21] ender: 050 Receiver: 060 000 39 01 23 45 67 00

Message Coder: RRC (UL-CCCH-Message) 👿 New Data2 • Setup: RRC VIL-CCCH-Message Make Default Encode Decode Jun2006_Rel6_C RRC Offset=3, Length=2 Hex OC OBin Spacer **UL-CCCH-Message** RRC NAS Config RLC/MAC SMS SS CBS Hex Field Value Туре 😑 UL-CCCH-Message SEQUENCE Spacer 0 ^ - integrityCheckInfo SEQUENCE 😑 message rrcConnectionRequest CHOICE 📄 rrcConn · Paste the data. initialUE-Identity tmsi-and-LAI CHOICE SEQUENCE 🛓 tmsi-and-LAI tmsi 0000000100100011010001... BIT STRING 🖃 lai SEQUENCE • Press Decode. 🛓 plmn-Identity SEQUENCE SEQUENCE OF 🖨 mcc 0 Digit INTEGER Digit 0 Digit INTEGER 1 🖨 mnc 2 SEQUENCE OF UL-CCCH-Message.message.rrcConnectionRequest 39 01 23 45 67 00 10 08 04 03 01 34 10 00 00 00 00 00 00 00 00 /inritsu Discover What's Possible™ Slide 8 MD8480C-E-E-5

File(E) TraceFilter(I) Trace	LogUo	ntrol(<u>C</u>)			Pro	gress Time Save	
PHY MAC RLC TE RRC NAS	BTS	Primitive	Channel		Message	Progress Time	
	1	CRLC_CONFIG_REQ	D DCCH D DCCH	1		000:00:28.72	1-
<	1	CRLC_CONFIG_REQ	D DCCH	2		000:00:28.74	
	1	CRLC_CONFIG_CNF	D DCCH	2		000:00:28.74	+
<	1	CRLC_CONFIG_REQ	D DCCH	3		000:00:28.76	
→	1	CHEC_CONFIG_CNF	D DCCH	3	PRC CONNECTION CETUR	000:00:28.76	
<u></u>	1	HEU_UM_DATA_HEU	D CCCH	0	RECONNECTION SETUP	000:00:28.83	
	4	MAC_DATA_REQ	D CCCH	0		000.00.28.83	
	4	MAC DATA BED	D CCCH	0		000:00:28.83	
	i i	MAC DATA BED	D CCCH	ñ		000.00.28.83	
<u> </u>	1	MAC DATA REQ	D CCCH	0		000:00:28.83	
<u> </u>	1	MAC_DATA_REQ	D CCCH	0		000:00:28.83	-
Message Data (Length=111)						10	
Sender:060 Receiver:050	Type	:00500032 Channel:020	000004 CH_No:0	000	Opt0:0000000 Opt1:00008000	0pt2:00000000	1
00 01 02 03 04 03 0000 30 e7 20 24 68 ac	e0	07 08 09 08 08 00 00 00 02 01 00 80 00 08 00	01 06 50 34	94	3c 09 4f 06 al 00 01 42 16	79 5a Ob 62	
0020 60 ac 2e 74 f0 a5		3a 8c 00 15 18 99 e5				a3 67 95 a2	
0040 b3 c6 8e c2 e7 4f	lk .	53 c7 a9 c0 03 53 20	00 18 94 a3	eÐ	3c 00 90 08 8e 7d 98 27 af	56 9a 0e 08	
0060 00 00 04 12 40 28	00	0 00 02 40 00 08 /o	04		Copy data only		
				24.0	Copy all		3



Message Prog	Channel	Primitive	HY MAC RLC TE RRC NAS BTS
00000 000.00 00.000000	D FACH 0 U DPCH 0 U DCCH 1 U DCCH 1 U DCCH 1 U DCCH 1 D DCCH 1 D DCCH 1 D DCCH 0 U DCCH 0 U DCCH 2 U DCCH 3 U D	PHY_DATA_REQ CPHY_SYNC_IND PHY_DATA_IND MAC_DATA_IND MAC_DATA_IND MAC_DATA_IND MAC_DATA_IND MAC_DATA_REQ PHY_DATA_REQ PHY_DATA_IND MAC_DATA_IND PHY_DATA_IND MAC_DATA_IND MAC_DATA_IND MAC_DATA_IND 200510031 Channel:12 27 08 09 0A 0B 0C 0D 22 aa d5 06 a5 56 a5	Image: Constraint of the state of

Make Default Encode Decode RRC	UL-DCCH-Message		• Setup:
RC NAS Config RLC/MAC SMS SS CBS Field UL-DCCH-Message integrityCheckInfo	Value 0	Type SEQUENCE SEQUENCE	UL-DCCH-Messag Hex Spacer
 message rrcConnectionSetupComplete rrc-TransactionIdentifier startList STARTSingle cn-DomainIdentity start-Value STARTSingle ue RadioAccessCapability pdcp-Capability 	rrcConnectionSetupComplete 101 0 2 cs-domain 0000000000000000100 ps-domain 0000000000000000010 1	CHOICE SEQUENCE INTEGER SEQUENCE OF SEQUENCE ENUMERATED BIT STRING SEQUENCE ENUMERATED BIT STRING SEQUENCE SEQUENCE	 Paste the data. Press Decode.
4a 88 00 01 20 00 05 22 aa d5 06 a5 56 a8 8a 59 80 Discover What's Possible™	68 83 04 08 00 18 00 11 82	2 34 9b Da 94	/inritsu

Trace: D_DCCH (RRC CONNECTION RELEASE)

MAC_DATA_IND PHY_DATA_IND	U DCCH 2		000:00:30.05	+
MAC_DATA_IND RLC_AM_DATA_IND RLC_AM_DATA_REQ PHY_DATA_REQ PHY_DATA_REQ PHY_DATA_REQ PHY_DATA_REQ PHY_DATA_IND MAC_DATA_IND RLC_UM_DATA_IND PHY_DATA_IND MAC_DATA_IND 00500032 Channe1:0200 7 08 09 00 ab 00 co to Copy data only Copy all	U DCCH 2 U DCCH 2 D DCCH 2 D DCCH 2 D DCCH 0 D DCCH 0 D DCCH 0 D DCCH 0 U D	GMM: ATTACH COMPLETE RRC CONNECTION RELEASE RRC CONNECTION RELEASE COMPLETE 1 Opt0:00000000 Opt1:00000000 Opt2 13 14 15 16 17 18 19 1A 1B 1C 1E SE.	000:00:33.16 000:00:33.16 000:00:33.16 000:00:33.16 000:00:33.17 000:00:33.18 000:00:33.18 000:00:33.18 000:00:33.18 000:00:33.18 000:00:33.18 000:00:33.30 000:00:33.30 000:00:33.62 000:00:33.62 2: 000:00:00 > 1B 1F	
	MAC_DATA_RED HMY_DATA_RED ALC_UM_DATA_RED ALC_UM_DATA_RED HMY_DATA_RED HMY_DATA_RED HMY_DATA_IND MAC_NATA_IND MAC_NATA_IND MAC_NATA_IND MAC_NATA_I	MAC_DATA_REQ D DCCH 2 HYU_DATA_REQ D DCH 0 AC_DATA_REQ D DCCH 0 MAC_DATA_REQ D DCCH 0 HYU_DATA_REQ D DCCH 0 HYU_DATA_REQ D DCCH 0 HYU_DATA_REQ D DCH 0 HYU_DATA_REQ D DCH 0 HYU_DATA_REQ D DCH 0 MAC_DATA_IND U DCH 0 MAC_DATA_IND U DCCH 0 MAC_D	MAC_DATA_REQ D DCCH 2 HY_DATA_REQ D DCCH 0 AAC_DATA_REQ D DCCH 0 MAC_DATA_REQ D DCCH 0 MAC_DATA_REQ D DCCH 0 PHY_DATA_REQ D DCCH 0 PHY_DATA_REQ D DCCH 0 MAC_DATA_REQ D DCCH 0 PHY_DATA_REQ D DCH 0 MAC_DATA_REQ D DCH 0 MAC_DATA_IND U DCH 0 MAC_DATA_IND U DCCH 0 MAC_DATA_IND U DCCH	MAC_DATA_REQ D DCCH 2 000.00.33.16 HY_DATA_REQ D DCH 0 000.00.33.16 AAC_DATA_REQ D DCCH 0 000.00.33.16 AAC_DATA_REQ D DCCH 0 000.00.33.16 AAC_DATA_REQ D DCCH 0 000.00.33.18 AAC_DATA_REQ D DCCH 0 000.00.33.18 MAC_DATA_REQ D DCCH 0 000.00.33.18 MAC_DATA_REQ D DCH 0 000.00.33.18 MAC_DATA_REQ D DCH 0 000.00.33.18 MAC_DATA_IND U DCH 0 000.00.33.30 MAC_DATA_IND U DCCH 0 000.00.33.00 MAC_DATA_IND U DCCH 0 000.00.33.00 MAC_DATA_IND U DCCH 0 000.00.33.62 MAC_DATA_IND U DCCH 0 000

