

3GPP2 A.S0012-D v2.0

August 2009



**3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"**

Interoperability Specification (IOS) for cdma2000 Access Network Interfaces — Part 2 Transport

(3G-IOS v5.1.1)

© 2009, 3GPP2

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. Refer to www.3gpp2.org for more information.

1

2

(This page intentionally left blank.)

3

4

5

6

Table of Contents

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55

1.0	Introduction	1
1.1	Overview	1
1.1.1	Purpose	1
1.1.2	Scope	1
1.2	References	1
1.2.1	Normative References	1
1.2.2	Informative References.....	3
1.3	Terminology	3
1.3.1	Acronyms.....	3
1.3.2	Definitions	6
2.0	General Protocol Requirements	7
2.1	Physical Layer (Layer 1)	7
2.2	Link Layer (Layer 2)	8
2.3	Use of ATM.....	9
2.3.1	ATM Adaptation Layer	9
2.3.2	Use of ATM AAL5 for Transmission of IP Datagrams.....	9
2.4	IP Transport Considerations	9
2.4.1	IP Topologies.....	9
2.4.2	IP Network and Transport Specifications (Layers 3/4).....	10
2.4.2.1	Addressing.....	10
2.4.2.2	Routing	10
2.4.2.3	Flow Association	10
2.4.3	IP Performance Specifications.....	10
2.4.4	Transport Network IP Quality of Service (QoS) Framework	10
2.4.5	IP Security Framework Specifications.....	11
2.5	Use of TCP	11
2.5.1	Message Delimiting in TCP.....	11
2.5.2	TCP Connection Establishment.....	13
2.5.3	TCP Connection Release	13
2.6	Use of GRE.....	13
2.6.1	GRE Attributes	16
2.6.1.1	Short Data Indicator.....	16
2.6.1.2	Flow Control Indication.....	16
2.6.1.3	IP Flow Discriminator	17
2.6.1.4	Segmentation Indication	18
2.6.2	Relationship of GRE tunnel to Quality of Service.....	18
2.6.3	GRE Protocol Usage for VoIP SOs	19
2.7	Use of RTP	19
2.8	Use of SUA.....	19
2.9	Base Station Application Part.....	19
2.9.1	The BS Management Application Part	20
2.9.2	The Direct Transfer Application Part	20
2.10	Use of SCTP.....	20
3.0	Interface Specific Protocol Requirements	23
3.1	A1, A2, and A5 Interfaces	23
3.1.1	Signaling Connection Transport Protocol Options	23
3.1.2	User Traffic Connection Transport Protocol Options.....	24
3.1.3	Use of ANSI SS7 Transport (Layer 2).....	24
3.1.3.1	Field of Application	25
3.1.3.2	Message Transfer Part	25
3.1.3.2.1	General.....	25
3.1.3.2.2	Level 1 (Chapter 2 of [21]).....	25
3.1.3.2.3	Level 2 (Chapter 3 of [21]).....	26

1	3.1.3.2.4	Level 3 (Chapter 4 of [21])	26
2	3.1.3.2.5	Testing and Maintenance (Chapter 7 of [21])	29
3	3.1.3.2.6	Interface Functions	29
4	3.1.3.2.7	Overload Control (Message Throughput Congestion)	29
5	3.1.3.3	SCCP Transport Layer Specification (SCCP Functions)	29
6	3.1.3.3.1	Overview	29
7	3.1.3.3.2	Primitives (Chapter 1 of [22])	30
8	3.1.3.3.3	SCCP Messages (Chapter 2 of [22])	30
9	3.1.3.3.4	SCCP Formats and Codes (Chapter 3 of [22])	32
10	3.1.3.3.5	SCCP Procedures (Chapter 4 of [22])	32
11	3.1.3.4	Use of the SCCP	34
12	3.1.3.4.1	Connection Establishment	34
13	3.1.3.4.1.1	Establishment Procedure - Case 1	34
14	3.1.3.4.1.2	Establishment Procedure - Case 2	36
15	3.1.3.4.2	Connection Release	39
16	3.1.3.4.3	Abnormal SCCP Release	40
17	3.1.3.4.3.1	SCCP Release by BS: Loss of SCCP Connection Information	40
18	3.1.3.4.3.2	SCCP Release by MSC: Loss of SCCP Connection Information	41
19	3.1.3.4.4	SCCP Reference Generation Philosophy	41
20	3.1.3.4.5	SCCP Transfer of DTAP and BSMAP Messages	42
21	3.2	A1p and A2p Interfaces	46
22	3.2.1	Performance Specifications	46
23	3.2.2	A1p Transport Protocol	46
24	3.2.2.1	Physical Layer (L1) Specification for A1p	46
25	3.2.2.2	Layer 2 Specification for A1p	46
26	3.2.2.3	Use of IP for A1p	46
27	3.2.2.4	QoS Specifications for A1p	47
28	3.2.2.5	Security Specifications for A1p	47
29	3.2.2.6	Use of the SUA for A1p	47
30	3.2.2.6.1	SUA Connection Establishment	47
31	3.2.2.6.1.1	Establishment Procedure - Case 1	48
32	3.2.2.6.1.2	Establishment Procedure - Case 2	49
33	3.2.2.6.2	Connection Release	50
34	3.2.2.6.3	Abnormal SUA Release	51
35	3.2.2.6.3.1	SUA Release by BS: Loss of SUA Connection Information	51
36	3.2.2.6.3.2	SUA Release by MSCe: Loss of SUA Connection Information	52
37	3.2.2.6.4	SUA Transfer of DTAP and BSMAP Messages	52
38	3.2.2.7	Base Station Application Part on A1p	56
39	3.2.2.8	Use of SCTP	56
40	3.2.3	A2p User Traffic Transport Protocol	56
41	3.2.3.1	Physical Layer (L1) Specification for A2p	59
42	3.2.3.2	Layer 2 Specification for A2p	59
43	3.2.3.3	Use of IP for A2p	59
44	3.2.3.4	QoS Specifications for A2p	59
45	3.2.3.5	Security Specifications for A2p	60
46	3.3	A3 and A7 Interfaces	60
47	3.3.1	Performance Specifications	60
48	3.3.1.1	Performance Specification for IP Protocol Stacks	61
49	3.3.2	A3 User Traffic Transport Requirements	61
50	3.3.2.1	ATM-Based User Traffic Transport	62
51	3.3.2.1.1	Physical Layer (L1) Specification	62
52	3.3.2.1.2	Use of ATM	62
53	3.3.2.1.3	Use of AAL2	62
54	3.3.2.2	IP-Based User Traffic Transport	62
55	3.3.2.2.1	Physical Layer (L1) Specification	62
56	3.3.2.2.2	Layer 2 Specification	62

1	3.3.2.2.3	Use of IP	63
2	3.3.2.2.4	QoS Specifications.....	63
3	3.3.2.2.5	Security Specifications.....	63
4	3.3.3	A3/A7 Signaling Transport Requirements.....	63
5	3.3.3.1	ATM-Based Signaling Protocol Stack.....	64
6	3.3.3.1.1	Use of Physical Layer	64
7	3.3.3.1.2	Use of ATM.....	64
8	3.3.3.1.3	Use of AAL5.....	64
9	3.3.3.1.4	Use of IP	64
10	3.3.3.1.5	Use of TCP	65
11	3.3.3.2	IP-Based Signaling Protocol Stack.....	65
12	3.3.3.2.1	Use of Physical Layer	65
13	3.3.3.2.2	Layer 2 Specification	65
14	3.3.3.2.3	Use of IP	65
15	3.3.3.2.4	QoS Specifications.....	66
16	3.3.3.2.5	Security Specifications.....	66
17	3.3.3.2.6	Use of SCTP	66
18	3.4	A8 and A9 Interfaces.....	66
19	3.4.1	Use of TCP	67
20	3.4.2	Use of UDP.....	67
21	3.4.3	Use of GRE.....	68
22	3.5	A10 and A11 Interface	68
23	3.5.1	Use of UDP.....	69
24	3.5.2	Use of GRE.....	69
25			

List of Figures

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

Figure 2-1	Transport Network Reference Model	7
Figure 2.5.1-1	Delimiting Messages in an IOS Application TCP Byte Stream.....	12
Figure 2.6-1	GRE Encapsulated User Traffic.....	14
Figure 2.6-2	3GPP2 GRE Frame.....	14
Figure 2.6-3	Attribute Format	15
Figure 2.9-1	A1 or A1p Interface Signaling Protocol Reference Model.....	20
Figure 3.1.1-1	A1 Signaling Protocol Stack.....	24
Figure 3.1.2-1	A2 User Traffic Protocol Stacks	24
Figure 3.1.2-2	A5 User Traffic Protocol Stacks	24
Figure 3.1.3.4.1.1-1	SCCP Connection Establishment.....	35
Figure 3.1.3.4.1.1-2	SCCP Connection Establishment Refusal.....	35
Figure 3.1.3.4.1.2-1	SCCP Connection Establishment with a Handoff Request message in an SCCP Connection Request message.....	36
Figure 3.1.3.4.1.2-2	SCCP Connection Refusal During Handoff.....	37
Figure 3.1.3.4.1.2-3	SCCP Connection Establishment with a Handoff Request message in an SCCP DT1 message.....	37
Figure 3.1.3.4.1.2-4	SCCP Connection with Handoff Failure via DT1	38
Figure 3.1.3.4.1.2-5	SCCP Connection Refused reply to a null SCCP Connection Request	39
Figure 3.1.3.4.3.1-1	BS Initiated SCCP Release: BS Lost SCCP Connection Information	40
Figure 3.1.3.4.3.2-1	MSC Initiated SCCP Release: MSC Lost SCCP Connection Information	41
Figure 3.1.3.4.4-1	SLR/DLR Usage	42
Figure 3.2.2-1	A1p Signaling Protocol Stack.....	46
Figure 3.2.2.6.1.1-1	SUA Connection Establishment.....	48
Figure 3.2.2.6.1-2	SUA Connection Establishment Refusal	49
Figure 3.2.2.6.1.2-1	SUA Connection Establishment During Handoff	50
Figure 3.2.2.6.1.2-2	SUA Connection Refusal During Handoff.....	50
Figure 3.2.2.6.3.1-1	BS Initiated SUA Release: BS Lost SUA Connection Information	51
Figure 3.2.2.6.3.2-1	MSCe Initiated SUA Release: MSCe Lost SUA Connection Information	52
Figure 3.2.3-1	Protocol stack for EVRC and SMV	57
Figure 3.2.3-2	Protocol stack for PCM (G.711)	57
Figure 3.2.3-3	Protocol Stack for 13k	58
Figure 3.2.3-4	Protocol Stack for DTMF	58
Figure 3.2.3-5	Protocol Stack for EVRC-B.....	58
Figure 3.2.3-6	Protocol Stack for EVRC-WB.....	59
Figure 3.2.3-7	Protocol Stack for EVRC-NW.....	59
Figure 3.3.2-1	A3 User Traffic Protocol Stack.....	61
Figure 3.3.3-1	A3 and A7 Signaling Protocol Stack	64
Figure 3.4-1	A9 Signaling Protocol Stack.....	67
Figure 3.4-2	A8 User Traffic Protocol Stack.....	67
Figure 3.5-1	A11 Signaling Protocol Stack.....	69
Figure 3.5-2	A10 User Traffic Protocol Stack.....	69

List of Tables

1
2
3
4
5
6
7
8
9

Table 3.1.3.4.5-1	Use of the User Data Field in SCCP Frames	42
Table 3.1.3.4.5-2	Use of SCCP for BSMAP and DTAP Messages	43
Table 3.2.2.6.4-1	Use of the User Data Field in SUA Frames	53
Table 3.2.2.6.4-2	Use of SUA for BSMAP and DTAP Messages	53
Table 3.3.1-1	Delay Budget Requirements	60
Table 3.3.1.1-1	A3/A7 Mapping Between Traffic Classes and Service-Level QoS	61

1
2
3
4
5

(This page intentionally left blank.)

1.0 Introduction

1.1 Overview

This document contains the protocol definitions and transport requirements for the interfaces defined in this specification.

1.1.1 Purpose

The purpose of this document is to describe the transport protocols and protocol stacks used on the interfaces, which make up the logical network model, and to indicate any unique aspects of these protocols that are relevant to the Interoperability Specification (IOS).

1.1.2 Scope

This document contains generic and specific requirements for the IOS interfaces. The document contains the generic protocol descriptions that are used through all of the IOS interfaces. In addition, protocol stack and transport network requirements for each IOS interface are contained in this document. Details of the IOS application and signaling layer messages are contained in the respective interface documents [14], [15], [16], and [17].

1.2 References

References are either normative or informative. A normative reference is used to include another document as a mandatory part of a 3rd Generation Partnership Project 2 (3GPP2) specification. Documents that provide additional non-essential information are included in the informative references section.

1.2.1 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

- [1~7] Reserved.
- [8] 3GPP2 X.S0011-D v2.0, *Wireless IP Network Standard, six parts*, November 2008.
- [9] Reserved.
- [10] Reserved.
- [11] 3GPP2 A.S0011-D v2.0, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 1 Overview*, August 2009.
- [12] Reserved.
- [13] 3GPP2 A.S0013-D v2.0, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 3 Features*, August 2009.

- 1 [14] 3GPP2 A.S0014-D v2.0, *Interoperability Specification (IOS) for cdma2000*
2 *Access Network Interfaces – Part 4 (A1, A1p, A2, and A5 Interfaces)*, August
3 2009.
- 4 [15] 3GPP2 A.S0015-D v2.0, *Interoperability Specification (IOS) for cdma2000*
5 *Access Network Interfaces – Part 5 (A3 and A7 Interfaces)*, August 2009.
- 6 [16] 3GPP2 A.S0016-D v2.0, *Interoperability Specification (IOS) for cdma2000*
7 *Access Network Interfaces – Part 6 (A8 and A9 Interfaces)*, August 2009.
- 8 [17] 3GPP2 A.S0017-D v2.0, *Interoperability Specification (IOS) for cdma2000*
9 *Access Network Interfaces – Part 7 (A10 and A11 Interfaces)*, August 2009.
- 10 [18] 3GPP2 C.S0047-0, Version 1.0, *Link-Layer Assisted Service Options for Voice-*
11 *over-IP: Header Removal (SO60) and Robust Header Compression (SO61)*,
12 April 14, 2003.
- 13 [19] 3GPP2 N.S0019, *Intersystem Link Protocol*, January 28, 2000.
- 14 [20] T1.101, *Synchronization Interface Standard*, November 2006.
- 15 [21] T1.111, *Signaling System No. 7 (SS7) - Message Transfer Part (Includes*
16 *T1.111a-2002)*, July 2005.
- 17 [22] T1.112, *Signaling System No. 7 (SS7) - Signaling Connection Control Part*
18 *(SCCP) January 2005 and T1.112-A, Subsystem Number Assignment Guidelines*
19 *- Supplement to T1.112*, January 2006.
- 20 [23] T1.627, *Broadband-ISDN - ATM Layer Functionality and Specification*, July
21 1993, Revised 1999.
- 22 [24] T1.105, *Synchronous Optical Network (SONET) – Basic Description Including*
23 *Multiplex Structure, Rates and Formats (Includes T1.105a-2002)*, January 2008.
- 24 [25] ITU-T Recommendation G.707, *Network Node Interface for the Synchronous*
25 *Digital Hierarchy (SDH)*, 1996.
- 26 [26] ITU-T Recommendation Q.2931, *Broadband-Integrated Services Digital*
27 *Network (B-ISDN) Digital Subscriber Signaling No. 2 (DSS2) User-Network*
28 *Interface Layer 3 Specification for Basic Call/Connection Control*, 1995.
- 29 [27] IETF, *RFC 768 – User Datagram Protocol (UDP)*, 1980.
- 30 [28] IETF, *RFC 791 – Internet Protocol (IP)*, 1981.
- 31 [29] IETF, *RFC 793 – Transmission Control Protocol (TCP)*, 1981.
- 32 [30] IETF, *RFC 1483 – Multiprotocol Encapsulation over ATM Adaptation Layer 5*,
33 1993.
- 34 [31] IETF, *RFC 2002 – IP Mobility Support Specification*, 1996.
- 35 [32] IETF, *RFC 2225 – Classical IP and ARP over ATM*, 1998.
- 36 [33] IETF, *RFC 2475 – An Architecture for Differentiated Services*, December 1998.
- 37 [34] IETF, *RFC 2658 – RTP Payload Format for PureVoice™ Audio*, www.ietf.org,
38 August 1999.
- 39 [35] IETF, *RFC 2784 – Generic Routing Encapsulation (GRE)*, 2000.
- 40 [36] IETF, *RFC 2833 – RTP Payload for DTMF Digits, Telephony Tones and*
41 *Telephony Signals*, www.ietf.org, May 2000.
- 42 [37] IETF, *RFC 2890 – Key and Sequence Number Extensions to GRE*, September
43 2000.
- 44 [38] IETF, *RFC 2960 – Stream Control Transmission Protocol*, October 2000.
- 45 [39] IETF, *RFC 3550 – RTP: A Transport Protocol for Real Time Applications*, July
46 2003
- 47 [40] IETF, *RFC 3551 – RTP Profile for Audio and Video Conferences with Minimal*
48 *Control*, July 2003.
- 49 [41] IETF, *RFC 3558 – RTP Payload Format for Enhanced Variable Rate Codecs*
50 *(EVRC) and Selectable Mode Vocoders (SMV)*, www.ietf.org, July 2003.
- 51 [42] IETF, *RFC 3868 – Signaling Connection Control Part User Adaptation Layer*
52 *(SUA)*, October 2004.
- 53 [43] IEEE 802.3, *IEEE Standard for Information technology – Telecommunications*
54 *and information exchange between systems – Local and metropolitan area*
55 *networks – Specific requirements – Part 3: Carrier Sense Multiple Access with*

1 *Collision Detection (CSMA/CD) Access Method and Physical Layer*
 2 *Specifications, 2002.*

3 [44] IETF, *RFC 4788 – Enhancements to RTP Payload Formats for EVRC Family*
 4 *Codecs, www.ietf.org, January 2007.*

5 [45] IETF RFC 5188, *RTP Payload Format for the Enhanced Variable Rate*
 6 *Wideband Codec (EVRC-WB) and the Media Subtype Updates for EVRC-B*
 7 *Codec, February 2008.*

8 [46] *draft-zfang-avt-rtp-evrc-nw, July 2009.*

9
 10 Editor's Note: The above document is a work in progress and should not be
 11 referenced unless and until it is approved and published. Until such time as this
 12 Editor's Note is removed, the inclusion of the above document is for
 13 informational purposes only.
 14

15 **1.2.2 Informative References**

16 [I-1] 3GPP2 A.S0008-C v2.0, *Interoperability Specification (IOS) for High Rate*
 17 *Packet Data (HRPD) Radio Access Network Interfaces with Session Control in*
 18 *the Access Network, January 2009.*

19 [I-2] 3GPP2 A.S0009-C v2.0, *Interoperability Specification (IOS) for High Rate*
 20 *Packet Data (HRPD) Radio Access Network Interfaces with Session Control in*
 21 *the Packet Control Function, January 2009.*
 22

23 **1.3 Terminology**

25 **1.3.1 Acronyms**

Acronym	Meaning
3GPP2	3rd Generation Partnership Project 2
AAL2	ATM Adaptation Layer type 2
AAL5	ATM Adaptation Layer type 5
ADDS	Application Data Delivery Service
Ack	Acknowledgement
AL	Application Layer
ANSI	American National Standards Institute
ATM	Asynchronous Transfer Mode
BS	Base Station
BSAP	Base Station Application Part
BSC	Base Station Controller
BSMAP	Base Station Management Application Part
BTS	Base Transceiver System
CC	Connection Confirm
CDMA	Code Division Multiple Access

Acronym	Meaning
CIC	Circuit Identity Code
CLDT	Connectionless Data Transfer (SUA)
CM	Connection Management
COAK	Connection Acknowledge (SUA)
CODT	Connection Oriented Data Transfer (SUA)
CORE	Connection Request (SUA)
COREF	Connection Refused (SUA)
CR	Connection Request
CREF	Connection Refused
DCCH	Dedicated Control Channel
DiffServ	Differentiated Services
DLR	Destination Local Reference
DPC	Destination Point Code
DS0	Digital Signal Level 0
DSCP	Differentiated Services Code Point
DT1	Data Transfer 1
DT2	Data Form 2
DTAP	Direct Transfer Application Part
E1	E1-type Digital Carrier
EIA	Electronics Industry Association
ESN	Electronic Serial Number
FCH	Fundamental Channel
GRE	Generic Routing Encapsulation
HRPD	High Rate Packet Data
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IOS	Interoperability Specification
IP	Internet Protocol
IS	Interim Standard
ISD	Interface Service Delay
ISL	Interface Service Packet Loss
ISLP	Intersystem Link Protocol
IT	Inactivity Test
ITU-T	International Telecommunications Union – Telecommunications Standardization Sector
kbps	Kilobits per second
L1	Layer 1 (Physical Layer)
L2	Layer 2 (Link Layer)
L3	Layer 3 (Network Layer)
LLC	Logical Link Control

Acronym	Meaning
LMSD	Legacy MS Domain
LSB	Least Significant Bit
Mbps	Million Bits per Second
MGW	Media Gateway
MS	Mobile Station
MSB	Most Significant Bit
MSC	Mobile Switching Center
MSCe	Mobile Switching Center Emulation
Msg	Message
MTP	Message Transfer Part
OAM&P	Operation Administration Maintenance and Provisioning
OC3	Optical Carrier Level 3
PACA	Priority Access and Channel Assignment
PCF	Packet Control Function
PCM	Pulse Code Modulation
PDSN	Packet Data Serving Node
PLMN	Public Land Mobile Network
PPP	Point to Point Protocol
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RAN	Radio Access Network
RELCO	Release Complete (SUA)
RELRE	Release Request (SUA)
RFC	Request For Comment
RLC	Release Complete (SCCP)
RLSD	Release (SCCP)
RTP	Real-time Transport Protocol
SCCP	Signaling Connection Control Part
SCH	Supplemental Channel
SCTP	Stream Control Transmission Protocol
SDU	Service Data Unit (ATM), Selector/Distribution Unit (IOS)
SI	Service Instance
SID	Session Identifier
SLR	Source Local Reference
SLTM	Signaling Link Test Message
SOG	Subsystem Out-of-service Grant
SOR	Subsystem Out-of-service
SS7	Signaling System Number 7
SSN	Subsystem Number
STP	Signaling Transfer Point

Acronym	Meaning
SUA	Signaling Connection Control Part User Adaptation Layer
T1	T1-type Digital Carrier
T3	T3-type Digital Carrier
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
TL	Transport Layer
UDI	Unrestricted Digital Information
UDP	User Datagram Protocol
UDT	Unit Data (SCCP)
UNI	User Network Interface
VC	Virtual Circuit
Ver	Version
VoIP	Voice over Internet Protocol

1

2 **1.3.2 Definitions**

3 Refer to [11] for definitions.

2.0 General Protocol Requirements

The Transport specification uses protocols and terminology for the interface in the IOS, that conform to the transport network reference model as outlined in Figure 2-1. Layer 1 is the physical layer. Layer 2 is the link layer. Layer 3 is the network layer, which may consist of several hops connected by routing or switching nodes. Figure 2-1 shows two hops but a network can have none or many hops. The transport layer is above L3 and is an end-to-end protocol. The transport layer (TL) is terminated at end nodes within the Radio Access Network (RAN). From a RAN perspective, the application layer (AL) consists of IOS signaling messages and bearer frames on the IOS interface. Note the transport network reference model may not be applicable to describe the protocol stack for user traffic.

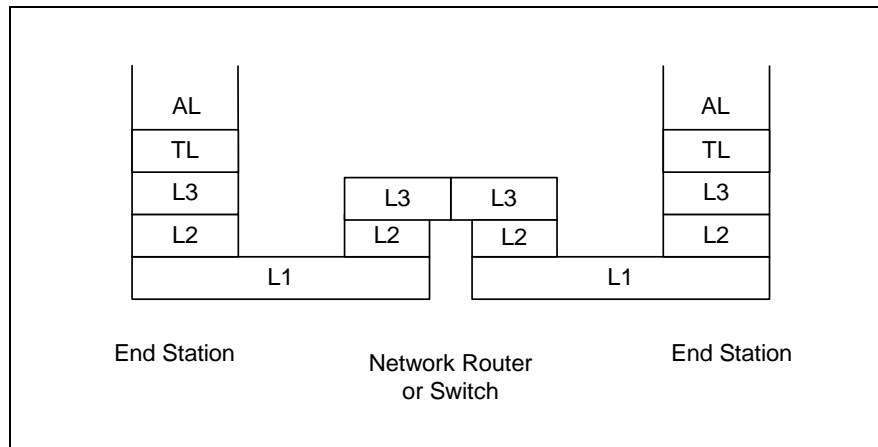


Figure 2-1 Transport Network Reference Model

The nodes comprising the RAN (e.g. Base Station (BS), Packet Control Function (PCF), Packet Data Service Node (PDSN) and Mobile Switching Centers (MSCs)) are often geographically distributed across and between areas of the transport network.

2.1 Physical Layer (Layer 1)

The IOS interfaces are based on the use of:

- T1 digital transmission system interfaces. Each 1.544 Mbps interface provides 24*56 kbps or 24*64 kbps channels or a 1.544 Mbps clear channel, which can be used for traffic or signaling as the operator requires. These types of interfaces can be full-duplex or half-duplex when they are used as a clear channel.
- E1 digital transmission interfaces consisting of 30*64 kbps user channels or a 2.048 Mbps clear channel can also be used for traffic or signaling, as the operator requires, and as applicable to the network.
- T3 digital transmission interfaces supporting transmission rates of 43.232 Mbps.
- Optical Carrier Level 3 (OC3) digital transmission interfaces supporting transmission rates of 155.52 Mbps.
- Optical Carrier Level 12 (OC12) [24] and Synchronous Transfer Mode 4 (STM4) [25] digital transmission interfaces supporting transmission rates of 622.08 Mbps.
- Synchronous Transfer Mode 1 (STM1) [25] digital transmission interfaces supporting transmission rates of 155.52 Mbps.

- Asynchronous layer 1 protocols (e.g. 10/100BaseT, Gigabit Ethernet [43]) may be used on some IOS interfaces. These types of L1 protocols can be full or half-duplex, shared or dedicated. These types of L1 protocols may provide guaranteed bandwidth to the L2 protocol.

When the L1 protocol cannot guarantee the bandwidth to the L2 protocol, a mechanism should be provided by the L2 protocol that enables compliance to the performance specifications in this document if required.

Common physical interface standards are found in [20] and related references. For a list of references, refer to section 1.2.

2.2 Link Layer (Layer 2)

This standard uses different link layers on different interfaces. Message Transfer Part 2 and Asynchronous Transfer Mode (ATM) are used as the link layer (L2) protocol on some interfaces. For Internet Protocol (IP)-based protocol stacks in this specification, Layer 2 is left unspecified. In these cases requirements on L2 are invoked on an interface-by-interface basis as stated in the interface specific section of this document.

The following requirements may apply to an unspecified L2 implementation or protocol for IP:

- Bandwidth efficiency:** The L2 protocol provides functions to improve the bandwidth efficiency of transport network layer protocols when the physical layer (L1) consists of narrow-band (i.e., T1/E1 or lower rate) circuits. Bandwidth efficiency is defined here as the ratio of the total number of bits comprising a “packet” to the number of information (or payload) bits contained within that packet.
- Delay/jitter control:** The L2 protocol provides functions to manage queuing delay and inter-packet transmission time variation (jitter) for all packet sources (e.g., queuing, scheduling, prioritization). Queuing delay is defined here as the amount of time that a network layer (layer 3) packet waits at link layer (layer 2) for transmission on the physical interface (e.g. source bit-rate exceeds the transmission bit-rate of the destination connection associated with that packet).
- Multiplexing:** This function collects and concatenates eligible buffered frames/packet into one larger frame/packet reducing the impact of the protocol overhead for each frame. If the IP transport network employs this type of function, it shall be implemented in the link layer (L2) protocol. The implementation shall also permit enabling and disabling this feature on an L2 connection basis.
- Compression:** This function eliminates the need for transmission of certain header information (e.g., User Datagram Protocol (UDP) header, IP header, Point to Point Protocol (PPP) ID) for every packet in a given flow by making use of well-known or pre-negotiated connection state information. If the IP transport network employs this type of function, it shall be implemented in the link layer (L2) protocol. The implementation shall also permit enabling and disabling this feature on an L2 connection basis.
- Segmentation and re-assembly (SAR):** This function segments a packet (from the transport network or higher layers) into multiple packets/frames to control latency. If the IP transport network employs this type of function, it shall be implemented in the link layer (L2) or IP layer (L3) protocol. If implemented in L2, the implementation shall permit enabling and disabling this feature and controlling the respective frame size on an L2 connection basis as required by performance specifications of the connection.

- Error detection: The L2 protocol provides an error detection function for the L2 protocol fields. The L2 protocol may provide error detection for layer 2 payload data. The implementation shall permit enabling and disabling of this feature, if required by the L2 protocol, on a per L2 connection basis.
- Addressing: L2 addressing (e.g. MAC, VCI/VPI) supports a means of translating an IP address (unicast, multicast or broadcast) to an associated L2 address.

2.3 Use of ATM

The ATM Layer uses a basic 53 octet cell consisting of a 5 octet header and 48 octet payload. This standard uses the ATM Layer as specified in [23] without modification.

2.3.1 ATM Adaptation Layer

To make use of the basic cell transfer capability of the ATM Transport Layer in specific usages, various ATM Adaptation Layers (AALs) have been defined.

Within this standard, two AALs are used:

- AAL5 — for the transfer of signaling, and
- AAL2 — for the transfer of user traffic (voice/data) on A3 traffic subchannels.

Both ATM Adaptation Layer Type 5 (AAL5) and ATM Adaptation Layer Type 2 (AAL2) are used without modification in this standard. The Service Specific Segmentation and Reassembly sublayer for AAL2, as specified in [25], is used for segmentation and reassembly of AAL2 SDUs.

In this version of this standard, the functionality of other sublayers of AAL2 are not supported. Specifically, Service Specific Transmission Error Detection and Service Specific Assured Data Transfer are not included.