Message Coder: RRC (DL-DCCH-Message) 🝿 New Data1 • Setup: RRC Make Default Encode Decode RRC DL-DCCH-Message Jun2006_Rel6_C Offset=51, Length=3 **DL-DCCH-Message** Hex OC OBin Spacer Hex RRC NAS Config RLC/MAC SMS SS CBS Field Value Type Spacer SEQUENCE DL-DCCH-Message 1 integrityCheckInfo SEQUENCE messageAuthenticationCode 110110010010011011110... BIT STRING rrc-MessageSequenceNumber · Paste the data. 0 INTEGER 😑 message rrcConnectionRelease CHOICE 🛓 rrcConnectionRelease r3 CHOICE SEQUENCE E 13 0 • Press Decode. SEQUENCE rrcConnectionRelease-r3 10 -rrc-TransactionIdentifier INTEGER 0 n-308 INTEGER 2 releaseCause normalEvent ENUMERATED rplmn-information SEQUENCE laterNonCriticalExtensions SEQUENCE DL-DCCH-Message,message.rrcConnectionRelease.r3.rrcConnectionRelease-r3.releaseCause ec 93 78 35 83 c8 20 /inritsu Discover What's Possible™ Slide 14 MD8480C-E-E-5



Analyzing NAS Messages from Trac	e Window
Message Coder decodes NAS Messages from the messages on the Trace window.	ne following
Uplink DCCH (U_DCCH-U_DCH): GMM, Attac Downlink DCCH (D_DCCH-D_DCH): GMM, AuthenticationAn	hRequest dCipheringRequest
There are two steps to analyze NAS messages.	
 First, analyze in the same way as RRC message Next, extract the NAS message from the decode decode the NAS message. 	es. ed RRC message and
Discover What's Possible™ MD8480C-E-E-5 Slide 16	/inritsu

	BTS Primitive	Channel	Message	Progress Time
	1 MAC_DATA_IND	LILDCCH 2		
\rightarrow	1 DUY DATA IND	TO DOUT Z		000:00:29.14
→		U DCH 0		000:00:29.15
	1 MAC DATA IND	LL DCCH 2		000.00.29.15
	1 PHY DATA IND	и рен о		000.00.29.16
		U DCCH 2		000:00:29:16
		U DCCH 2	GMM: ATTACH BEQUEST	000:00:29:16
	MAC DATA BEO	D DCCH 2	dinin. Ar recirrie goest	000:00:29:16
	1 PHY DATA BED	р рен о		000:00:29:17
			GMM: AuthenticationAndCinheringBE0	000:00:29 25
	MAC DATA BED		anim. Automication Andelphening new	000.00.29.25
	MAC DATA REO			000.00.29.25
	MAC DATA DEO			000.00.23.23
	1 DUY DATA DED			000.00.23.25
Message Data (Length=44.)	I DIM_DAIA_NEQ	ju bun u		000.00.23.20
00 01 02 03 04 05 0000 15 80 84 01 18 40 0020 33 12 65 4b 19 88	06 07 08 09 0A 0B 0C 0 08 17 2a 00 18 50 08 2 00 b8 2a 00 00 40	OE OF 10 11 12 a0 09 1a 2b 38	13 14 15 16 17 18 19 1A 1B 10 07 88 80 04 00 00 68 56 98 19 Copy data only Copy all	1D 1E 1F 54 b8 aa



Message Coder: NAS (GMM, Attach request) 👿 New Data3 • Setup: Make Default Encode Decode NAS GMM,Attach request Jun2006_Rel6_C NAS Hex OC OBin Spacer Options **GMM,Attach request** RRC NAS Config RLC/MAC SMS SS CBS Hex Field Value Type 😑 Attach request DIVISION ^ **No Spacer** 🛓 Skip Indicator 11 Skip Indicator FIX 0 GPRS mobility management protocol discriminat... v • Paste the data. 8 Protocol Discriminator PD 🛓 Attach request Message type v Message type 01 MSG 🛓 MS network capability LV • Press Decode. 😑 Octet1 DIVISION Length of MS network capability contents 2 LEN DIVISION G Octet2-Octet9 🛓 MS network capability value DIVISION GEA1 DIVISION GEA/1 encription algorithm GEA/1 ... CHOICE v 080102E540030A0105F40123456700F1100080000D16D3032A971546624CA96331001705 /inritsu Discover What's Possible™ Slide 19 MD8480C-E-E-5

Trace: D_DCCH (GMM, AuthenticationAndCipherREQ)

		DTC	Drimitium	Channel		Massage	Diamona Tima	1
FRI MAC ALC I		013	Fillinove	Channel		message	Flogless Time	
\rightarrow		1	MAC_DATA_IND	U DCCH	2		000:00:29.15	1
\rightarrow			PHY_DATA_IND	U DCH	0		000:00:29.16	
->			MAC_DATA_IND	U DCCH	2		000:00:29.16	
		1	RLC_AM_DATA_IND	U DCCH	2	GMM: ATTACH REQUEST	000:00:29.16	-
<			MAC_DATA_REQ	D DCCH	2		000:00:29.16	
<u>←</u>		11	PHY_DATA_REQ	D DCH	0		000:00:29.17	
	<u> </u>	1	HLC_AM_DATA_HEQ	D DCCH	2	GMM: AuthenticationAndLipheringHEQ	000:00:29.25	
<hr/>			MAC_DATA_REQ	D DCCH	2		000:00:29.25	
<hr/>			MAC_DATA_REQ	D DCCH	2		000:00:29.25	
<u> </u>			MAC_DATA_REQ	D DCCH	2		000:00:29.25	
<			PHY_DATA_REQ	D DCH	U		000:00:29.26	
<		11	PHY_DATA_REQ	D DCH	U		000:00:29.27	
K			IPHY_DATA_REQ	то осн	0		000:00:29.28	1
00 01 0 0000 14 20 0 0020 7a 00 0	02 03 04 0 4e 10 24 0 00 6a 48 2	5 06 0 0 20 4 a 16 4	17 08 09 0A 0B 0C 0D 12 6a 6a 6a 70 60 66 18 cc ac 84	0E 0F 10 11 60 6a 6a 60	. 12 : 70	13 14 15 16 17 18 19 1A 1B 1C 60 66 61 99 99 00 50 20 16 e8 Copy data only Copy all	1D 1E 1F cc ac 85	
						Copy all		

Message Coder: R	RC(DL-DCCH-Mes	ssage)
Wew Data2 Make Default Encode Decode RRC Make Default Encode Decode RRC Mex OC OBin	DL-DCCH-Message	Setup: RRC DL-DCCH-Message Hex
RRC NAS Config RLC/MAC SMS SS CBS		
DL-DCCH-Message integrityCheckInfo	0 SEQUENCE SEQUENCE	Spacer
message downlinkDirectTransfer downlinkDirectTransfer do r3 downlinkDirectTransfer-r3	downlinkDirectTransfer CHOICE r3 CHOICE 0 SEQUENCE SEQUENCE	Paste the data.
− rrc-TransactionIdentifier − cn-DomainIdentity − nas-Message	0 INTEGER ps-domain ENUMERATED 0812001021353537383033 OCTET STRING	Press Decode.
LaterNonCriticalExtensions	nas-Message OCTET STRING 081200102135353798303305555379830333 0CCC6028100B74665642BD00003524150 B74665642	 Double-click nas- Message.
DL-DCCH-Message.message.downlinkDirectTransfer.r3.c		Copy the entire
14 20 4e 10 24 00 20 42 6a 6a 6e 70 60 66 60 6 e8 cc ac 85 7a 00 00 6a 48 2a 16 e8 cc ac 84	5a 6 Size : (1 4095) Input size : (40) OK Cancel	OCTET STRING data.
<u>k</u>		Press Cancel.
Discover What's Possible™ MD8480C-E-E-5	Slide 21	/inritsu