2.3.2 Use of ATM AAL5 for Transmission of IP Datagrams

Use of the AAL5 Permanent Virtual Circuit (PVC) and Switched Virtual Connection as the link layer of IP protocol stack shall follow [32]. Specification of either Logical Link Control (LLC) and Sub Network Attachment Point encapsulation or Virtual Channel (VC) multiplexing as per [30] is left to the discretion of operators and manufacturers.

2.4 IP Transport Considerations

The standard IP protocol, as defined in [28], shall be used for routing Internet Protocol packets.

2.4.1 IP Topologies

Within the IOS RAN, an IP transport network may be used to provide communication between the end nodes. This IP transport network itself may consist of transport nodes (routers, switches, etc) arranged into a number of different topologies (e.g. point-to-point, hierarchical, meshed, hub-spoke, star, etc). The transport network may also consist of one or more communication links that connect the end nodes to the transport network and the transport nodes to each other. The IP transport network may also consist of edge transport nodes that interface to other RANs or packet data networks providing security, address

1 translation and other functions specific to the type of network to which they are
 2 connected. There is no restriction on the number or types of topologies or devices that
 3 can be used to implement this RAN transport network.

4 **2.4.2 IP Network and Transport Specifications (Layers 3/4)**

5 This section provides a minimum set of requirements on transport and network layer
 6 (layer 3/4) interfaces to the BS, PCF, PDSN, MSCe, MGW or other network devices in
 7 the RAN.

8 **2.4.2.1 Addressing**

9 The IP transport network may support a class-less IP addressing scheme. This is
 10 necessary to allow flexibility in both routing and network design. To support this, a
 11 hierarchical addressing scheme shall be implemented with Variable Length Subnet
 12 Masks.

13 **2.4.2.2 Routing**

14 An implementation may choose one or more IP routing protocols as needed for non
 15 point-to-point network topologies.

16 **2.4.2.3 Flow Association**

17 Every logical element defined in an IOS interface that may be an information source or
 18 target may be individually addressable (e.g., via an IP address and UDP port number). In
 19 cases where logical sub-elements exist, the IP address and port number (such as for UDP,
 20 Transmission Control Protocol (TCP), or Stream Control Transmission Protocol (SCTP))
 21 may be used to uniquely identify a sub-element. Specific addressing requirements are set
 22 forth in the individual interface specifications.

23 A traffic flow (i.e., radio frame protocols, call control signaling, OAM&P, etc.) may be
 24 uniquely identified by the IP address of the destination element. In cases where logical
 25 sub-flows exist, the IP address and port number of the destination sub-element may be
 26 used to uniquely identify a flow. Mapping application flows to transport flows is
 27 specified by the individual IOS interfaces.

28 **2.4.3 IP Performance Specifications**

29 Each IOS interface may specify the performance it requires from the transport network.
 30 The following parameters may be specified by IOS interfaces that require performance
 31 specifications:

- 32 • Interface Service Delay (ISD): This is composed of the cumulative queuing,
 33 transmission, and propagation delays across the transport network between nodes
 34 supporting an IOS interface.
- 35 • Interface Service Packet Loss (ISL): This is the packet loss across the transport
 36 network between nodes supporting an IOS interface.

37 **2.4.4 Transport Network IP Quality of Service (QoS) Framework**

38 To ensure that the transport network provides the necessary performance characteristics,
 39 the end nodes and transport network interfaces which require transport QoS shall support

1 the Differentiated Services (DiffServ) framework as specified in [33], with the following
2 clarifications:

- 3 • The A1p/A2p, A3/A7, A8/A9 and A10/A11 network portions of the RAN transport
4 network may be over-provisioned in comparison to the air interface (BS to MS)
5 capacity, and the A1p/A2p, A3/A7, A8/A9 and A10/A11 network traffic loads, or
6 both. In case a RAN transport network is over-provisioned, the QoS framework in
7 this section is not applicable to that transport network.
- 8 • Transport nodes (e.g., interior routers) shall support the following:
 - 9 – Per packet classification according to the Type of Service (TOS)/Differentiated
10 Services Code Point (DSCP) field in the IPv4 header
 - 11 – One or more queuing disciplines to meet the interface's delay/jitter
12 requirements.
- 13 • Edge transport nodes (e.g., border routers) shall support the following:
 - 14 – Policing disciplines to meet the traffic flow requirements.
- 15 • End host nodes (e.g., BS, PCF, PDSN's) shall support the following when required:
 - 16 – Per packet marking of a DSCP via the IPv4 TOS octet according to the
17 prescribed DSCP value (refer to section 2.6.2).
 - 18 – Four or more traffic classes as defined by the relevant interface. The parameters
19 of each class include mandatory and optional traffic types, service delay, and
20 packet loss rate.

21 **2.4.5 IP Security Framework Specifications**

22 The IOS RAN may be realized as a managed network. In this case, it is assumed that all
23 interfaces are physically secured as a minimum and any additional security measures are
24 beyond the scope of this standard. For security measures specific to particular IOS
25 interfaces, refer to [13].

26 **2.5 Use of TCP**

27 The standard TCP protocol, as described in [29], shall be used for establishing, using, and
28 clearing TCP connections.

29 TCP connections for signaling may be set up on a per-call basis or signaling messages for
30 multiple calls may be multiplexed on a single TCP connection.

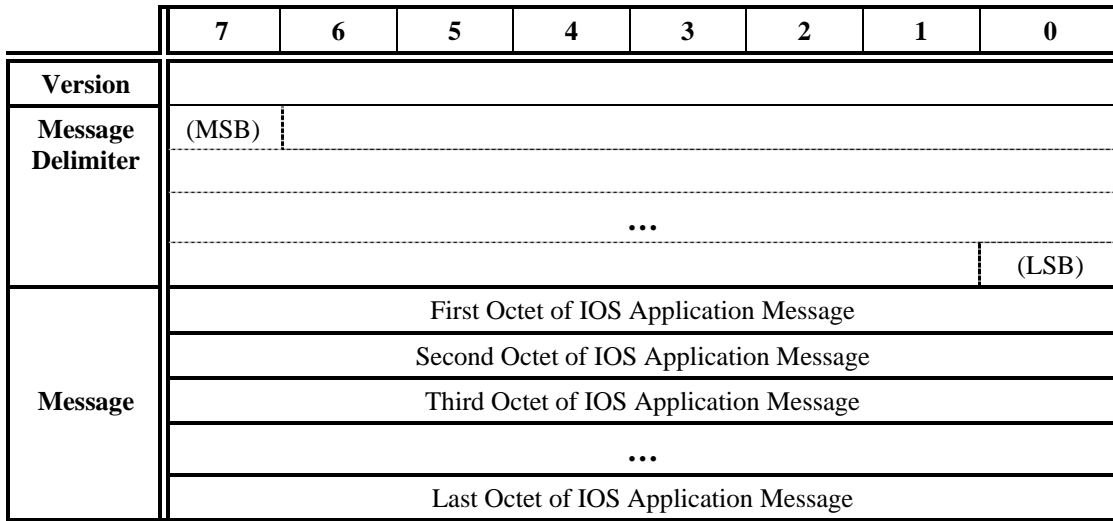
31 The TCP protocol provides a reliable byte stream transfer. Therefore, a means needs to be
32 provided for two application entities to delimit the messages sent between them. The
33 technique for such delimitation is as follows.

34 **2.5.1 Message Delimiting in TCP**

35 TCP provides reliable transfer of byte streams between two application entities. Because
36 the protocol in this standard uses IOS Application messages to communicate, these
37 messages shall be delimited in the TCP byte stream. Such delimitation shall be done by
38 means of a message delimitation header, comprising of a one byte field and a variable
39 length message delimiter whose format is specified by the version in use, inserted at the
40 beginning of each IOS Application message. Refer to Figure 2.5.1-1.

1 A TCP segment (i.e., a segment of the byte stream transferred in one TCP PDU) may
 2 contain all or portions of several IOS Application messages. IOS Application messages
 3 follow each other in the TCP byte stream. The beginning of each IOS Application
 4 message is preceded immediately by a message delimitation header as shown in the
 5 Figure 2.5.1-1.

6 When a TCP connection is opened, the first octet of the payload of the first TCP segment
 7 sent over that connection shall coincide with the Version field of a message delimitation
 8 header.

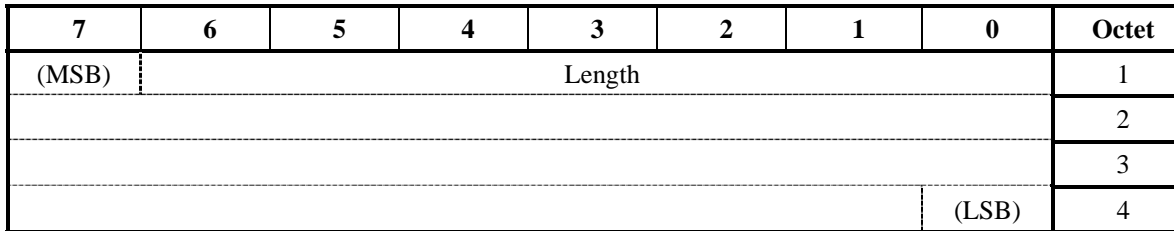


9 **Figure 2.5.1-1 Delimiting Messages in an IOS Application TCP Byte Stream**

10 Version This field contains the version number and specifies the
 11 remainder of the message delimiter format. This field is set to
 12 the range of values as follows:

Binary Values	Meaning
0000 0000	Reserved
0000 0001	Version 1
All other values	Reserved

13 Message Delimiter: The contents of this field are specified by the version of the
 14 message delimitation header. For version '0000 0001', the
 15 delimiter format is coded as follows:



16 Length: This field contains the number of octets in the IOS
 17 Application message following this field as a binary number.

2.5.2 TCP Connection Establishment

A new TCP connection is established when a signaling message is required to be exchanged over an interface and no such connection exists for that interface. Normal active-passive TCP connection establishment procedures are used.

2.5.3 TCP Connection Release

An existing TCP connection over an interface may be released when there are no more signaling messages to be exchanged over the interface. Normal TCP connection release procedures are used.

2.6 Use of GRE

The upper layer for the A8 and A10 interfaces is the Generic Routing Encapsulation (GRE) protocol as defined in [35] and extended in [37]. Refer to sections 3.4 and 3.5 for A8 and A10 protocol stack descriptions.

The A8 and A10 connections are used for the transport of user data for a packet data session. Link layer/network layer frames are carried between the BS, PCF and the PDSN encapsulated in GRE packets, which in turn are carried over IP. Each GRE packet is encapsulated in exactly one IP datagram. The BS Address, PCF Address and the PDSN Address are used in the source address and destination address fields of the IP header used with the GRE packet.

In the bearer traffic direction from the PDSN to the PCF, the key field in the GRE header contains the PCF Session Identifier (SID) that indicates to which A10 connection a particular payload packet belongs.

In the bearer traffic direction from the PCF to the PDSN, the key field in the GRE header contains the PDSN SID.

If the PDSN assigns a unique SID to each A10 connection, the PDSN SID can be used to identify to which A10 connection the packet belongs. Otherwise, the PDSN may use the combination of the PCF Address and the PDSN SID parameters of each received packet to identify the associated A10 connection.

In the bearer traffic direction from the PCF to the BS, the key field in the GRE header contains a unique BS identifier that indicates to which A8 connection a particular payload packet belongs.

In the bearer traffic direction from the BS to the PCF, the key field in the GRE header contains a unique PCF identifier that indicates to which A8 connection a particular payload packet belongs.

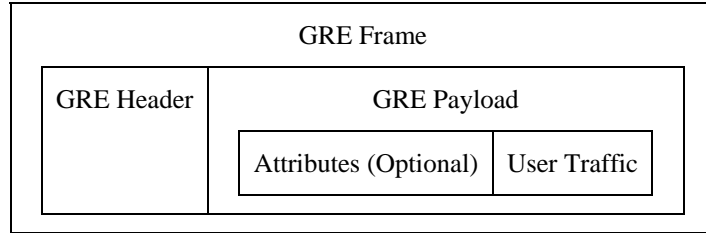
For A8 connections, when the Protocol Type field is set to '88 D2H' (3GPP2 Packet), the receiver of the GRE packet shall assume that the protocol type in the User Traffic field is set to what is indicated in the A8 Traffic ID IE in the A9-Setup-A8 and A9-Connect-A8 messages.

For A10 connections, when the Protocol Type field is set to '88 D2H' (3GPP2 Packet), the receiver of the GRE packet shall assume that the protocol type in the User Traffic

1 field is set to what is indicated in the Session Specific Extension IE in the A11-
 2 Registration Request and A11-Registration Reply messages.

3 With the A8 and A10 connections in place, link layer/network layer packets pass over
 4 these connections in both directions between the BS and the PDSN using GRE framing.
 5 In the direction towards the BS, the PDSN encapsulates the link/network layer frames in
 6 GRE frames and sends them on the IP connection between the PDSN and PCF. The PCF
 7 decapsulates the link/network layer frames in GRE frames before forwarding them on the
 8 IP connection between the PCF and the BS. The BS accepts these GRE frames, strips the
 9 GRE headers, and processes the link/layer frames as normal incoming frames by passing
 10 them to the upper layer. The other direction behaves analogously: The BS encapsulates
 11 the link layer/network layer frames in GRE frames and sends them on the IP connection
 12 between the BS and the PCF, the PCF decapsulates the link/network layer frames
 13 received from the IP connection and re-encapsulates the link/network layer frames in
 14 GRE frames before forwarding them on the IP connection between the PCF and the
 15 PDSN. The PDSN accepts the GRE frames, strips the GRE headers, and processes the
 16 link/layer frames as normal incoming frames by passing them to the upper layer.

17 GRE encapsulates user traffic as shown in Figure 2.6-1.



18 **Figure 2.6-1 GRE Encapsulated User Traffic**

19 Figure 2.6-2 shows the structure of the 3GPP2 GRE frame.

0					1					2					3																
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
C	r	K	S	Reserved					Ver		Protocol Type																				
Key																															
Sequence number (Optional)																															
Attributes (Optional)																															
User Traffic (Optional)																															

20 **Figure 2.6-2 3GPP2 GRE Frame**

21 The 3GPP2 GRE header shall be encoded as follows:

- 22 C (Checksum Present) '0'
- 23 r (reserved) '0'
- 24 K (Key Present) '1'
- 25 S (Sequence Number Present) '0 or 1'

1 Reserved '00000000'

2 Ver (Version Number) '000'

3 Protocol Type Hex '88 81H' for "Unstructured Byte Stream", or hex
 4 '88 D2H' for "3GPP2 Packet". The protocol type
 5 shall be set to "3GPP2 Packet" only if the packet
 6 contains attributes. Otherwise it shall be set to
 7 "Unstructured Byte Stream". If the receiving entity
 8 does not recognize the value of this field, it should
 9 discard the GRE frame.

10 Key The Key field contains a four-octet number. The Key
 11 field is used for identifying an individual A8 or A10
 12 connection.

13 Sequence number If the link layer/network layer protocol requires that
 14 the GRE packets be delivered in sequence (e.g. if a
 15 state-full compression mechanism is in use) over the
 16 connection, the S indicator shall be set to '1' and the
 17 sequence number field shall be included in each GRE
 18 packet sent over the connection. The sequence
 19 number field is used for in-order delivery of the
 20 encapsulated user data. For each GRE connection
 21 (identified by the Key field) and direction, the
 22 sending and receiving entities shall each maintain at
 23 most one Sequence Number counter independent of
 24 the Protocol Type field. When the sequence number
 25 field is included, the sender and receiver shall
 26 perform the following:

- 27 • The sequence numbers shall be set to zero after
 28 the connection is established.
- 29 • The sequence number shall be incremented
 30 according to [37] in each subsequent packet sent
 31 on the same connection
- 32 • Receipt of an out-of-sequence packet on a
 33 connection shall be handled according to [37].

34 Attributes If the Protocol Type field is set to '88 D2H' for
 35 "3GPP2 Packet", one or more attributes are included.
 36 Each attribute includes four or more octets and
 37 contains information specific to the attribute.

38 The Attribute format is as follows. The fields are
 39 transmitted from left to right.

0	1	2	3	4	5	6	7	Octet
E	Type							1
Length								2
Value								3
								n

40 **Figure 2.6-3 Attribute Format**

41 E: The E bit is set to 1 for the last attribute in the
 42 attribute list. It is set to zero for all other attributes.

1	Type:	The Type field identifies the type of attribute. If the receiving entity does not recognize the value of this field, it should discard the attribute, but process the remainder of the GRE frame.
2		
3		
4		
5	Length:	The Length field indicates the length in octets of the Value field.
6		
7	Value:	The Value field is two or more octets in length and contains information specific to the attribute. The format and length of the Value field are determined by the Type and Length fields. The Value field may contain one or more reserved bits. The sending entity shall set the reserved bits to '0' and the receiving entity shall ignore the value of the reserved bits. If the receiving entity does not recognize the value of any non-reserved portion of this field, it should discard the attribute, but process the remainder of the GRE frame.
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18	User Traffic	The User Traffic may follow the last attribute in the attribute list, indicated by the E bit set to 1.
19		

2.6.1 GRE Attributes

This section contains the specification of attributes that may be included in a GRE frame when the Protocol Type field is set to '88 D2H' for "3GPP2 Packet".

2.6.1.1 Short Data Indicator

If the packet is tagged by the PDSN as being suitable for SDB transmission, it is identified by an attribute defined as follows:

0	1	2	3	4	5	6	7	Octet
E = [0,1]	Type = '000 0001'							1
Length = 02H								2
SDI = '1'	Reserved							3
Reserved								4

26	Type	'000 0001' – Short Data Indication
27	Length	02H
28	SDI	0 – Reserved
29		1 – packet suitable for SDB transmission

2.6.1.2 Flow Control Indication

If the PDSN has enabled flow control, the PCF may control the flow of packet data in the forward direction by including XON/XOFF signals in GRE frames sent to the PDSN, as follows:

0	1	2	3	4	5	6	7	Octet
E = [0,1]	Type = '000 0010'							1
Length = 02H								2

0	1	2	3	4	5	6	7	Octet
Reserved								4

- 1 Type: '000 0011' – IP Flow Discriminator
- 2 Length: 02H
- 3 Flow ID: This field contains the flow ID. Refer to [8] for detailed information.

4 **2.6.1.4 Segmentation Indication**

5 If the packet is segmented, sequence numbers shall be required and the overall User
6 Traffic length is identified by an attribute defined as follows:

0	1	2	3	4	5	6	7	Octet
E = [0,1]	Type = '000 0100'							1
Length = 02H								2
Value = '00'-'10'		Reserved						3
Reserved								4

- 7 Type: '000 0100' - Segmentation Indication
- 8 Length: 02H
- 9 Value: The segmentation indication Value is coded as follows.
- 10 '00' - Packet started
- 11 '01' - Packet continued
- 12 '10' - Packet ended
- 13 Other - reserved

14 **2.6.2 Relationship of GRE tunnel to Quality of Service**

15 The user's IP traffic associated with the packet data service is tunneled across the RAN
16 using GRE/IP transport. The inner IP packet is the packet transmitted between the user
17 (e.g. Mobile Station (MS)) and its correspondent node (e.g. Internet server). The outer IP
18 packet transports (or tunnels) a portion of the inner packet between the RAN components
19 (i.e., BS, PCF, PDSN). Thus, the inner and outer packets may have inner and outer DSCP
20 values whose usage is described as follows.

21 If the RAN supports QoS on the A8/A9 and A10/A11 interfaces, the RAN shall have a
22 local RAN transport network QoS policy which indicates which outer DSCP values can
23 be used by the PDSN, PCF and BS for traffic. These DSCP values shall be made
24 available to the PDSN (e.g. via OAM&P functions) to enable QoS for the RAN transport
25 network.

26 When QoS is required for GRE tunnels across the A8/A10 transport network, the IOS
27 shall implement Diffserv as described in section 2.4.4 to support intra-network QoS
28 requirements. In addition, the BS, PCF and PDSN shall follow specific mapping rules as
29 follows:

- 30 1. The PDSN shall mark packets in the GRE tunnel (outer DSCP value) according to
- 31 the policy in use by the RAN transport network (refer to section 2.4.4) connecting
- 32 the PDSN to the PCF. This policy is local and specifies the DSCP values for use on
- 33 each GRE tunnel (i.e., service instance) instantiated on the PDSN.

- 1 2. The PCF and BS shall use the local QoS policy (refer to section 2.4.4) to set the
2 outer DSCP value of the packets in the GRE tunnels (i.e., service instance). Since the
3 PCF and BS are not required to inspect the encapsulated IP packets to derive the
4 inner DSCP value, the PCF and BS may mark all GRE packets in the same service
5 instance (SI) with the same DSCP value. The PCF and BS may also set the DSCP
6 value of all GRE packets associated with the same user to the same value if this is
7 the local policy.
- 8 3. The BS may use the outer DSCP value for RAN QoS functions (e.g. RLP frame
9 prioritization). However, the BS is not required to differentiate between packets in
10 the same SI or between users.

11 **2.6.3 GRE Protocol Usage for VoIP SOs**

12 GRE encapsulation is used to transport Voice over Internet Protocol (VoIP) frames. Like
13 the A8/A10 connections for ordinary packet data, the GRE Key field is used to
14 demultiplex these connections in the BS, PCF and PDSN. The GRE frame shall be
15 encapsulated in an IP packet sent between the PCF and PDSN on the A10 interface. The
16 GRE frame shall be encapsulated in an IP packet sent between the BS and PCF on the A8
17 interface. 1x VoIP SOs 60 and 61 define their own format for the GRE payload and may
18 make use of the GRE sequence number or may require the sequence number to be absent.
19 Refer to the SO specification [18] for more details.

20 **2.7 Use of RTP**

21 Real-time Transport Protocol (RTP) provides an end-to-end network transport function
22 suitable for applications transmitting real-time data, such as audio, video, or simulation
23 data, over multicast or unicast network services [39]. The complete specification of RTP
24 also includes profile specifications (e.g. RTP/AVP) and payload type definitions [40].

25 **2.8 Use of SUA**

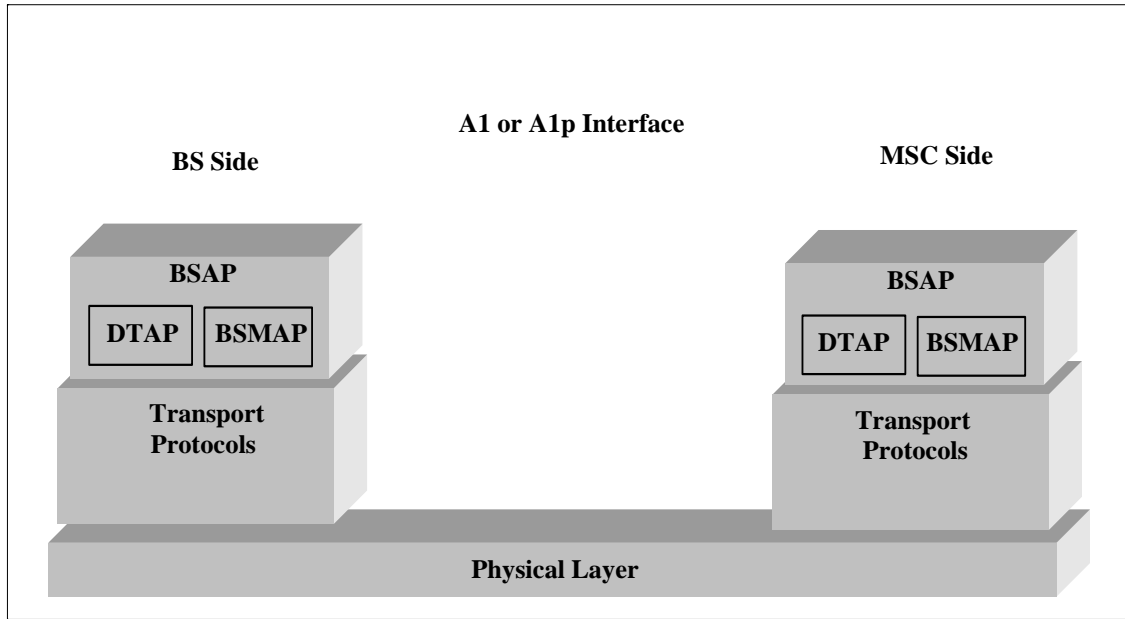
26 The Signaling Connection Control Part User Adaptation Layer (SUA) [42] defines a
27 protocol for the transport of SS7 SCCP user-protocols, such as BSAP, over IP using
28 SCTP.

29 **2.9 Base Station Application Part**

30 The Base Station Application Part (BSAP) is the application layer signaling protocol that
31 provides messaging to accomplish the functions of the A1 or A1p interface component of
32 the MSC - BS interface. BSAP is split into two sub-application parts; the BS
33 Management Application Part (BSMAP), and the Direct Transfer Application Part
34 (DTAP).

35 A distribution function located in the BSAP, which is reflected in the protocol
36 specification by the layer 3 (A1 or A1p) header, performs the discrimination between
37 BSMAP and DTAP messages. Refer to [14] for more information.

38 Refer to Figure 2.9-1 for an illustration of this structure.



1
2 **Figure 2.9-1 A1 or A1p Interface Signaling Protocol Reference Model**

3 **2.9.1 The BS Management Application Part**

4 The BSMAP supports all Radio Resource Management and Facility Management
5 procedures between the MSC and the BS or a cell(s) within the BS. BSMAP messages
6 are not passed to the MS, but are used only to perform functions at the MSC or the BS. A
7 BSMAP message (Complete Layer 3 Information) is also used together with a DTAP
8 message to establish a connection for an MS between the BS and the MSC, in response to
9 the first layer 3 air interface message sent by the MS to the BS for each MS system
10 request. The description of the layer 3 protocol for the BSMAP information exchange is
11 contained in [14].

12 **2.9.2 The Direct Transfer Application Part**

13 The DTAP messages are used to transfer call processing and mobility management
14 messages between the MSC and BS. DTAP messages carry call processing and mobility
15 management information that is primarily used by the MS. The BS shall map the DTAP
16 messages going to the MSC from the appropriate air interface signaling protocol.

17 **2.10 Use of SCTP**

18 SCTP provides a reliable message transport in IP networks. SCTP is used without any
19 modifications and is defined in [38].

20 An SCTP connection between two endpoints is called an association. One SCTP
21 association can be considered as a logical aggregation of streams. A stream is a
22 unidirectional logical channel between two endpoints. To achieve bi-directional
23 communications, two streams are necessary, one in each direction. Each user message
24 (i.e., a message originated from the user application above SCTP) handled by SCTP has
25 to specify the stream to which it is attached. A stream identifier exists for each stream
26 within an association. Therefore, each SCTP stream can be considered as an independent

1 flow of user messages from one node to another. This stream independence characteristic
2 provides a mechanism to avoid and/or manage blocking between streams.

3

1

2

(This page intentionally left blank.)

3

4

5

3.0 Interface Specific Protocol Requirements

This section provides specific requirements for various protocol layers used in the IOS interfaces.

3.1 A1, A2, and A5 Interfaces

This section applies only to circuit-switched MSCs. All references to “MSC” in this section are references to circuit-switched MSCs.

The MSC-BS interface consists of user traffic channels and signaling channels. In general, user traffic channels are independent of signaling channels. Different paths and different underlying transport technologies can be employed for each.

The A1 interface shall use one of the channelized physical layer protocols T1 or E1 interface from section 2.1. The T1 and E1 may be mapped into one of the higher digital hierarchy protocols (e.g., T3, OC3, or STM1) specified in section 2.1. The A1 signaling interface is used to establish A2 and A5 user traffic circuit connections.

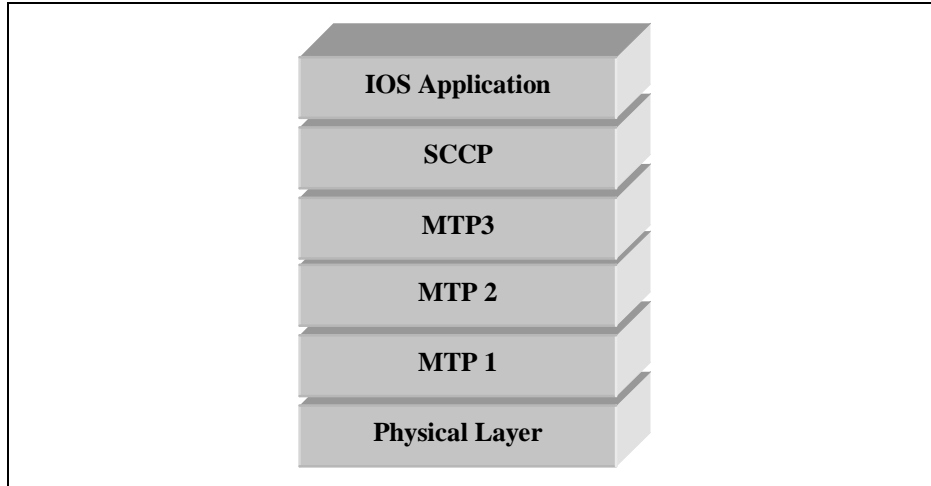
As a BS/MSC agreed option, Dedicated Signal Level 0 (DS0) signaling link(s) may be used instead of the T1/E1 interface.

The A2 and A5 interface shall use one of the channelized physical layer protocols T1 or E1 interface from section 2.1. The T1 and E1 may be mapped into one of the higher digital hierarchy protocols (e.g., T3, OC3, or STM1) specified in section 2.1.

This standard assumes the use of Signaling System Number 7 (SS7) signaling for the transport protocol on the A1 interface.

3.1.1 Signaling Connection Transport Protocol Options

Signaling over the A1 interfaces requires a reliable transport protocol and appropriate addressing and routing mechanisms to deliver messages from source to destination. The IOS application is independent of the underlying transport, which is left to the discretion of operators and manufacturers. The signaling protocol stack options available to operators and manufacturers for the A1 interface is shown in Figure 3.1.1-1.