Message Coder: NAS (GMM, Authentication and ciphering)

GMM,Authentication Type DIVISION
Type DIVISION A Hex
v .
FIX No Spacer
V
PD
A Decto the data
V
DIVISION
• Press Decode .
not requested CHOICE
V
DIVISION
FIX 💽
V



Analyzing System I	nformation from	Trace window
Message Coder decodes messages on the Trace	System Information frow window.	om the following
Downlink BCCH (D_BC Downlink BCCH (D_BC	CH-D_BCH): MasterInfo CH-D_BCH): SystemInfo	rmationBlock prmationBlockType5
There are two steps to Ar	nalyze System Information	۱.
 First, analyze in the sar Next, extract the Syste and decode the Syste 	ne way as RRC message m Information from the de em Information.	s ecoded RRC message
If the System Information	is segmented, it must be	combined.
 Discover What's Possible™ MD8480C-E-E-5	Slide 24	/inritsu

Trace: D_BCCH (SYSTEM INFORMATION-BCH) MasterInformationBlock

	E DOC MAG	DTC	Drimitium	Channe	J	Managa	Program Time	1
THT MAC HEC I		013			2	message		
			CREC_CONFIG_REQ	D PLLH	0		000:00:03.54	-
	⊢>		CHEC_CONFIG_CNF	D PCCH	0	CVCTEM INFORMATION DOLL	000:00:03.54	
	1 N		HLL_IH_DATA_HEQ	D BLCH	0	STSTEM INFORMATION-BUR	000:00:03.61	
			MAL_UATA_HEU	D BUCH	0	CVCTEM INFORMATION BOLL	000:00:03.61	
			HLU_TH_DATA_HEQ	D BUCH	U	STSTEM INFORMATION-BUR	000:00:03.62	
←	-		MAL_UATA_HEU	D BCCH	0	EVETEM INFORMATION DOL	000:00:03.62	
					0	STSTEM INFORMATION BCH	000.00.03.63	
			MAC DATA DED		0		000.00.03.03	
			BLC TR DATA BED	D BCCH	0	SYSTEM INFORMATION.BCH	000-00-03-64	
		1	MAC DATA BED	D BCCH	0	STSTEM INFORMATION BEI	000-00-03-64	
		l i l	RIC TR DATA BED	D BCCH	0	SYSTEM INFORMATION.BCH	000.00.03.65	
		1	PHY DATA BED	D BCH	ñ	STOTEM IN CHIMATION DOT	000:00:03:65	
		1	MAC DATA BEQ	D BCCH	õ		000:00:03.65	-
Message Data (Length=31)	<u>d </u>		CARL CONTRACTOR	190		Less services	
00 01 0000 00 0e	02 03 04 0 00 a7 00 0	1ype 5 06 (0 40 2	17 08 09 0A 08 0C 0D 4 00 00 62 20 32 21	OB OF 10 J 91 98 88 J	.1 12 .8 44	13 14 15 16 17 18 19 1A 18 a8 45 4a 40 10 02 00 00 00 Copy data only Copy all	10 10 18 1F	2
		STF	M INFORM		-B(CH.		

Message Coder: RRC (BCCH-BCH-Message) 1 MasterInformationBlock

Wew Data2	BCCH-BCH-Message	Jun2006_Rel6_C	• Setup: RRC
RRC NAS Config RLC/MAC SMS SS CBS Field BCCH-BCH-Message sfn-Prime payload completeSIB-List CompleteSIB-short sib-Type sib-Data-variable 00 0e 00 a7 00 00 40 24 00 00 62 20 32 21 91 00 00 00	Value Value Value Value 0 completeSIB-List 1 masterInformationBlock 00000000000000010000.	Type SEQUENCE SEQUENCE INTEGER CHOICE SEQUENCE OF SEQUENCE OF ENUMERATED BIT STRING	BCCH-BCH-Message Hex Spacer • Paste the data. • Press Decode.
Discover What's Possible™ MD8480C-E-E-5	Slide 20	6	/inritsu

Message Coder: RRC (BCCH-BCH-Message) 2 MasterInformationBlock



Message Coder: RRC MasterInformationBlock 👿 New Data3 • Open a new MDI MasterInformationBlock Make Default Encode Decode RRC Jun2006_Rel6_C_ window. Offset=0, Length=1 Hex OC O Bin Spacer RRC NAS Config RLC/MAC SMS SS CBS Field • Setup: Value Type 😑 MasterInformationBl RRC mib-ValueTag INTEGER 😑 pimn-Type gsm-MAP CHOICE MasterInformation-🚊 gsm-MAP SEQUENCE j plmn-Identity SEQUENCE **Block** SEQUENCE OF in mcc Digit 0 INTEGER Bin Digit INTEGER 0 Digit INTEGER No Spacer mnc 📄 SEQUENCE OF 2 Digit n. INTEGER INTEGER Digit 1 · Paste the data. SEQUENCE OF sibSb-ReferenceList 5 E SchedulingInformationSIBSb SEQUENCE MasterInformationBlock • Press Decode. /inritsu Discover What's Possible™ Slide 28 MD8480C-E-E-5

Trace: D_BCCH (SYSTEM INFORMATION-BCH) SystemInformationBlockType5 firstSegment

			1			1	
PHY MAC RLC TE RRC NAS	BTS	Primitive	Channe	el	Message	Real Time	
	1	CPHY_RL_SETUP_CNF	D PICH	0		018:04:06.53	-
<hr/>	1	CRLC_CONFIG_REQ	D PCCH	0		018:04:06.54	
→	1	CRLC_CONFIG_CNF	D PCCH	0		018:04:06.54	
<u>←</u>	1	RLC_TR_DATA_REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.61	
←	1	MAC_DATA_REQ	D BCCH	0		018:04:06.61	
→ → → → → → → → → → → → → → → → → → →	1	RLC_TR_DATA_REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.62	
←	1	MAC_DATA_REQ	D BCCH	0		018:04:06.62	
<	1	RLC_TR_DATA_REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.63	
<u>←</u>	1	PHY_DATA_REQ	D BCH	0		018:04:06.63	
<	1	MAC_DATA_REQ	D BCCH	0		018:04:06.63	
<u> </u>	1	RLC TR DATA REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.64	
<u> </u>	1	MAC DATA REQ	D BCCH	0		018:04:06.64	
<u></u>	1	BLC TR DATA REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.65	
	1	PHY DATA BED	D BCH	0		018:04:06:65	
	1	MAC DATA BEQ	D BCCH	ō		018:04:06.65	+
Message Data (Length=31)							
Sender:060 Receiver:050 00 01 02 03 04 05 0000 00 0e 03 67 00 00	Type: 06 0 00 0	00500033 Channel:0200 07 08 09 0A 0B 0C 0D 0 00 16 0c 00 08 00 00 9	0002 CH_No: 08 07 10 1 06 95 80 0	0000	0pt0:00000000 0pt1:0020004 13 14 15 16 17 18 19 1A 1B 1 00 00 00 00 00 00 00 00 00 0 Copy data only Conv all	0pt2:00000000 .C 1D 1E 1F	~
Select SYS	TE			-B(CH.		

Message Coder: RRC (BCCH-BCH-Message) SystemInformationBlockType5 firstSegment

Make Default Encode Deco	de RRC 💽 BCCH-BCH-Me	ssage Jun2006_Rel6_C_	
	Hex ○C ○ Bin Spacer	Offset=24, Length=222	Message
Field	Value	Туре	Hex
BCCH-BCH-Message message sfn-Prime payload firstSegment	0 firstSegment	SEQUENCE SEQUENCE INTEGER CHOICE SEQUENCE	SpacerPaste the data.Press Decode.
sib-Type seg-Count sib-Data-fixed	3 0000010101101100001110101111111111 sib-Data- BIT STRIN	INTEGER INTEGER IIII BIT STRING fixed	 Double-click the sib-Data-variable
BCCH-BCH-Message.message	payload firstSegment.sib-Data-fi # f f c 52 10 f0 29 0c 0a	11011000011101011111111111111111111111	 Copy the entire BIT STRING data
JU UU JC	L	×	Press Cancel.
Discover What's Possible	тм		/incitsi

		Jun2005_F	window.
00000000000000000000000000000000000000	211000000000000000000000000000000000000	000000000000000000000000000000000000000	Setup: RRC Bin No Spacer Paste the data.