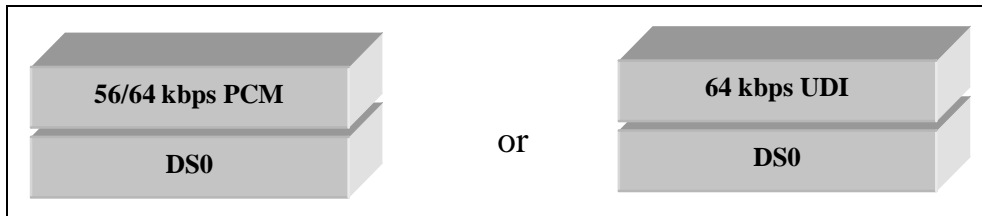
1
2

Figure 3.1.1-1 A1 Signaling Protocol Stack

3.1.2 User Traffic Connection Transport Protocol Options

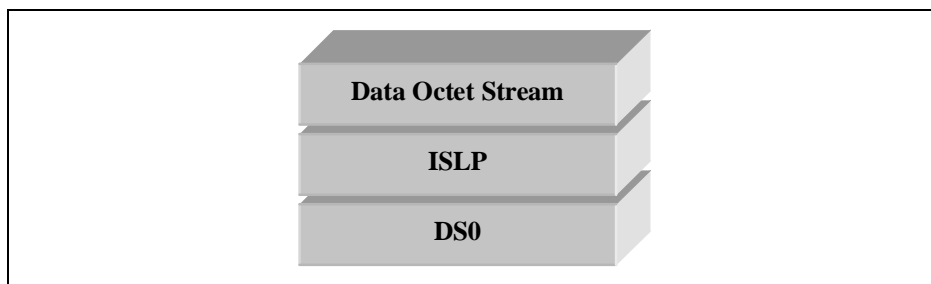
3
4
5
6

The protocol stack options for transport of user traffic that are available to operators and manufacturers are shown in Figure 3.1.2-1 and Figure 3.1.2-2. The link layer for the A5 interface uses the Intersystem Link Protocol (ISLP) [19].



7
8

Figure 3.1.2-1 A2 User Traffic Protocol Stacks



9
10

Figure 3.1.2-2 A5 User Traffic Protocol Stacks

3.1.3 Use of ANSI SS7 Transport (Layer 2)

11
12
13

This standard specifies multiple protocols for the transport of signaling and user information. Refer to sections 3.1.1 and 3.1.2.

1 When SS7 is used to provide signaling transport, the underlying transport mechanism
 2 defined to carry signaling information between the BS and the MSC is the Message
 3 Transfer Part (MTP) and the Signaling Connection Control Part (SCCP).

4 The MTP and SCCP are used to transport the application layer signaling protocol, which
 5 is defined as the BSAP.

6 Information for this section was excerpted from [21] and [22]. Section 3.1.3.2 deals with
 7 the MTP. Section 3.1.3.3 deals with SCCP and its use.

8 The MTP provides a mechanism giving reliable transfer of signaling messages. Section
 9 3.1.3.2 deals with the subset of the MTP that can be used between a BS and a MSC,
 10 which is compatible with a full MTP.

11 SCCP is used to provide a referencing mechanism to identify a particular transaction
 12 relating to, for instance, a particular call. Section 3.1.3.3 identifies the SCCP subset that
 13 shall be used between a BS and an MSC. SCCP can also be used to enhance the message
 14 routing for operations and maintenance information.

15 3.1.3.1 Field of Application

16 This section is applicable to the signaling between BSs and MSCs in Public Land Mobile
 17 Networks (PLMNs). It provides a minimum set of MTP requirements that may be
 18 implemented at a BS or MSC, while maintaining compatibility with the implementation
 19 of a full specification of the MTP.

20 This section defines the interfaces at the 56 or 64 kbps boundary to the BS or MSC and
 21 applies primarily to digital access arrangements. The use of analog arrangements is not
 22 supported.

23 The reliability of signaling links is an administrative concern. It is recommended that in
 24 the case where more than one multiplex system is required and reliability reasons dictate
 25 the use of multiple link sets, then each signaling link should be assigned in a different
 26 multiplex system.

27 Only the associated mode of signaling is applicable to the BS.

28 3.1.3.2 Message Transfer Part

29 The American National Standards Institute (ANSI) recommendations concerning MTP
 30 shall be taken as being requirements unless covered by a statement in this section.

31 3.1.3.2.1 General

32 The MTP functions as specified in [21] are applicable. However, the following
 33 exceptions and modifications to those recommendations may be applied for the MSC to
 34 BS signaling. Refer to section 3.1.3.2.2 through section 3.1.3.2.4.

35 3.1.3.2.2 Level 1 (Chapter 2 of [21])

36 **Chapter 2, Figure 2**

37 These figures are for information only. For the A1 interface, interface point C is
 38 appropriate.

1 **Chapter 2, Section 1.4 Analog Signaling Link**

2 The use of analog signaling links is not an available option.

3 **Chapter 2, Section 2 General**

4 A signaling rate of 56/64 kbps is normally used. When higher speeds are needed, 1.536
5 Mbps digital paths can be used for the signaling data link.

6 **Chapter 2, Section 3 Error Characteristics and Availability**

7 Error characteristics and availability are an operator concern. Excessive errors could lead
8 to inefficient use of the signaling links.

9 **Chapter 2, Section 5 Digital Signaling Link**

10 The standard arrangement is to derive the signaling link from a T1/E1 digital path.
11 However, dedicated DS0 signaling link(s) may be used as a BS/MSC agreed option.

12 **Chapter 2, Section 6 Analog Signaling Data Link**

13 Only digital signaling data links are supported.

14 3.1.3.2.3 Level 2 (Chapter 3 of [21])

15 **Chapter 3, Section 1.4 Signal Unit Error Correction**

16 Only the basic error correction protocol is required.

17 **Chapter 3, Section 7 Signaling Link Initial Alignment Procedure**

18 In the initial alignment procedure specified in Chapter 3 of [21], only the emergency
19 proving period is applicable for the BS. Thus, in states 02 and 03 of the initial alignment
20 procedure status indication "N" is not sent from the BS. The BS should be capable of
21 recognizing status indication "N" if received in order for the alignment procedure to
22 complete.

23 3.1.3.2.4 Level 3 (Chapter 4 of [21])

24 **Chapter 4, Section 1.1.2 End Point of a Signaling Link**

25 The BS is only implemented as the end point of a signaling link. There are no Signaling
26 Transfer Point (STP) network management features in the BS.

27 **Chapter 4, Section 2**

28 Since STP functions are not required for discrimination and routing, MTP functions used
29 between the MSC and the BS can be simplified. Since the implementation of this
30 interface is intended only for point-to-point applications, the routing function within MTP
31 is preset to select the point code appropriate to the parent MSC.

1 **Chapter 4, Section 2.2 Routing Label**

2 Load sharing is performed on the BS with more than one signaling link by means of the
3 Signaling Link Selection field.

4 **Chapter 4, Section 2.3 Message Routing Function**

5 Load sharing between link sets is not required since there can only be one link set
6 between the BS and MSC.

7 **Chapter 4, Section 2.3.5 Handling of Messages under Signaling Link Congestion**

8 The procedures for handling message congestion priority levels as defined for U. S.
9 Signaling Networks in Chapter 4, section 2.3.5.2 of [21] shall be followed. The message
10 priorities given in Appendix B (of Chapter 5 of [21]) for SCCP and MTP messages shall
11 be used. The remaining message priorities for BSMAP and DTAP messages are provided
12 in [14].

13 **Chapter 4, Section 2.4 Message Discrimination**

14 At the BS, only messages with a correct Destination Point Code (DPC) are accepted.
15 Other messages are discarded. It is recommended that discarding a message because of an
16 incorrectly set point code should cause an incident report to be generated.

17 At an MSC (which has the capability of acting as an STP), administration procedures
18 may determine that each message received from a BS signaling link is passed through a
19 “screening” function that checks that the DPC of the message is the same as the Signaling
20 Point code of the exchange. If that is the case, the message is sent to the normal MTP
21 message handling functions. Otherwise, the message is discarded and an incident report is
22 made.

23 **Chapter 4, Section 3 Signaling Network Management**

24 Since the A1 interface utilizes point to point signaling between the BS and the MSC, the
25 Signaling Route Management procedures, including the status of signaling routes,
26 signaling route restricted, signaling route unavailability and availability, are not required.

27 **Chapter 4, Section 3.8 Signaling Network Congestion**

28 The procedures defined for U. S. Networks shall be followed for handling congestion on
29 signaling links.

30 **Chapter 4, Section 4 Signaling Traffic Management**

31 Since the A1 interface utilizes point to point signaling, the Traffic Management
32 procedures supporting signaling routes, including signaling route restricted, signaling
33 route unavailability and availability, are not required.

34 **Chapter 4, Section 4.2**

35 The normal routing situation is that there are one or more signaling links available
36 between the BS and MSC, and these links constitute a link set. They are run in load
37 sharing mode and changeover and change back procedures are supported between these
38 signaling links.

1 **Chapter 4, Section 4.3.3**

2 There is no alternative link set.

3 **Chapter 4, Section 5 Changeover**

4 Changeover between link sets is not applicable.

5 **Chapter 4, Section 6 Change back**

6 Change back between link sets is not applicable.

7 **Chapter 4, Section 7 Forced Rerouting**

8 Forced rerouting is not applicable since there is only one signaling route existing between
9 the BS and the MSC.

10 **Chapter 4, Section 8 Controlled Rerouting**

11 Controlled rerouting is not applicable since there is only one signaling route existing
12 between the BS and the MSC.

13 **Chapter 4, Section 9 MTP Restart**

14 The MTP Restart procedure is not required.

15 **Chapter 4, Section 11 Signaling Traffic Flow Control**

16 The Signaling Route Management procedures supporting signaling traffic flow control
17 including signaling route unavailability and signaling route set congestion are not
18 applicable for the A1 interface.

19 **Chapter 4, Section 12 Signaling Link Management**

20 Only basic link management procedures are applicable.

21 **Chapter 4, Section 13 Signaling Link Management**

22 Signaling Route Management procedure is not applicable for the A1 interface since it is a
23 point to point connection. No action is required upon reception of a Transfer-Prohibited
24 Signal, Transfer-Restricted Signal, Transfer-Allowed Signal, Signaling Route Set Test,
25 Signaling Route Set Congestion Test, or Transfer Control message.

26 **Chapter 4, Section 14.2.1**

27 Since all messages are passed using the SCCP, the service indicator is: D=0, C=0, B=1,
28 A=1.

29 **Chapter 4, Section 14.2.2**

30 The sub service field is always set to D=1, C=0, to indicate a national network.

31 **Chapter 4, Section 15**

32 The formats and codes listed are only relevant to the messages that are required.

3.1.3.2.5 Testing and Maintenance (Chapter 7 of [21])

Chapter 7, Section 2.1 Signaling Data Link Test

The Signaling Data Link Test procedure is not required for the A1 interface.

Chapter 7, Section 2.2

The generation of a Signaling Link Test Message (SLTM) is not applicable at the BS; however the BS shall be capable of responding with an acknowledgment message to an SLTM.

3.1.3.2.6 Interface Functions

The method of interfacing to the higher layers is by the primitives defined in Chapter 1 of [21].

The primitives defined are:

- MTP Pause indication
- MTP Resume indication
- MTP Status indication
- MTP Transfer request
- MTP Transfer indication

3.1.3.2.7 Overload Control (Message Throughput Congestion)

MTP overload control is not required.

3.1.3.3 SCCP Transport Layer Specification (SCCP Functions)

3.1.3.3.1 Overview

The purpose of this section is to identify the subset of the SCCP functions that are necessary to achieve the management of the MS transactions in the A1 interface, and to provide addressing facilities. If this subset of SCCP functions is implemented, compatibility with a full ANSI SCCP shall be maintained. Only the needs of the BSAP are taken into account in this section.

The following simplifications are applicable to the signaling between BS and MSC in PLMNs:

- To limit the complexity of the procedures, a BS exchanges signaling messages only with its MSC, where a protocol conversion may be needed in some cases. Therefore, no SCCP translation function is required in the MSC between the national and the local SCCP and MTP within the MSC area.
- Several functions of the SCCP are not used on the A1 interface: error detection, receipt confirmation, and flow control.
- The segmenting/reassembling function shall be used if the total message length exceeds the maximum allowed message length that can be carried by the MTP.

1 **Chapter 2, Section 2.6**

2 The Data Form 2 (DT2) message is not used.

3 **Chapter 2, Section 2.7**

4 The Expedited Data message is not used.

5 **Chapter 2, Section 2.8**

6 The Expedited Data Acknowledgment message is not used.

7 **Chapter 2, Section 2.10**

8 The Protocol Data Unit Error message is not used; the inconsistent messages of the SCCP
9 protocol are discarded.

10 **Chapter 2, Section 2.13**

11 The Reset Confirm message is not used.

12 **Chapter 2, Section 2.14**

13 The Reset Request message is not used.

14 **Chapter 2, Section 3.5**

15 The Subsystem-Out-Of-Service-Grant (SOG) message is not used.

16 **Chapter 2, Section 3.4**

17 The Subsystem-Out-Of-Service (SOR) message is not used.

18 **Chapter 2, Section 2.16**

19 The Unit Data Service message is not used.

20 **Chapter 2, Section 4.2**

21 The “credit” parameter field is not used for protocol class 2. However, the parameter
22 shall still be included in the Inactivity Test (IT) message for syntax reasons.

23 **Chapter 2, Section 4.6**

24 The “error cause” parameter field is not used.

25 **Chapter 2, Section 4.10**

26 The “receive sequence number” parameter is not used.

27 **Chapter 2, Section 4.13**

28 The “reset cause” parameter field is not used.

1 **Chapter 2, Section 4.16**

2 The “sequencing/segmenting” parameter field is not used for protocol class 2. However,
3 the parameter shall still be included in the IT message for syntax reasons.

4 **3.1.3.3.4 SCCP Formats and Codes (Chapter 3 of [22])**

5 **Chapter 3, Section 3.4**

6 For point-to-point network structures (i.e., direct connections between the MSC and BS),
7 the called party address may consist of the single element: subsystem number.

8 No global title is used. The signaling point code which is coded in the MTP routing label
9 and the Subsystem Number (SSN) in the called party address allow the routing of the
10 message.

11 **Chapter 3, Section 3.4.2.2**

12 SSN Values: BSAP = 11111100, (252)

13 Use of alternative values is an administrative concern.

14 Note: It was determined that the IOS A1 interface should use its own SSN value and this
15 was selected as BSAP = 11111100 (252).

16 **Chapter 3, Section 3.4.2.3**

17 Global title: refer to Chapter 3, section 3.4 of [22].

18 **Chapter 3, Section 3.6**

19 Protocol classes 1 and 3 are not used.

20 **Chapter 3, Sections 3.8, 3.9, 3.10, 3.13, 3.14**

21 Parameters are not used.

22 **Chapter 3, Sections 4.8, 4.9, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16**

23 Messages are not used.

24 **Chapter 3, Section 5.1.1**

25 SOR and SOG are not needed.

26 **3.1.3.3.5 SCCP Procedures (Chapter 4 of [22])**

27 **Chapter 4, Sections 1.1.2.2, 1.1.2.4**

28 Protocol classes 1 and 3 are not used.

1 **Chapter 4, Section 1.1.3**

2 A signaling connection consists of a single connection section. No intermediate nodes are
3 defined in the A1 interface.

4 The use of multiple connections sections is an administrative concern.

5 **Chapter 4, Section 1.2.1 (b)**

6 Not applicable for single connections.

7 **Chapter 4, Section 2.1 (1.)**

8 Global title is not used for single connections.

9 **Chapter 4, Section 2.2.1**

10 SSN is only present in the called party address for single connections.

11 **Chapter 4, Section 2.2.2**

12 The addressing information may take the following form in the N-CONNECT request
13 primitive: DPC+SSN (for single connections).

14 **Chapter 4, Section 2.2.2.2**

15 No SCCP translation function is required for single connections.

16 **Chapter 4, Section 2.3.1 (3)**

17 Not applicable for single connections.

18 **Chapter 4, Section 2.3.2 (4)**

19 Not applicable for single connections.

20 **Chapter 4, Section 3.1.3**

21 Not applicable: no protocol class and flow control negotiations.

22 **Chapter 4, Section 3.1.5**

23 Not applicable.

24 **Chapter 4, Section 3.2.2**

25 Not applicable.

26 **Chapter 4, Section 3.3.4**

27 Not applicable.

28 **Chapter 4, Section 3.5.1.2**

29 Not applicable.

1 **Chapter 4, Section 3.5.2**

2 Not applicable.

3 **Chapter 4, Sections 3.6, 3.7, 3.9, 3.10**

4 Not applicable.

5 **Chapter 4, Section 4.2**

6 Message return is not applicable.

7 **Chapter 4, Section 5**

8 Only those messages and procedures relating to non-replicated subsystems or nodes are
9 required. At the BS the concerned point is the parent MSC. The subsystem involved is
10 the BSAP.

11 **3.1.3.4 Use of the SCCP**

12 The SCCP is used to support signaling messages between the MSC and the BS. BSAP
13 (refer to section 2.9) uses one SCCP signaling connection for the transfer of layer 3 (A1)
14 messages per MS.

15 The SCCP uses both connectionless (Class 0) and connection-oriented (Class 2)
16 procedures to support the BSAP. The procedures in this specification identify whether
17 connection-oriented or connectionless procedures are to be used for each layer 3 (A1)
18 procedure.

19 **3.1.3.4.1 Connection Establishment**

20 The initial messages exchanged in call setup are used to establish an SCCP connection
21 for subsequent signaling communications relating to the call. A new connection is
22 established when individual information related to an MS transaction is required to be
23 exchanged between a BS and an MSC, and no such transaction exists between the MSC
24 and that BS.

25 Two connection establishment cases are distinguished:

26 Case 1. A new transaction (e.g., Location updating, incoming or outgoing call –
27 refer to [13]) is initiated on the radio path. Following an Access
28 Request made by the MS on the Access Channel, the connection
29 establishment is then initiated by the BS.

30 Case 2. The MSC decides to perform an inter-BS handoff (refer to [13]). The
31 connection establishment is then initiated by the MSC.

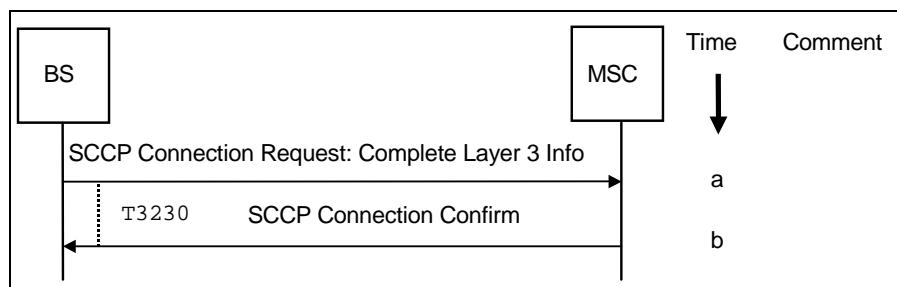
32 **3.1.3.4.1.1 Establishment Procedure - Case 1**

33 In this case, the connection establishment is initiated at the reception by the BS of the
34 first layer 3 message from the MS. Generally, such a message contains the Mobile
35 Identity parameter (Electronic Serial Number (ESN), or International Mobile Subscriber
36 Identity (IMSI)). The BS then constructs the first A1 interface BSMAP message
37 (Complete Layer 3 Information), which includes one of the appropriate DTAP messages
38 (Location Updating Request, Connection Management (CM) Service Request, or Paging
39 Response) depending on whether the MS is accessing the network for the purpose of

1 registration, call origination, or termination. The Complete Layer 3 Information message
 2 is sent to the MSC in the user data field of the SCCP Connection Request message (refer
 3 to [14]). The Complete Layer 3 Information message includes the cell identity and the
 4 layer 3 message that was received from the MS. The exact coding of the BSMAP
 5 message is specified in [14].

6 Upon receipt of the SCCP Connection Request message, the MSC may determine (for
 7 example based on the type of DTAP message received, or based on the received identity,
 8 whether another association already exists for the same MS) if it should proceed with
 9 connection establishment or not. In the latter case the connection establishment is
 10 refused. This message may optionally contain a BSMAP or DTAP message in the user
 11 data field. Otherwise, an SCCP Connection Confirm message is sent back to the BS. This
 12 message may optionally contain a BSMAP or DTAP message in the user data field.

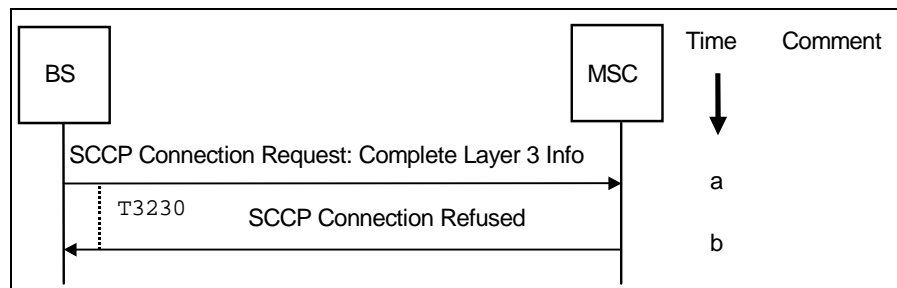
13 The diagram in Figure 3.1.3.4.1.1-1 shows a successful SCCP connection establishment
 14 procedure.



15
 16 **Figure 3.1.3.4.1.1-1 SCCP Connection Establishment**

- 17 a. The BS sends an SCCP Connection Request message, including a user data field, to
 18 the MSC. The BS starts timer T_{3230} . Refer to [14] for the T_{3230} timer definition.
- 19 b. Upon receipt of the SCCP Connection Request message, the MSC sends an SCCP
 20 Connection Confirm message, which may contain a Layer 3 application message, to
 21 the BS. Upon receipt of this message, the BS stops timer T_{3230} and establishes the
 22 connection.

23 The procedures in case of connection establishment refusal are shown in Figure
 24 3.1.3.4.1.1-2.



25
 26 **Figure 3.1.3.4.1.1-2 SCCP Connection Establishment Refusal**

- 27 a. The BS sends an SCCP Connection Request message, including a user data field, to
 28 the MSC. The BS then starts timer T_{3230} .
- 29 b. Upon receipt of the SCCP Connection Request message, the MSC sends an SCCP
 30 Connection Refused message to the BS. Upon receipt of this message, the BS stops
 31 timer T_{3230} .

1 If the user data field of the SCCP Connection Request message contains a Complete
 2 Layer 3 Info message with a Location Updating Request application message, the MSC
 3 shall respond with an SCCP Connection Refused message with a Location Updating
 4 Accept, Location Updating Reject or Service Redirection message in the user data field.

5 **3.1.3.4.1.2 Establishment Procedure - Case 2**

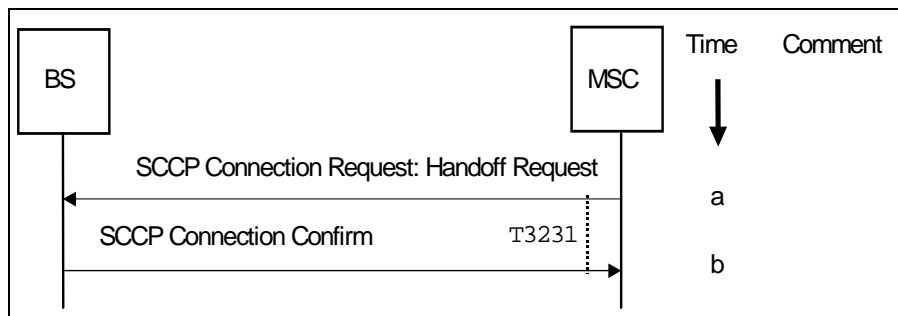
6 In this case, the connection establishment is initiated by the MSC as soon as the MSC
 7 decides to perform an inter-BS handoff.

8 An SCCP Connection Request message is sent to the BS. The user data field of this
 9 message may contain the BSMAP Handoff Request message (refer to [14]). If the layer 3
 10 message is included, it shall be transferred in the user data field of the SCCP Connection
 11 Request to complete the establishment of the relation between the radio channel
 12 requested and the SCCP connection as soon as possible. The exact structure of the user
 13 data field is explained in [14]. If the BS received the SCCP Connection Request message
 14 without the Handoff Request message in the user data field, the BS establishes the SCCP
 15 connection by sending an SCCP Connection Confirm message. In this case, the Handoff
 16 Request and Handoff Request Ack messages are sent as DT1 messages after the SCCP
 17 connection is established.

18 When a BS receives an SCCP Connection Request message that contains a Handoff
 19 Request message in the user data field, the BS performs the necessary checking and
 20 reserves, in the successful case, a radio channel for the requested handoff. If the BS fails
 21 to reserve a radio channel, it may send an SCCP Connection Refuse message with a
 22 Handoff Failure message in the user data field to the MSC. Otherwise, an SCCP
 23 Connection Confirm message is returned to the MSC that may contain the BSMAP
 24 Handoff Request Acknowledge message in the user data field.

25 If the Handoff Request message is received as a DT1 message and the BS fails to reserve
 26 a radio channel for the call, then it shall send a Handoff Failure message as a DT1
 27 message to the MSC.

28 The diagram in Figure 3.1.3.4.1.2-1 shows a successful SCCP connection establishment
 29 procedure during handoff with a Handoff Request message sent in the SCCP Connection
 30 Request message.

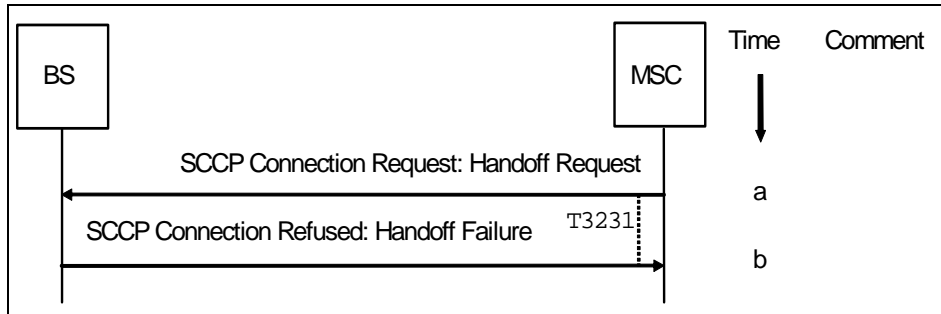


31 **Figure 3.1.3.4.1.2-1 SCCP Connection Establishment with a Handoff Request message in an**
 32 **SCCP Connection Request message**

- 33
- 34 a. The MSC sends an SCCP Connection Request message, including a user data field
 35 that contains a Handoff Request application message, to the BS. The MSC starts
 36 timer T₃₂₃₁. Refer to [14] for the T₃₂₃₁ timer definition.
- 37 b. Upon receipt of the SCCP Connection Request message, the BS sends an SCCP
 38 Connection Confirm message, which shall contain the Layer 3 application message

1 Handoff Request Acknowledge, to the MSC and establishes the connection. Upon
 2 receipt of this message, the MSC stops timer T₃₂₃₁.

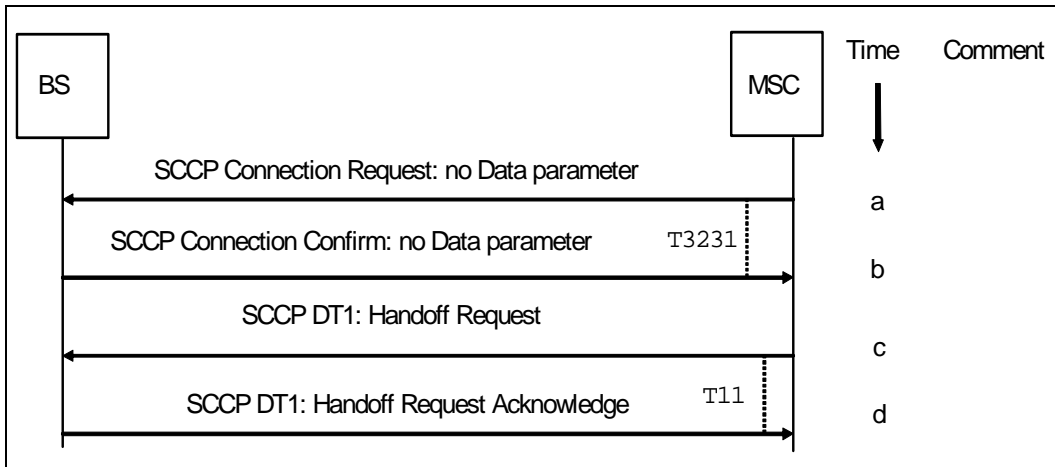
3 The diagram in Figure 3.1.3.4.1.2-2 shows an SCCP connection refusal during handoff.



4
5 **Figure 3.1.3.4.1.2-2 SCCP Connection Refusal During Handoff**

- 6 a. The MSC sends an SCCP Connection Request message, including a user data field
 7 that contains a Handoff Request application message, to the BS. The MSC starts
 8 timer T₃₂₃₁.
- 9 b. Upon receipt of the SCCP Connection Request message, the BS sends an SCCP
 10 Connection Refused message, which contains the Layer 3 application message
 11 Handoff Failure, to the MSC. Upon receipt of this message, the MSC stops timer
 12 T₃₂₃₁.

13 Figure 3.1.3.4.1.2-3 shows a successful SCCP connection establishment procedure during
 14 handoff with a Handoff Request message in the SCCP DT1 message.