Trace: D_BCCH (SYSTEM INFORMATION-BCH) SystemInformationBlockType5 subsequentSegment

		1	1				. 1
PHY MAC RLC TE RRC NAS	BIS	Primitive	Chann	el	Message	Real I	ime
	1	CPHY_RL_SETUP_CNF	D PICH	0		018:04:06.	53
<	1	CRLC_CONFIG_REQ	D PCCH	0		018:04:06.	54
	1	CRLC_CONFIG_CNF	D PCCH	0		018:04:06.	54
<	1	RLC_TR_DATA_REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.	61
<	1	MAC_DATA_REQ	D BCCH	0		018:04:06.	61
	1	RLC_TR_DATA_REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.	62
←	1	MAC_DATA_REQ	D BCCH	0	Conception and the second s	018:04:06.	62
	1	RLC_TR_DATA_REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.	63
<	1	PHY_DATA_REQ	D BCH	0		018:04:06.	63
<	1	MAC_DATA_REQ	D BCCH	0		018:04:06.	63
<	1	RLC_TR_DATA_REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.	64
K	1	MAC_DATA_REQ	D BCCH	0		018:04:06.	64
K	1	RLC_TR_DATA_REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.	65
←	1	PHY_DATA_REQ	D BCH	0		018:04:06.	65
	1	MAC_DATA_REQ	D BCCH	0		018:04:06.	65
Message Data (Length=31)	191 - M. F.		erior anarona				
Sender:060 Receiver:050 00 01 02 03 04 03 0000 00 02 52 05 6c 3;	Type 5 06 1 a 11	:00500033 Channel:020 07 08 09 0A 0B 0C 0D ff 43 ff fc 52 10 f0	00002 CH_No: OE OF 10 J 29 OC OA 8	0000 1 12 0 18	Opt0:00000000 Opt1:00200 13 14 15 16 17 18 19 1A 00 0c 8f f7 bl 7e el 0f	006 0pt2:00000000 1B 1C 1D 1E 1F ro 00 00 3c Copy data only Copy all)
Select SYS Bight-click	TE and	M INFORMA	ATION- v data	BC on	CH. Iv.		

Message Coder: RRC (BCCH-BCH-Message) SystemInformationBlockType5 subsequentSegment

	RRC M BCCH-BCH-Message	Offset=24, Length=222		
RRC NAS Config RLC/MAC SMS	S SS OBS			
Field Val	lue	Туре		
BCCH-BCH-Message		SEQUENCE	Jun2006 Rel6 C	
🚊 message		SEQUENCE		
sfn-Prime 0		INTEGER		
😑 payload 🛛 sub	osequentSegment	CHOICE		
😑 subsequentSeg		SEQUENCE	be	
_sib-Type sys	temInformationBlockType5	ENUMERATED		
- segmentindex 1		INTEGER		
RCCH RCH Maccade maccade and	100001010011001	000010100101000000000000000000000000000		
BCCH-BCH-Message message paylor 00 04 50 cd 91 ff c0 c8 08 0e c6 30 40	ad.subsequentSegment.s 04 21 82 04 00 22 19	Input size : (222) Cancel	010010000100001110 1111101111011000101	

Message Coder: RRC SystemInformationBlockType5 subsequentSegment 🖤 New Data1 _ _ X Jun2006_Rel6_C Make Default Encode Decode RRC BCCH-BCH-Message Hex OC O Bin Spacer Offset=24. Length=222 RRC NAS Config RLC/I 🝿 New Data2 Field Make Default Encode Decode RRC 💉 😑 BCCH-BCH-Message Jun2006_Rel6_C 😑 message Hex OC OBin Spacer sfn-Prime payload RRC NAS Config RLC/MAC SMS SS CBS subsequentSe Field Value payload Туре sib-Type segmentl sib-Data-f BCCH-BCH-Message.mes 00 04 50 cd 91 ff c0 c c6 30 40 /inritsu Discover What's Possible™ Slide 34 MD8480C-E-E-5

Trace: D_BCCH (SYSTEM INFORMATION-BCH) SystemInformationBlockType5 lastSegmentShort

PHY MAC BLC TE BBC NAS	BTS	Primitive	Chappe	al.	Message	Beal Time	1
THE MAC THE THE THE MAS	013				message	010 04 00 50	-
		CPHY_RL_SETUP_UNF	D PICH	U		018:04:06.53	-
<		CREC_CONFIG_REQ	D PULH	U		018:04:06.54	
		CHLC_CONFIG_CNF	D PUCH	U		018:04:06.54	
<		HLC_TH_DATA_REQ	D BUCH	U	SYSTEM INFURMATION-BUH	018:04:06.61	
<		MAL_DATA_HEU	D BUCH	U		018:04:06.61	
K	1.1	HLC_TH_DATA_REQ	D BUCH	U	SYSTEM INFURMATION-BUH	018:04:06.62	
←		MAC_DATA_REU	D BCCH	U		018:04:06.62	
<		RLC_TH_DATA_REQ	D BCCH	U	SYSTEM INFURMATION-BCH	018:04:06.63	
<u>←</u>	1	PHY_DATA_HEU	D BCH	U		018:04:06.63	
←	1	MAC_DATA_REQ	D BCCH	0		018:04:06.63	
,	1	RLC_TR_DATA_REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.64	
K-1	1	MAC_DATA_REQ	D BCCH	0		018:04:06.64	
	1	RLC_TR_DATA_REQ	D BCCH	0	SYSTEM INFORMATION-BCH	018:04:06.65	
<	1	PHY_DATA_REQ	D BCH	0		018:04:06.65	
K−−	1	MAC_DATA_REQ	D BCCH	0		018:04:06.65	-
Message Data (Length=31)							
ender:050 Receiver:050 00 01 02 03 04 0 0000 00 04 50 cd 91 f	1ype 5 06 1 1 c0 1	:00500033 Channel:020 07 08 09 0A 0B 0C 0D 0 c8 08 0e 04 21 82 04 0	JUUUZ CH_NO: DE OF 10 1 DO 22 19 C	0000 1 12 a 64	13 14 15 16 17 18 19 1A 1B 29 40 05 02 22 a5 50 40 03 Copy data only Copy all	0pt2:00000000 IC ID IE IF 26 30 40	< >
Select SYS Bight-click	STE and	M INFORM	ATION v data	BO	CH.		

Message Coder: RRC (BCCH-BCH-Message) SystemInformationBlockType5 lastSegmentShort



Message Cod	ler: RRC
SystemInform	nationBlockType5 lastSegmentShort
W New Data1	
Make Default Encode De	ecode RRC BCCH-BCH-Message Jun2006_Rel6_C
RRC NAS Confie RLC/f	Image: Wight of the sector
rieiu	Make Default Encode Decode RRC Image: Control of the state of the
iastSegmentS astSegmentS astDype	RRC NAS Config RLC/MAC SMS SS CBS Field Value Type
— segmentin — sib-Data-va	
BCCH-BCH-Message.mess 00 06 51 52 8b 6d 85 00 00 00 00	00000010101101000011101011111111111111
<u></u>	L000000000001001100010000110010000110010000
Discover What's Possible™ MD8480C-E-E-5	Slide 37

Make Default Encode Decode	SysInfoType5	Jun2006_Rel6_C_	
	⊙ Bin Spacer	Offset=0, Length=3	
C NAS Config RLC/MAC SMS SS	CBS		
ield	Value	Туре	
SysInfoType5	000	SEQUENCE	
sib6indicator	FALSE	BOOLEAN	
pich-PowerOffset	-5	INTEGER	
😑 modeSpecificInfo	fdd	CHOICE	
🛓 fdd		SEQUENCE	
i aich-PowerOffset	5	INTEGER	
 primaryCCPCH-Info 		CHOICE	
🚊 prach-SystemInformationList	1	SEQUENCE OF	
PRACH-SystemInformation	11101	SEQUENCE	
😑 prach-RACH-Info		SEQUENCE	
🚊 modeSpecificInfo	fdd	CHOICE	
vsInfoType5			
00001011011010001110111111111111111 00001010010	1010000111111111111110 100000000000001001	0101000100001000011110 111111101111011	



Checking and Modifying Byte Array Message in C-Scenario

Steps:

- Copy the byte array message from the C-Scenario
- Paste it into Message Coder
- Decode
- Check the Value, Offset, and Length message items
- Modify the message items
- Encode
- Copy the message data to the C-Scenario

Discover What's Possible™
MD8480C-E-E-5

Slide 40



20



Message Coder: RRC (DL-DCCH-Message) radioBearerSetup

Make Detault Encode Decode		Jun	RRC
	C O Bin Spacer	Offset=8, Length=24	DL-DCCH-Message
C NAS Config RLC/MAC SMS	SS CBS		C
ield	Value	Type	C
DL-DCCH-Message	0	SEQUENCE	Spacer
 integrityCheckInfo 		SEQUENCE	- pavoi
😑 message	radioBearerSetup	CHOICE	
🚊 radioBearerSetup	r3	CHOICE	
🚊 r3	0	SEQUENCE	 Paste the data.
adioBearerSetup-r3	001000000100101010101	111 SEQUENCE	
rrc-TransactionIdentif	er O	INTEGER 🔍	
0x38, 0x20, 0x4A, 0xAF 0x84, 0x9C, 0x93, 0x4F 0x20, 0x40, 0x98, 0x24 0x97, 0x4C, 0x26, 0x4A 0xE7, 0x1A, 0xE2, 0x0A 0x40, 0x81, 0x60, 0x0C 0x19, 0xEB, 0xD5, 0xCE 0x51, 0x36, 0xBA, 0xE5 0x17, 0x89, 0x00, 0x3A 0x68	<pre>, 0x04, 0x00, 0x01, 0x70, , 0x05, 0xE2, 0x71, 0x85, , 0x52, 0x49, 0x34, 0x42, , 0x3C, 0x0B, 0xC4, 0x09, , 0x11, 0x06, 0x08, 0x62, , 0x66, 0x42, 0x98, 0xE8, , 0x60, 0x14, 0x22, 0x8C , 0xA0, 0x00, 0x0A, 0x00, , 0x00, 0x01, 0x00, 0x48,</pre>	0x23, 0x30, 0xDE, 0x17, 0x55, 0x20, 0x00, 0x88, 0x28, 0x56, 0x44, 0x96, 0x1, 0x40, 0x10, 0x00, 0x00, 0x00,	
Discover What's Possible™ MD8480C-E-E-5		Slide 42	/inrits

New Data1			Press Encode .
Make Default Encode Decode RRC	DL-DCCH-Message	et=1, Length=5	
RRC NAS Config RLC/MAC SMS SS			
Field	Value	Type	
 DL-DCCH-Message integrityCheckInfo 	0	SEQUENCE SEQUENCE	
🖃 message	radioBearerSetup	CHOICE	
😑 radioBearerSetup	later-than-r3	CHOICE	
Inter-Than-r3 rrc TransactionIdentifier	0	SEQUENCE	
criticalExtensions	o criticalExtensions	CHOICE	
2 • • • • • • • • • • • • • • • • • • •		STICLE N	
- Incomessage message			
DX3A, DX41, DX10, DX95, DX5F, DX64, DXCF, DX4D, DX25, DXEC, DX71, DXB1,	Ux12, 0x34, 0x00, 0x05, 0x05 0x08. 0x51. 0x39. 0x61. 0x77	, 0xF6, 🗠	
Dx61, 0x77, 0x82, 0xFA, 0xB4, 0x00,	0x74, 0xB1, 0x01, 0x02, 0x60	, 0x91,	
0x49, 0x24, 0xD2, 0x89, 0x54, 0xB2,	0x5D, 0x30, 0x99, 0x28, 0xF0	, 0x2F,	
DX10, DX24, DXU2, DX23, DX9F, DX6B, DXA3, DX9A, DXA0, DX01, DX6D, DX00,	0x88, 0x28, 0x44, 0x18, 0x21 0x86, 0x42, 0x90, 0xE <u>0, 0x4</u> A	, 0x88, . 0x96,	
Dx29, 0xE5, 0xEA, 0xD5, 0xD4, 0x20,	0x26, 0x01, 0x4F, 0x12, 0xE0	, 0x02,	
0x84, 0x51, 0x82, 0x29, 0xAA, 0x26,	0xD7, 0x5D, 0x35, 0xE6, 0x1E	, 0x99,	
Dx82, 0x00, 0x00, 0x00, 0xBC, 0x60,	0x08, 0x61, 0x0B, 0xC4, 0x00	, 0xE0,	
IXIU, UXUZ, UXDU, UXUU, UXUU, UXDU		and the second se	

Message Coder: Check activationTime Offset and Length radioBearerSetup

	O Bin Snacer Offs	et=34, Length=8	• Offset = 34
RRC NAS Config BLC/MAC SMS SS	CBS		• Length = 8
Field	Value	Type	
DL-DCCH-Message	0	SEQUENCE	
IntegrityCheckInfo ■ message	activationTime		
 radioBearerSetup r3 radioBearerSetup-r3 rrc-TransactionIdentifier integrityProtectionModeInfo cipheringModeInfo 	INTEGER Value : (0 . 255) OK Ca		Overwritten by following codes. Int2MsbIE(CFN, buff, 8); ReplaceIE(SndData, buff, 34, 8);
DL-DCCH-Message.message.radioBearerSetu	p.r3.radioBearerSetup-r3.activatic	nTime	
<pre>Jx38, 0x20, 0x4A, 0xAF, 0x<mark>04, 0x0</mark>, 0 0x93, 0x4F, 0x05, 0xE2, 0x71, 0x85, 0 0x52, 0x49, 0x34, 0xA2, 0x55, 0x2C, 0 0xC4, 0x09, 0x00, 0x88, 0xE7, 0xDA 0x28, 0xE6, 0x40, 0x81, 0x60, 0</pre>	x01, 0x70, 0x23, 0x3C, 0xB xDE, 0x17, 0x20, 0x40, 0x9 x97, 0x4C, 0x26, 0x4A, 0x3 xE2, 0x0A, 0x11, 0x06, 0x0 x86, 0x42, 0x98, 0xE8, 0x4 x22, 0x86, 0x11, 0x4D, 0x5	4, 0x9C, 3, 0x24, C, 0x0B, 3, 0x62, A, 0x96, L, 0x36,	



Message Coder: Modify 2 radioBearerSetup 🐨 New Datai Modify the message DL-DCCH-Message Make Default Encode Decode RRC 🛃 Ju item. Hex OC OBin Spacer Offset=9, Length=1 RRC NAS Config RLC/MAC SMS SS CBS Example: Field Value Type 😑 DL-DCCH-Message SEQUENCE CHOICE type item 0 SEQUENCE - integrityCheckInfo radioBearerSetup CHOICE 😑 message 🚊 radioBearerSetup later-than-r3 CHOICE SEQUENCE 🚊 later-than-r3 rrc-TransactionIdentifier 0 INTEGER criticalExtensions r4 CHOICE SEQUENCE 🖨 r4 0 🛓 radioBearerSetup-r4 00000000000000000000000... SEQUENCE integrityProtection... criticalExtensions cipheringModeInfo activationTime CHOICE new-U-RNTI priticalExtensions * new-C-RNTI r4 new-DSCH-RNTI OK Cancel DL-DCCH-Message.message.radioBearerSetup. 0x3A, 0x<mark>0</mark>0, 0x00, 0x00, 0x00 /inritsu Discover What's Possible™ Slide 46 MD8480C-E-E-5





lessage Coder: adioBearerSetup	Final Encode an	nd Copy
Vew Data1		After all modifications:
Make Default Encode Decode RRC	UL-DUCH-Message Jun Bin Spacer Offset=1, Length=5	• Press Encode.
Field DL-DCCH-Message integrityCheckInfo message radioBeareSetup cratioBeareSetup cratioBeareSetup craticalExtensions DL-DCCH-Message.message Dx3A, 0x41, 0x10, 0x95, 0x5F, 0x64, 0x12 0xCF, 0x4D, 0x25, 0xEC, 0x71, 0xB1, 0x0E 0x61, 0x77, 0x82, 0xFA, 0x89, 0x54, 0x82, 0x57 0x10, 0x24, 0x02, 0x89, 0x54, 0x64, 0x80 0x10, 0x24, 0x02, 0x89, 0x54, 0x64, 0x68	Value Type 0 SEQUENCE aradioBearerSetup CHOICE later-than-r3 CHOICE o INTEGER o INTEGER criticalExtensions CHOICE cricalExtensions CHO	 Copy the entire message data.
0xA3, 0x9A, 0xA0, 0x01, 0x60, 0x00, 0x00 0x29, 0xE5, 0xBA, 0xD5, 0xD4, 0x20, 0x26 0x84, 0x51, 0x82, 0x29, 0xAA, 0x26, 0xD0 0x82, 0x00, 0x00, 0x00, 0xBC, 0x60, 0x00 0x10, 0x02, 0x60, 0x00, 0x00, 0xD0 Discover What's Possible™	5, 0x42, 0x90, 0xE0, 0x4A, 0x96, 5, 0x01, 0x4F, 0x12, 0xE0, 0x02, 7, 0x5D, 0x35, 0xE6, 0x1E, 0x99, 5, 0x61, 0x0B, 0xC4, 0x00, 0xE0,	