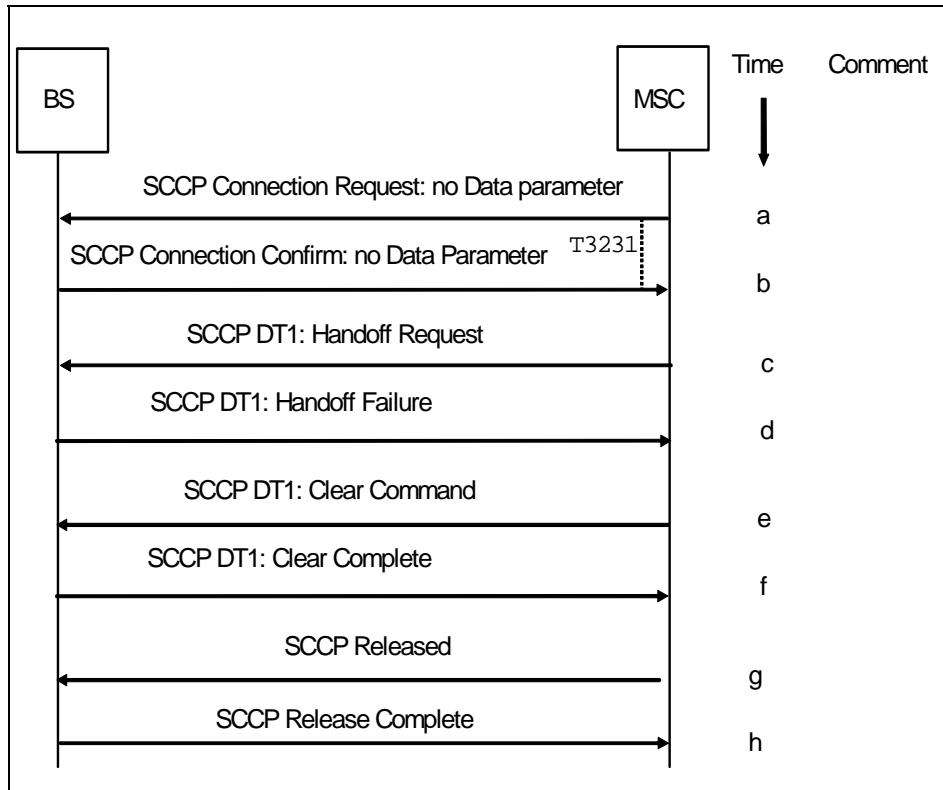


15
16 **Figure 3.1.3.4.1.2-3 SCCP Connection Establishment with a Handoff Request message in an**
 17 **SCCP DT1 message**

- 18 a. The MSC sends an SCCP Connection Request message, excluding the user data field
 19 (i.e., the Data parameter of the SCCP message), to the BS. The MSC starts timer
 20 T₃₂₃₁. Refer to [21] for the T₃₂₃₁ timer definition.
- 21 b. Upon receipt of the SCCP Connection Request message, the BS sends an SCCP
 22 Connection Confirm message, excluding the user data field (i.e., the Data parameter
 23 of the SCCP message), to the MSC and establishes the SCCP connection. Upon
 24 receipt of this message, the MSC stops timer T₃₂₃₁.

- 1 c. The MSC sends an SCCP DT1 message, which includes the user data field (i.e., the
- 2 Data parameter of the SCCP message) containing the Handoff Request message, to
- 3 the BS. The MSC starts timer T₁₁.
- 4 d. Upon receipt of the SCCP DT1 message containing a Handoff Request message and
- 5 if the BS can complete the handoff, the BS sends an SCCP DT1 message in the user
- 6 data field (i.e., the Data parameter of the SCCP message), which shall contain the
- 7 Layer 3 application message Handoff Request Acknowledge, to the MSC. The MSC
- 8 stops timer T₁₁.

9 Figure 3.1.3.4.1.2-4 shows an SCCP connection with handoff failure in which the
 10 Handoff Request message is sent in a DT1 message.



11

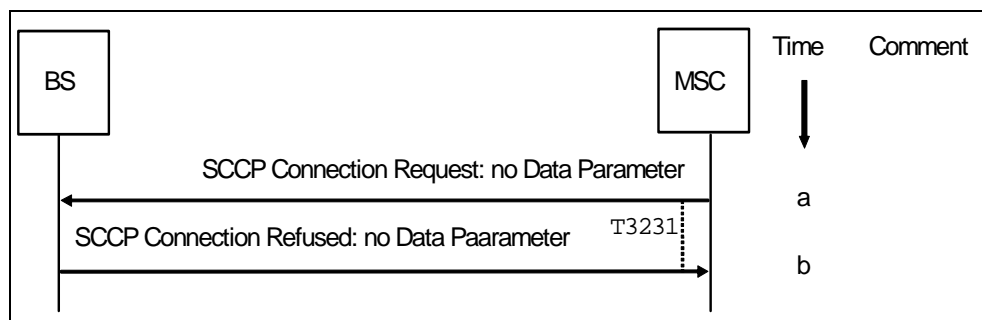
12

Figure 3.1.3.4.1.2-4 SCCP Connection with Handoff Failure via DT1

- 13 a. The MSC sends an SCCP Connection Request message, excluding the user data field
- 14 (i.e., the Data parameter of the SCCP message), to the BS. The MSC starts timer
- 15 T₃₂₃₁.
- 16 b. Upon receipt of the SCCP Connection Request message, the BS sends an SCCP
- 17 Connection Confirmed message, excluding the user data field (i.e., the Data
- 18 parameter of the SCCP message), to the MSC. Upon receipt of this message, the
- 19 MSC stops timer T₃₂₃₁.
- 20 c. The MSC sends an SCCP DT1 message with a Handoff Request message in the user
- 21 data field (i.e., the Data parameter of the SCCP message).
- 22 For additional details of the Handoff Request, Handoff Failure, Clear Command, and
- 23 Clear Complete messages in steps ‘c’ through ‘f’, refer to the Hard Handoff Failure
- 24 call flow in [13].

- 1 d. Upon receipt of the SCCP DT1 message containing a Handoff Request message and
 2 if the BS cannot perform the handoff, the BS sends an SCCP DT1 message
 3 containing a Handoff Failure message in the user data field (i.e., the Data parameter
 4 of the SCCP message) to the MSC.
- 5 e. The MSC sends an SCCP DT1 message with a Clear Command message in the user
 6 data field (i.e., the Data parameter of the SCCP message).
- 7 f. The BS sends an SCCP DT1 message with a Clear Complete message in the user
 8 data field (i.e., the Data parameter of the SCCP message).
- 9 g. The MSC sends an SCCP Released message to the BS.
- 10 h. The BSC sends an SCCP Release Complete message to the MSC.

11 Figure 3.1.3.4.1.2-5 shows an SCCP Connection Refused in response to an SCCP
 12 Connection Request with a null user data field.



13
 14 **Figure 3.1.3.4.1.2-5 SCCP Connection Refused reply to a null SCCP Connection Request**

- 15 a. The MSC sends an SCCP Connection Request message excluding the user data field
 16 (i.e., the Data parameter of the SCCP message) to the BS. The MSC starts timer
 17 T₃₂₃₁.
- 18 b. Upon receipt of the SCCP Connection Request message and if the BS can not
 19 support the connection request, the BS sends an SCCP Connection Refused message
 20 excluding the user data field (i.e., the Data parameter of the SCCP message) to the
 21 MSC. Upon receipt of this message, the MSC stops timer T₃₂₃₁.

22 3.1.3.4.2 Connection Release

23 This procedure is normally initiated at the MSC side but in the case of abnormal SCCP
 24 connection release (refer to section 3.1.3.4.3), the BS may initiate connection clearing.

25 The MSC initiates this procedure with respect to the source BS in normal conditions for
 26 all calls supported by A1 connections.

27 A connection is released when a given signaling connection is no longer required. This
 28 may occur in normal cases:

- 29
- at the end of a transaction (call, location updating);
 - after completion of a successful hard handoff: the connection with the source BS is released.
- 30
 31

32 When either the MSC or the BS sends an SCCP Released (RLSD) message, the user data
 33 field is optional and may contain a transparent layer 3 message (e.g., DTAP) or be empty.
 34 The structure of the user data field, if any, is explained in [14].

1 When receiving this message, the BS releases or the MSC initiates release of all the radio
 2 resources allocated to the relevant MS, if there are still any left, and returns an SCCP
 3 Release Complete (RLC) message.

4 For abnormal cases a connection failure may be detected by the connection supervision
 5 service provided by SCCP. If so, the Reset Circuit procedure described in [14] is used.
 6 For other abnormal SCCP connection releases, refer to section 3.1.3.4.3, "Abnormal
 7 SCCP Release".

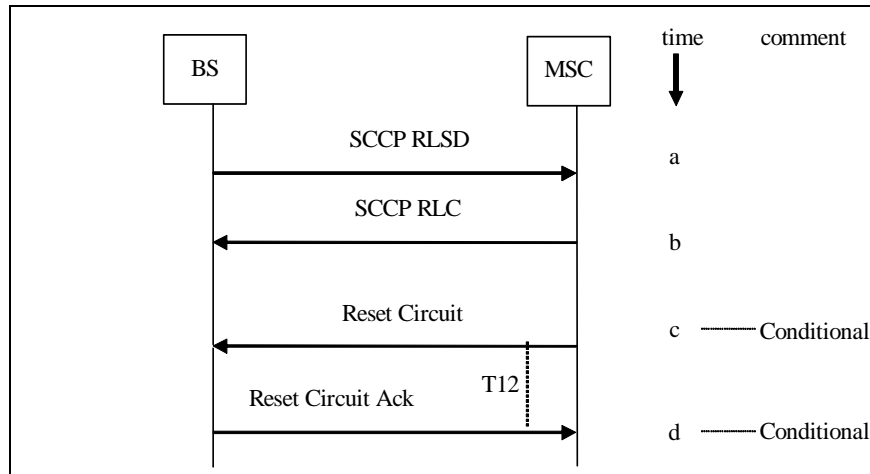
8 **3.1.3.4.3 Abnormal SCCP Release**

9 The normal release of SCCP A1 connections is initiated by the MSC. Under abnormal
 10 conditions, an SCCP connection may be released by the BS to clear resources.

11 Whenever an SCCP connection is abnormally released, all resources associated with that
 12 connection shall be cleared. Abnormal release can result from, for example, resource
 13 failure, protocol error, or unexpected receipt of the SCCP RLSD or SCCP RLC
 14 command.

15 **3.1.3.4.3.1 SCCP Release by BS: Loss of SCCP Connection Information**

16 Figure 3.1.3.4.3.1-1 demonstrates release of an SCCP connection by the BS due to loss of
 17 SCCP connection information. Note that when a circuit(s) is associated with the call at
 18 the MSC, Reset Circuit/Reset Circuit Ack [14] messages need to be exchanged between
 19 the MSC and BS to guarantee release of the circuit by both the MSC and BS.



20 **Figure 3.1.3.4.3.1-1 BS Initiated SCCP Release: BS Lost SCCP Connection Information**

- 21
- 22 a. An unexpected SCCP RLSD message (under abnormal termination) is received by
 23 the MSC from the BS.
- 24 b. The MSC sends an SCCP RLC message to the BS to indicate that the SCCP RLSD
 25 message has been received and that the appropriate procedures have been completed.
- 26 c. If a circuit was involved with the call at the MSC, the MSC sends a Reset Circuit
 27 message to inform the BS that had sent the SCCP RLSD to clear its call data and
 28 starts timer T₁₂. Refer to [14] for the T₁₂ timer definition. The Reset Circuit message
 29 carries the Circuit Identity Code (CIC) of the trunk whose corrupted connection was
 30 released.

- d. The Reset Circuit Ack message informs the MSC that the Reset Circuit has been received and acted upon. The MSC stops timer T_{12} .

3.1.3.4.3.2 SCCP Release by MSC: Loss of SCCP Connection Information

Figure 3.1.3.4.3.2-1 demonstrates release of an SCCP connection by the MSC due to loss of SCCP connection information. Note that when a circuit(s) is associated with the call at the BS, Reset Circuit/Reset Circuit Ack messages [14] need to be exchanged between the MSC and BS to guarantee release of the circuit by both the MSC and BS.

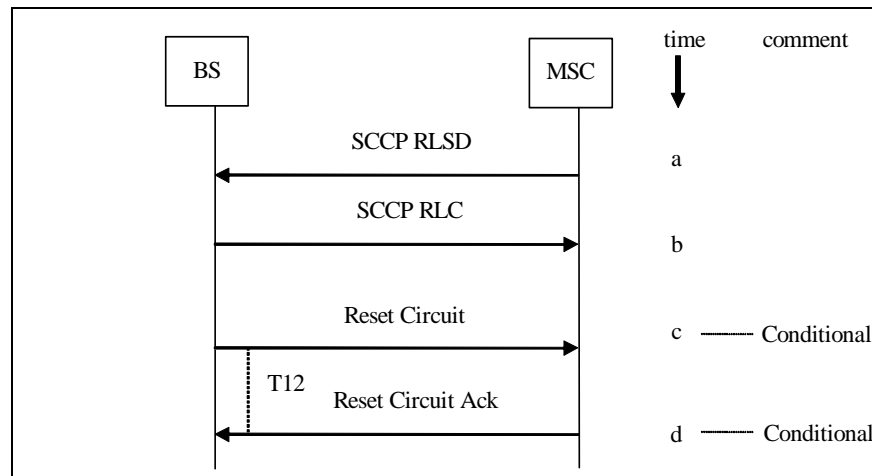
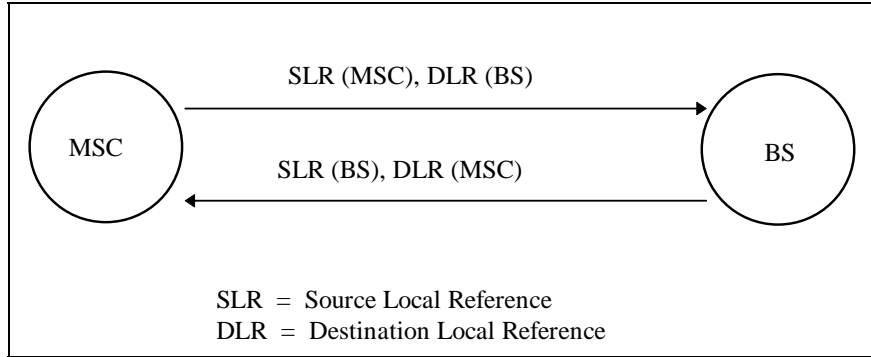


Figure 3.1.3.4.3.2-1 MSC Initiated SCCP Release: MSC Lost SCCP Connection Information

- An unexpected SCCP RLSD message (under abnormal termination) is received by the BS from the MSC.
- The BS sends an SCCP RLC message to the MSC to indicate that the SCCP RLSD message has been received and that the appropriate procedures have been completed.
- If a circuit was involved with the call at the BS, the BS sends a Reset Circuit message to inform the MSC which had sent the SCCP RLSD to clear its call data and starts timer T_{12} . The Reset Circuit message carries the CIC of the trunk whose corrupted connection was released.
- The Reset Circuit Ack message informs the BS that the Reset Circuit has been received and acted upon. The BS stops timer T_{12} .

3.1.3.4.4 SCCP Reference Generation Philosophy

Referring to Figure 3.1.3.4.4-1 “SLR/DLR Usage”, the SCCP local reference number (source/destination) is a three byte element internally chosen by the MSC or BS to uniquely identify a signaling connection. In the direction MSC to BS, the source local reference is chosen by the MSC and the destination local reference is chosen by the BS. In the direction BS to MSC, the source local reference is chosen by the BS and the destination local reference is chosen by the MSC. In the direction MSC to BS, the MSC always echoes the BS Source Local Reference (SLR) in the Destination Local Reference (DLR) field. In the direction BS to MSC, the BS always echoes the MSC SLR in the DLR field. Note that it is the responsibility of the BS and MSC to insure that no two calls have identical SCCP local reference numbers.