Visual Studio: Paste and Replace byte array radioBearerSetup

/* Ser {	osoduć / wujpacke_muosodućs d Message: Radio Bearer Setup #/
	HAR SndData[] = {
0.004, 0.24	, 0,10, 0,33, 0,37, 0,464, 0,12, 0,34, 0,400, 0,00, 0,63, 0,76, 0,457, 0,447, 0,23
1	CHAR buff[4]:
	CFN = ((BtsReadCFN(UNIT_BTS1, NO_TIMEOUT) + 150) % 256) & (short)(~
	Int2MsbIE(CFN, buff, 8); ReplaceIE(SndData, buff, 34, 8);
	Int2MsbIE(Nsapi, buff, 8); ReplaceIE(SndData, buff, 50, 8);
	RICMUI = 1; RICCNF = 1;
	SndMessageIntegrity(UNIT_BTS1, RLC_AM_DATA_REQ, D_DCCH, 1, SndData, 728);
	RicCNF = 0;
Paste and repla	ce.
	Anaika



	Appendix	
Discover What's Possible™ MD8480C-E-E-5	Slide 52	/inritsu



Real Time Save HY MAC RLC TE RRC NAS BTS Primitive Channel Message Real Time Save HY MAC RLC TE RRC NAS BTS Primitive Channel Message Real Time Image: Save HY MAC RLC TE RRC NAS BTS Primitive D S_SCH 0 01804:06.25 Image: Stup_CNF 0 01804:06.26 Image: Stup_CNF 0 01804:06.27 Image: Stup_CNF 0 01804:06.27 Image: Stup_CNF 0 01804:06.28 Image: Stup_CNF 0 01804:06.29 Image: Stup_CNF 0 01804:06.29 Image: Stup_CNF 0 01804:06.30 Image: Stup_CNF 0 01804:06.31 Image: Stup_CNF 0 01804:06.31 Image: Stup_CNF 0 0 01804:06.32 Image: Stup_CNF 0 0 01804:06.32 Image: Stup_CNF 0 <t< th=""><th>G:¥Mx848000¥Trace¥F</th><th>R99. lo LogCon</th><th>e stral(C)</th><th></th><th></th><th></th><th></th><th>×</th></t<>	G:¥Mx848000¥Trace¥F	R99. lo LogCon	e stral(C)					×
HY MAC RLC TE RRC NAS BTS Primitive Channel Message Real Time 1 CPHY_RL_SETUP_REQ D_S_SCH 0 018:04:06.25 • 1 CPHY_RL_SETUP_REQ D_P_SCH 0 018:04:06.26 • 1 CPHY_RL_SETUP_REQ D_P_SCH 0 018:04:06.26 • 1 CPHY_RL_SETUP_REQ D_P_SCH 0 018:04:06.27 • 1 CPHY_RL_SETUP_CNF D_S_SCH 0 018:04:06.28 • 1 CPHY_RL_SETUP_CNF D_P_CCPCH 0 018:04:06.29 • 1 CPHY_RL_SETUP_CNF D_P_CCPCH 0 018:04:06.32 • 1 CPHY_RL_SETUP_CNF D_P_CCPCH 0 018:04:06.32 • 1 CPHY_RL_SETUP_REQ D_P_CCPCH 0 018:04:06.32 • 1 CPHY_RL_SETUP_REQ D_P_CPCH 0 018:04:06.33 • 1 CPHY_RL_SETUP_REQ D_P_CPCH 0 018:04:06.35 • 1 </th <th>The Cr. Harring Harr</th> <th></th> <th>aren<u>e</u>z.</th> <th></th> <th></th> <th>Real</th> <th>Time Save</th> <th></th>	The Cr. Harring Harr		aren <u>e</u> z.			Real	Time Save	
	PHY MAC RLC TE RRC NAS	BTS	Primitive	Channel	1	Message	Real Time	T
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0B 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1B 1F 00 00 00 1e 00 00 00 00 00 00 00 00 00 00 02 01 00 00 00 00 00 00 00 ± f 7e 00 00 00 00 00 =	Message Data (Length=97) Sender: 060 Receiver: 030 00 01 02 03 04 02	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CPHY_RL_SETUP_REQ CPHY_RL_SETUP_CNF CPHY_RL_SETUP_CNF CPHY_RL_SETUP_CNF CPHY_RL_SETUP_CNF CPHY_RL_SETUP_CNF CMAC_CONFIG_REQ CMAC_CONFIG_CNF CPHY_RCH_CONFIG_CNF CPHY_RL_SETUP_REQ CPHY_RL_SETUP_REQ CPHY_RL_SETUP_CNF CPHY_RL_SETUP_CNF CPHY_RL_SETUP_CNF CMAC_CONFIG_REQ 10300024 Channel:00000 7 08 09 04 08 00 00 00	D S_SCH D P_CCPCH D P_CCPCH D S_SCH D P_CCPCH D P_CCPCH D P_CCPCH D P_CCPCH D P_CCPCH D P_CCPCH D P_CCPCH D S_CCPCH D S_CCPCH	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0p=0:00000000 0p=1:00000000 0 13 14 15 16 17 18 19 1A 1F 1C 00 06 00 00 07 #7 26 00 36 00	018:04:06:25 018:04:06:26 018:04:06:27 018:04:06:27 018:04:06:29 018:04:06:30 018:04:06:30 018:04:06:31 018:04:06:32 018:04:06:33 018:04:06:33 018:04:06:33 018:04:06:37 018:04:06:37 018:04:06:39 018:04:06:39 018:04:06:39 018:04:06:39 018:04:06:39	
CONTRACTOR CONTRA	• Select CDL	IV		DEO a	nc			
• Select COLV DI SETUD BEO and D S CCOCH	• Dight click	· · _	KL_SETUP_	NEW a	nu			

Message Coder: Config CPHY-RL-SETUP-DL-PAR



File(E) TraceFilter(T) Trac	eLogCo	ntrol(<u>C</u>)			Rea	il Time Save	
PHY MAC RLC TE RRC NAS	BTS	Primitive	Channel		Message	Real Time	1
	1	CMAC_CONFIG_CNF	D P_CCPCH	0		018:04:06.32	7.
	1	CPHY_TRCH_CONFIG_CNF	D P_CCPCH	0		018:04:06.32	
<	1	CPHY_RL_SETUP_REQ	D P_CPICH	0		018:04:06.33	1
<	1	CPHY_RL_SETUP_REQ	D S_CCPCH	0		018:04:06.35	
>	1	CPHY_RL_SETUP_CNF	D P_CPICH	0		018:04:06.36	
< <u> </u>	1	CPHY_TRCH_CONFIG_REQ	D S_CCPCH	0		018:04:06.37	
	1	CPHY_RL_SETUP_CNF	D S_CCPCH	0		018:04:06.38	
<	1	CMAC_CONFIG_REQ	D S_CCPCH	0		018:04:06.39	
	1	CMAC_CONFIG_CNF	D S_CCPCH	0		018:04:06.40	
	1	CPHY_TRCH_CONFIG_CNF	D S_CCPCH	0		018:04:06.40	
<u> </u>	1	CPHY_RL_SETUP_REQ	U PRACH	0		018:04:06.41	
<u> </u>	1	CPHY_TRCH_CONFIG_REQ	U PRACH	0		018:04:06.43	
<	1	CPHY_TRCH_CONFIG_REQ	U PRACH	0		018:04:06.44	
	1	CPHY_RL_SETUP_CNF	U PRACH	0		018:04:06.44	
	1	CMAC_CONFIG_REQ	U PRACH	0		018:04:06.46	
Message Data (Length=4672 ender:060 Receiver:030 00 01 02 03 04 0 000 (01 01 00 00 00 0 020 (01 01 00 00 00 040 (00 01 00 00 0	1 Type 5 06 0 00 0 00 0 00	CMAC_CONFIG_REQ :10300022 Channel:00000 07 08 09 0A 0B 0C 0D 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 01 10 00 00 00	U PRACH 0006 CH_No:0 0 07 10 11 0 00 01 00 0 00 01 02 0 00 00 00	0 000 12 00 00 00	0pt0:00000000 0pt1:000000000 13 14 15 16 17 18 19 1A 18 1 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00	018:04:06.46 018:04:06.46 0pt2:FFFFFFFF C 1D 1E 1F C 00 00 00 Copy data only C 00 data only	

Message Coder: Config CPHY-TRCH-SETU	P-DL-PAR	
👿 New Data1		
Make Default Encode Decode Config V CPHY-TRCH-CONFIG	-DL-PAR Jun2006 Rel6 C	Setup:
	Offcat-32 Length-8	Config
M O Hex OC O Bin Spacer		Conng
RRC NAS Config RLC/MAC SMS SS CBS	70082 31	CPHY-TRCH-
Field Value	Type	
CPHY-TRCH-CONFIG-DL-PAR	SEQUENCE	SETUP-DE-PAR
- DTXPosition DTX-FLEXIBLE-POSITION	SizedENUMERATED	Нех
InterLv2nd INTERLEAVE-ON	SizedENUMERATED	
PuncLimit 0	INTEGER	Spacer
-NumOfTrch 3	INTEGER	
E TFCS	SEQUENCE	
NumOfTFC 9	INTEGER	Paste the data
Reserve	SEQUENCE OF	• Faste the uata.
UCHAR D	INTEGER	
	INTEGER	
U UCHAR U	INTEGER	• Press Decode .
B-TFC-0	SEQUENCE OF	
	INTEGER	
	INTEGER	
	INTEGER	
CPHY-TRCH-CONFIG-DL-PAR TECS NumOffEC	× ×	
01 01 00 03 09 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 01 00 00	
С		1
Discover What's Possible™		/incitsu
MD8480C-E-E-5 Slide	e 57	/ //////.50



Message Coder: Config CMAC-CONFIG-DL-PAR 👿 New Data1 CMAC-CONFIG-PAR. • Setup: Make Default Encode Decode Config Jun2006_Rel6_C Offset=32, Length=8 Hex OC OBin Spacer Config RRC NAS Config RLC/MAC SMS SS CBS **CMAC-CONFIG-DL-**Field Value Type PAR CMAC-CONFIG-PAR MAC-ACTIVE ActFlag Hex SaveTime 0 NumOfTrch INTEGER 3 Spacer OCTET STRING Reserve2 00 TFCS SEQUENCE NumOfTFC Paste the data. SEQUENCE OF - Reserve UCHAR 0 INTEGER UCHAR INTEGER 0 UCHAR 0 INTEGER • Press **Decode**. TFC-0 SEQUENCE OF UCHAR 0 INTEGER UCHAR Π INTEGER UCHAR INTEGER 0 UCHAR INTEGER 0 CMAC-CONFIG-PAR.TFCS.NumOfTFC < > /inritsu Discover What's Possible™ Slide 59 MD8480C-E-E-5

Definitions Setup

Message Coder requires matching versions for target message and Definitions Setup.

Correct:

Rel. 5 HSDPA radioBearerSetup message with Rel. 6 Definitions Setup.

Incorrect:

Rel. 5 HSDPA radioBearerSetup message with Rel. 99 Definitions Setup.

Correct:

Rel. 99 radioBearerSetup message with Rel. 99 Definitions Setup.

Discover What's Possible™ MD8480C-E-E-5

Slide 60



30

		1 1(0)					
-ne(r) traceFinter(1) tra	raceLogCo	ntrol\ <u>C</u> /			Real	Time Churc	
PHY MAC RLC TE RRC NA	AS BTS	Primitive	Channel		Message	Real Time	T
Message Data [Length=119 ender: 060 Receiver: 050 00 01 02 03 04 000 b0 c6 d4 c8 85 00 01 02 03 04 000 b0 c6 d4 c8 85 000 d3 56 61 e9 98	9) 9) 50 Type 05 06 0 04 11 0 10 26 0 00 88 0 20 00 0	PHY_DATA_IND MAC_DATA_IND RLC_AM_DATA_IND RAC_DATA_REQ PHY_DATA_REQ RAC_DATA_REQ MAC_DATA_REQ MAC_DATA_RE	U DCH U DCH U DCCH D D DCH D D DCH D D DCH D D DCH D D D D D D D D D D D D D D D D D D D	0 2 2 2 0 1 1 1 1 1 1 1 1 1 1 2 2 2 6	SM: ACTIVATE PDP CONTEXT REQ RADIO BEARER SETUP 0pt0:000000000 0pt1:00008001 0p 13 14 15 16 17 18 19 1A 1B 1C 5e c7 1b 10 b5 13 96 17 79 06 02 f1 02 40 22 99 f5 18 22 98 00 00 00 00	019.40.03.11 019.40.03.11 019.40.03.11 019.40.03.11 019.40.03.12 019.40.03.15	

Message Coder: Rel. 5 HSDPA radioBearerSetup message with Rel. 6 Definitions Setup 1

	Definitions Setup		Jun2006_Rel6_C_
RRC NAS Config RLC/MAC SMS Field DL-DCCH-Message integrityCheckInfo messageAuthenticationCode rrc-MessageSequenceNumbe message radioBearerSetup criticalExtensions criticalExtens	Reference Standard Version: Selected Version: Jun2006_Rel6_C_V560 Image: C_V560 Version Name Ma/2002_A8_V560 De=2002_A8_V560 Jun2001_A8_V560 De=2002_A8_V560 Jun2001_C_V560 De=2002_C_V560 De=2002_C_V560 De=2002_C_V560 De=2005_Rel5_A8_V560 De=2005_Rel5_C_V560 Jun2006_Rel6_C_V560 Jun2006_Rel6_C_V560	QK Cancel	V560.
Discover What's Possible™	Slide 62	,	/inritsu

Message Coder: Rel. 5 HSDPA radioBearerSetup message with Rel. 6 Definitions Setup 2



Message Coder: Rel. 5 HSDPA radioBearerSetup message with Rel. 99 Definitions Setup 1

iatioBearerSetup ☐ laterthan-r3 — rrc-TransactionIdentifier — criticalExtensions	Mar2002_AB_V560 Dec2002_AB_V560 W02_AB_V560 Mar2002_C_V560 Bec2002_0_V560 W02_C_V560 Dec2002_0_V560 Dec2005_Rel5_AB_V560 Dec2005_Rel5_AB_V560	Add Setup Delete	
DL-DCCH-Message message radioBeare 8a 39 aa 08 16 00 88 64 29 8e 84 9a a2 6d 75 d3 5e 61 e9 98 20 00 00 0b c6 00			

Message Coder: Rel. 5 HSDPA radioBearerSetup message with Rel. 99 Definitions Setup 2

Make Default Encode Decode RRC	DL-DCCH-Message	Dec2002_C_V560	
Hex OC OBin	Spacer	Offset=42, Length=1	Reis-HSDPA
RC NAS Config RLC/MAC SMS SS CBS			radioBearerSetup
Field	Value	Туре	message
 DL-DCCH-Message integrityCheckInfo messageAuthenticationCode 	1 0110000110001101101000	SEQUENCE SEQUENCE BIT STRING	message.
rrc-MessageSequenceNumber	1	INTEGER	It is incorrect
🖨 message	radioBearerSetup	CHOICE	
🖨 radioBearerSetup	later-than-r3	CHOICE	
🚊 later-than-r3		SEQUENCE	
rrc-TransactionIdentifier	0	INTEGER	
DL-DCCH-Message.message.radioBearerSetup			
	ad 5d 42 02 60 14 fl 2e 0) 28 45 18 22 🔥	
3a 39 aa 08 16 00 88 64 29 8e 84 a9 62 9e 5e			
3a 39 aa 08 16 00 88 64 29 8e 84 a9 62 9e 5e 9a a2 6d 75 13 5e 61 e9 98 20 00 00 0b c6 00 86 10 bc 40	0e 01 00 26 00 00 04 00		
3a 39 aa 08 16 00 88 64 29 8e 84 a9 62 9e 5e 9a a2 6d 75 13 5e 61 e9 98 20 00 00 0b c6 00 86 10 bc 40	0e 01 00 26 00 00 0d 00		
3a 39 aa 08 16 00 88 64 29 8e 84 a9 62 9e 5e 9a a2 6d 75 13 5e 61 e9 98 20 00 00 0b c6 00 86 10 bc 40 Discover What's Possible™	Oe Ol OO 26 OO OO Od OO		

Trace: Rel. 99 radioBearerSetup message 🚟 C:¥Mx848000¥Trace¥R99.log File(F) TraceFilter(T) TraceLogControl(C) Real Time PHY MAC RLC TE RRC NAS BTS Real Time Primitive Channel Message PHY_DATA_IND U DCH 018:04:52.75 MAC_DATA_IND RLC AM DATA IND U DCCH 2 2 018:04:52.75 1 SM: ACTIVATE PDP CONTEXT REQ 1 U DCCH 018:04:52 75 D DCCH MAC_DATA_REQ 2 018:04:52.75 1 PHY DATA BEQ. 018:04:52.76 RLC_AM_DATA_REQ MAC_DATA_REQ D DCCH RADIO BEARER SETUP 018:04:52.80 1 1 018:04:52.80 MAC_DATA_REQ D DCCH 018:04:52.80 MAC_DATA_REQ MAC_DATA_REQ D DCCH 018:04:52.80 D DCCH 018:04:52.80 MAC_DATA_REQ MAC_DATA_REQ D DCCH D DCCH 018:04:52.80 018:04:52.80 MAC DATA REQ D DCCH 018:04:52.80 018:04:52.81 PHY DATA REQ D DCH 0 Message Data (Length=101) ender:060 Receiver:050 Type:00500031 Channel:02000005 CH_No:0001 Opt0:00000000 Opt1:00008001 Opt2:00000000 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0B 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1B 1F 0000 | f5 98 50 50 0b 82 44 aa 70 30 a0 02 e0 76 69 a6 | d2 72 4d 3c 16 89 c6 17 78 5c 81 02 60 91 49 24 91 49 24 0a 63 al 24 00 Copy all Select RADIO BEARER SETUP. • Right click and select Copy data only. /inritsu Discover What's Possible™ Slide 66 MD8480C-E-E-5

Message Coder: Rel. 99 radioBearerSetup message with Rel. 99 Definitions Setup

Hex OC O Bin	Spacer [Offset=42, Length=1	Rel99
RC NAS Config RLC/MAC SMS SS CBS			TaulobearerSetu
Field	Value	Туре	message.
DL-DCCH-Message	1	SEQUENCE	, C
😑 integrityCheckInfo		SEQUENCE 🚽	
messageAuthenticationCode	1110101100110000101000	BIT STRING	It is correct
Inc-MessageSequenceNumber	1	INTEGER	
🖻 message	radioBearerSetup	CHOICE	
🖨 radioRearerSetup	r3	CHOICE	
i⊒- r3	0	SEQUENCE	
a radioBearerSetup-r3	0010010001001010101001	SEQUENCE	
- rrc-TransactionIdentifier	0	INTEGER	
- integrityProtectionModeInfo		SEQUENCE	
cipheringModeinto	10	SEQUENCE	
activation i ime	12	INTEGER	
new-O-RNTI		SEQUENCE	
- new-C-RN11			
L-DCCH-Message.message.radioBearerSetup			
a 58 65 c0 0a 11 46 08 a6 a8 9b 5d 73 d7 ab	4d 07 14 00 00 00 2f 12 0	0 75 00 00 80 🛛 🔼	
4 00 00 34			
c cc cc cc cO		~	

<u>/inritsu</u>

Anritsu Corporation

5-1-1 Onna, Atsugi-shi, Kanagawa, 243-8555 Japan Phone: +81-46-223-1111 Fax: +81-46-296-1264

• U.S.A.

Anritsu Company 1155 East Collins Blvd., Suite 100, Richardson, TX 75081, U.S.A. Toll Free: 1-800-267-4878 Phone: +1-972-644-1777 Fax: +1-972-671-1877

• Canada Anritsu Electronics Ltd. 700 Silver Seven Road, Suite 120, Kanata, Ontario K2V 1C3, Canada Phone: +1-613-591-2003 Fax: +1-613-591-1006

• Brazil Anritsu Eletrônica Ltda. Praca Amadeu Amaral, 27 - 1 Andar 01327-010-Paraiso-São Paulo-Brazil Phone: +55-11-3288-6940 Fax: +55-11-3288-6940

• Mexico Anritsu Company, S.A. de C.V. Av. Ejército Nacional No. 579 Piso 9, Col. Granada 11520 México, D.F., México Phone: +52-55-1101-2370 Fax: +52-55-5254-3147

• U.K.

Anritsu EMEA Ltd. 200 Capability Green, Luton, Bedfordshire, LU1 3LU, U.K. Phone: +44-1582-433200 Fax: +44-1582-731303

France

Anritsu S.A. 16/18 avenue du Québec-SILIC 720 91961 COURTABOEUF CEDEX, France Phone: +33-1-60-92-15-50

Fax: +33-1-64-46-10-65

 Germany Anritsu GmbH

Nemetschek Haus, Konrad-Zuse-Platz 1 81829 München, Germany Phone: +49-89-442308-0 Fax: +49-89-442308-55 • Italy

Anritsu S.p.A. Via Elio Vittorini 129, 00144 Roma, Italy Phone: +39-6-509-9711 Fax: +39-6-502-2425

Sweden

Anritsu AB Borgafjordsgatan 13, 164 40 KISTA, Sweden Phone: +46-8-534-707-00 Fax: +46-8-534-707-30

Finland Anritsu AB

Teknobulevardi 3-5, FI-01530 VANTAA, Finland Phone: +358-20-741-8100 Fax: +358-20-741-8111

Denmark
 Anritsu A/S
 Kirkebjerg Allé 90, DK-2605 Brøndby, Denmark
 Phone: +45-72112200

Phone: +45-72112200 Fax: +45-72112210

Spain Anritsu EMEA Ltd. Oficina de Representación en España

Edificio Veganova Avda de la Vega, n° 1 (edf 8, pl 1, of 8) 28108 ALCOBENDAS - Madrid, Spain Phone: +34-914905761 Fax: +34-914905762

• United Arab Emirates Anritsu EMEA Ltd. Dubai Liaison Office

P O Box 500413 - Dubai Internet City Al Thuraya Building, Tower 1, Suit 701, 7th Floor Dubai, United Arab Emirates Phone: +971-4-3670352 Fax: +971-4-3688460

Singapore Anritsu Pte. Ltd.

60 Alexandra Terrace, #02-08, The Comtech (Lobby A) Singapore 118502 Phone: +65-6282-2400 Fax: +65-6282-2533

• India

Anritsu Pte. Ltd. India Branch Office

Unit No. S-3, Second Floor, Esteem Red Cross Bhavan, No. 26, Race Course Road, Bangalore 560 001, India Phone: +91-80-32944707 Fax: +91-80-22356648

• P.R. China (Hong Kong)

Anritsu Company Ltd. Units 4 & 5, 28th Floor, Greenfield Tower, Concordia Plaza, No. 1 Science Museum Road, Tsim Sha Tsui East, Kowloon, Hong Kong Phone: +852-2301-4980 Fax: +852-2301-3545

P.R. China (Beijing) Anritsu Company Ltd.

Beijing Representative Office Room 1515, Beijing Fortune Building, No. 5, Dong-San-Huan Bei Road, Chao-Yang District, Beijing 10004, P.R. China Phone: +86-10-6590-9230 Fax: +86-10-6590-9235

Korea

Anritsu Corporation, Ltd. 8F Hyunjuk Building, 832-41, Yeoksam Dong, Kangnam-ku, Seoul, 135-080, Korea Phone: +82-2-553-6603 Fax: +82-2-553-6604

Australia

Anritsu Pty. Ltd. Unit 21/270 Ferntree Gully Road, Notting Hill, Victoria 3168, Australia Phone: +61-3-9558-8177 Fax: +61-3-9558-8255

Taiwan

Anritsu Company Inc. 7F, No. 316, Sec. 1, Neihu Rd., Taipei 114, Taiwan Phone: +886-2-8751-1816 Fax: +886-2-8751-1817

Please Contact:	
	080123

Specifications are subject to change without notice.