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

Figure 3.1.3.4.4-1 SLR/DLR Usage

MSC generation of SCCP local reference numbers shall conform to [22].

3.1.3.4.5 SCCP Transfer of DTAP and BSMAP Messages

The DTAP and BSMAP messages on the A1 interface are contained in the user data field of the exchanged SCCP frames. Table 3.1.3.4.5-1 below summarizes the use of the User Data Field in SCCP frames.

Table 3.1.3.4.5-1 Use of the User Data Field in SCCP Frames

SCCP Frame	User Data Field (BSMAP/DTAP)
Connection Oriented Protocol Class 2	
SCCP Connection Request (CR)	Optional
SCCP Connection Confirm (CC)	Optional
SCCP Connection Refused (CREF)	Optional
SCCP Released (RLSD)	Optional
SCCP Release Complete (RLC)	Not Applicable
SCCP Data Transfer 1 (DT1)	Mandatory
Connectionless Protocol Class 0	
SCCP Unit Data (UDT)	Mandatory

For connection oriented transactions, a connection is requested, obtained or refused using the following SCCP messages (protocol class 2):

- SCCP Connection Request (CR)
- SCCP Connection Confirm (CC)
- SCCP Connection Refused (CREF)
- SCCP Released (RLSD) and SCCP Release Complete (RLC) messages are used to break a connection.

The use of the User Data Field in SCCP frames in the various establishment and release cases is described in section 3.1.3.4.1, “Connection Establishment” and section 3.1.3.4.2, “Connection Release”.

1 For connection oriented (protocol class 2) transactions, once the signaling connection is
 2 confirmed between the MSC and the BS, all A1 interface messages are transported in the
 3 SCCP Data Transfer 1 (DT1) message until the connection is to be dropped.

4 For Connectionless (protocol class 0) transactions, where there is no SCCP connection,
 5 A1 interface messages are transported in the SCCP Unit Data (UDT) message.

6 Table 3.1.3.4.5-2 below indicates which SCCP messages shall be used to transport each
 7 of the application messages on the A1 interface.

Table 3.1.3.4.5-2 Use of SCCP for BSMAP and DTAP Messages

Application Message	Message Discriminator	SCCP Message
Call Processing Messages		
Complete Layer 3 Information	BSMAP	CR ^a
CM Service Request	DTAP	CR ^{a,b}
Paging Request	BSMAP	UDT ^a
Paging Response	DTAP	CR ^{a,b}
CM Service Request Continuation	DTAP	DT1 ^c
Connect	DTAP	DT1
Event Notification	BSMAP	UDT, CREF
Event Notification Ack	BSMAP	UDT
Progress	DTAP	DT1
Service Release	DTAP	DT1
Service Release Complete	DTAP	DT1
Assignment Request	BSMAP	CC ^d , DT1
Assignment Complete	BSMAP	DT1
Assignment Failure	BSMAP	DT1
Clear Request	BSMAP	DT1
Clear Command	BSMAP	DT1
Clear Complete	BSMAP	DT1
Alert With Information	DTAP	DT1
BS Service Request	BSMAP	UDT
BS Service Response	BSMAP	UDT
Additional Service Request	DTAP	DT1
Additional Service Notification	BSMAP	DT1
Supplementary Services Messages		
Flash with Information	DTAP	DT1
Flash with Information Ack	DTAP	DT1
Feature Notification	BSMAP	UDT ^a
Feature Notification Ack	BSMAP	UDT ^a

Table 3.1.3.4.5-2 Use of SCCP for BSMAP and DTAP Messages

Application Message	Message Discriminator	SCCP Message
Priority Access Channel Assignment (PACA) Command	BSMAP	CC ^d , DT1
PACA Command Ack	BSMAP	DT1
PACA Update	BSMAP	UDT
PACA Update Ack	BSMAP	UDT
Radio Measurements for Position Request	BSMAP	DT1
Radio Measurements for Position Response	BSMAP	DT1
Mobility Management Messages		
Authentication Request	DTAP/BSMAP	DT1, UDT ^e
Authentication Response	DTAP/BSMAP	DT1, UDT ^e
SSD Update Request	DTAP	DT1
Base Station Challenge	DTAP	DT1
Base Station Challenge Response	DTAP	DT1
Status Request	DTAP/BSMAP	DT1, UDT ^e
Status Response	DTAP/BSMAP	DT1, UDT ^e
SSD Update Response	DTAP	DT1
Location Updating Request	DTAP	CR ^{a,b}
Location Updating Accept	DTAP	CREF
Location Updating Reject	DTAP	CREF
Mobile Station Registered Notification	BSMAP	DT1
Parameter Update Request	DTAP	DT1
Parameter Update Confirm	DTAP	DT1
Privacy Mode Command	BSMAP	DT1
Privacy Mode Complete	BSMAP	DT1
Registration Request	BSMAP	UDT
User Zone Reject	DTAP/BSMAP	DT1, UDT ^e
User Zone Update	DTAP	DT1
User Zone Update Request	DTAP	DT1
BS Authentication Request	BSMAP	DT1
BS Authentication Response	BSMAP	DT1
Handoff Messages		
Handoff Required	BSMAP	DT1
Handoff Request	BSMAP	CR, DT1 ^h
Handoff Request Acknowledge	BSMAP	CC, DT1 ^f
Handoff Failure	BSMAP	DT1 ^f , CREF ^g

Table 3.1.3.4.5-2 Use of SCCP for BSMAP and DTAP Messages

Application Message	Message Discriminator	SCCP Message
Handoff Command	BSMAP	DT1
Handoff Required Reject	BSMAP	DT1
Handoff Commenced	BSMAP	DT1
Handoff Complete	BSMAP	DT1
Handoff Performed	BSMAP	DT1
Facilities Management Messages		
Block	BSMAP	UDT
Block Acknowledge	BSMAP	UDT
Unblock	BSMAP	UDT
Unblock Acknowledge	BSMAP	UDT
Reset	BSMAP	UDT
Reset Acknowledge	BSMAP	UDT
Reset Circuit	BSMAP	UDT
Reset Circuit Acknowledge	BSMAP	UDT
Service Redirection	DTAP	DT1, CREF
Transcoder Control Request	BSMAP	DT1
Transcoder Control Acknowledge	BSMAP	DT1
Application Data Delivery Service (ADDS) Messages		
ADDS Page	BSMAP	UDT
ADDS Transfer	BSMAP	UDT
ADDS Deliver	DTAP	DT1
ADDS Page Ack	BSMAP	UDT
ADDS Deliver Ack	DTAP	DT1
ADDS Transfer Ack	BSMAP	UDT
Error Handling Messages		
Rejection	DTAP/BSMAP	DT1, UDT ^e

Following are the footnotes referred to in Table 3.1.3.4.5-2.

- a. Required, SCCP DT1 is not an option.
- b. Sent within Complete Layer 3 Information, which is a BSMAP message.
- c. This message may be used in addition to the CM Service Request.
- d. May be used if responding to a CM Service Request or Paging Response.
- e. Used only when the procedure is done on a paging channel.
- f. May be used after an SCCP connection has been established.
- g. May be used if responding to an SCCP Connection Request/Handoff Request.

- 1 h This message is sent as DT1 if it is too large to fit into the User Data field of the
2 Connection Request.

3 **3.2 A1p and A2p Interfaces**

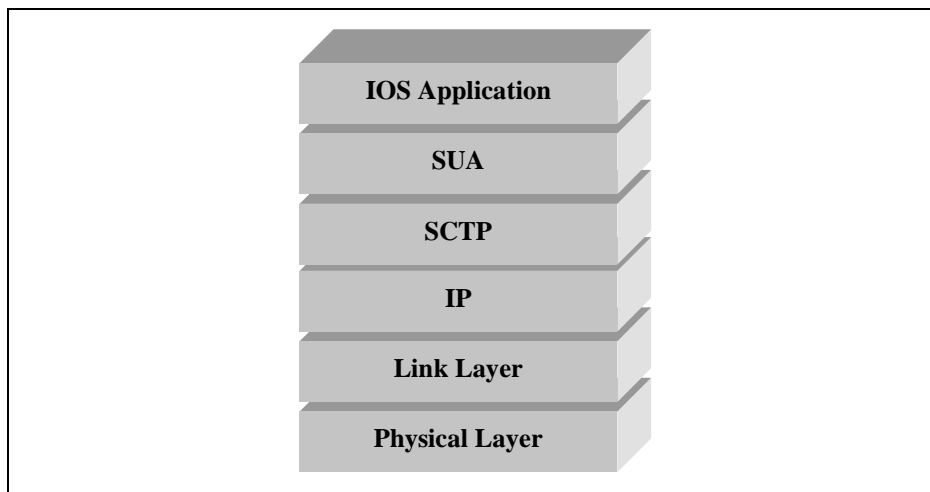
4 The A1p packet based signaling interface between the Legacy MS Domain (LMSD)
5 Mobile Switching Center Emulation (MSCe) and the BS is used in part to establish
6 packet based A2p user traffic connections between the Media Gateway (MGW) and the
7 BS. Message details for A1p and A2p are contained in [14].

8 **3.2.1 Performance Specifications**

9 The performance requirements for the A1p and A2p interface are for further study.

10 **3.2.2 A1p Transport Protocol**

11 Signaling over the A1p interfaces requires a reliable transport protocol and appropriate
12 addressing and routing mechanisms to deliver messages from source to destination. The
13 IOS application is independent of the underlying physical layer and link layer transport,
14 which is left to the discretion of operators and manufacturers. The signaling protocol
15 stack for the A1p interface is shown in Figure 3.2.2-1.



16
17 **Figure 3.2.2-1 A1p Signaling Protocol Stack**

18 **3.2.2.1 Physical Layer (L1) Specification for A1p**

19 The A1p interface shall use one of the L1 specifications in section 2.1.

20 **3.2.2.2 Layer 2 Specification for A1p**

21 The A1p L2 requirements as specified in section 2.2 may apply as per inter-vendor
22 agreements.

23 **3.2.2.3 Use of IP for A1p**

24 The requirements for 2.4.1 and 2.4.2 may apply as per inter-vendor agreements.

1 3.2.2.4 QoS Specifications for A1p

2 The A1p QoS requirements are for further study.

3 3.2.2.5 Security Specifications for A1p

4 The A1p bearer Security Framework requirements are specified in section 2.4.5.

5 3.2.2.6 Use of the SUA for A1p

6 The SUA is used to support signaling messages between the MSCe and the BS. BSAP
7 (refer to section 3.2.2.7) uses one SUA signaling connection for the transfer of layer 3
8 (A1p) messages per MS.

9 The SUA uses both connectionless (Class 0) and connection-oriented (Class 2)
10 procedures to support the BSAP. The procedures in this specification identify whether
11 connection-oriented or connectionless procedures are to be used for each layer 3 (A1p)
12 procedure.

13 The use of SUA in this standard is limited to the equivalent subset of functions that SCCP
14 is limited to in this standard.

15 The procedures and formats for the following SUA messages shall be supported by the
16 A1p interface (refer to [42]). Support for other SUA messages and procedures are for
17 further study.

18 Connectionless messages:

- 19 • Connectionless Data Transfer (CLDT)

20 Connection-Oriented messages:

- 21 • Connection Request (CORE)
- 22 • Connection Acknowledge (COAK)
- 23 • Connection Refused (COREF)
- 24 • Connection Oriented Data Transfer (CODT)
- 25 • Release Request (RELRE)
- 26 • Release Complete (RELCO)

27 3.2.2.6.1 SUA Connection Establishment

28 The initial messages exchanged in call setup are used to establish an SUA connection for
29 subsequent signaling communications relating to the call. A new connection is
30 established when individual information related to an MS transaction is required to be
31 exchanged between a BS and an MSCe, and no such transaction exists between the
32 MSCe and that BS.

33 Two connection establishment cases are distinguished:

34 Case 1. A new transaction (e.g., Location updating, incoming or outgoing call –
35 refer to [13]) is initiated on the radio path. Following an Access
36 Request made by the MS on the Access Channel, the connection
37 establishment is then initiated by the BS.

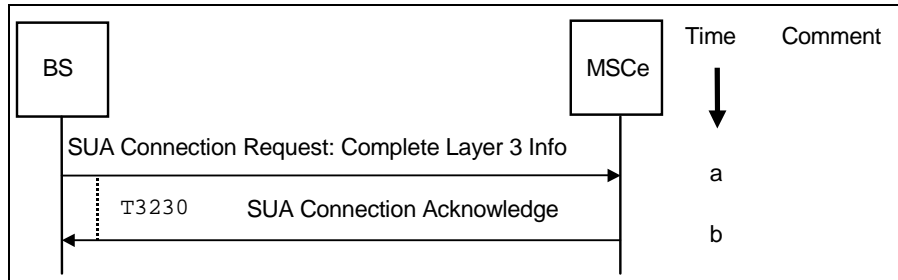
1 Case 2. The MSCe decides to perform an inter-BS handoff (refer to [13]). The
 2 connection establishment is then initiated by the MSCe.

3 **3.2.2.6.1.1 Establishment Procedure - Case 1**

4 In this case, the connection establishment is initiated at the reception by the BS of the
 5 first layer 3 message from the MS. Generally, such a message contains the Mobile
 6 Identity parameter (Electronic Serial Number (ESN), or International Mobile Subscriber
 7 Identity (IMSI)). The BS then constructs the first A1p interface BSMAP message
 8 (Complete Layer 3 Information), which includes one of the appropriate DTAP messages
 9 (Location Updating Request, Connection Management (CM) Service Request, or Paging
 10 Response) depending on whether the MS is accessing the network for the purpose of
 11 registration, call origination, or termination. The Complete Layer 3 Information message
 12 is sent to the MSCe in the user data field of the SUA Connection Request (CORE)
 13 message (refer to [42]). The Complete Layer 3 Information message includes the cell
 14 identity and the layer 3 message that was received from the MS. The exact coding of the
 15 BSMAP message is specified in [14].

16 Upon receipt of the SUA Connection Request message, the MSC may determine (for
 17 example based on the type of DTAP message received, or based on the received identity,
 18 whether another association already exists for the same MS) if it should proceed with
 19 connection establishment or not. In the latter case the connection establishment is
 20 refused. This message may optionally contain a BSMAP or DTAP message in the user
 21 data field. Otherwise, an SUA Connection Acknowledge (COAK) message is sent back
 22 to the BS. This message may optionally contain a BSMAP or DTAP message in the user
 23 data field.

24 The diagram in Figure 3.2.2.6.1.1-1 shows a successful SUA connection establishment
 25 procedure.



26

27 **Figure 3.2.2.6.1.1-1 SUA Connection Establishment**

- 28 a. The BS sends an SUA Connection Request message, including a user data field, to
 29 the MSCe. The BS starts timer T₃₂₃₀. Refer to [14] for the T₃₂₃₀ timer definition.
- 30 b. Upon receipt of the SUA Connection Request message, the MSCe sends an SUA
 31 Connection Acknowledge message, which may contain a Layer 3 application
 32 message, to the BS. Upon receipt of this message, the BS stops timer T₃₂₃₀ and
 33 establishes the connection.

34 The procedures in case of connection establishment refusal are shown in Figure 3.2.2.6.1-
 35 2.

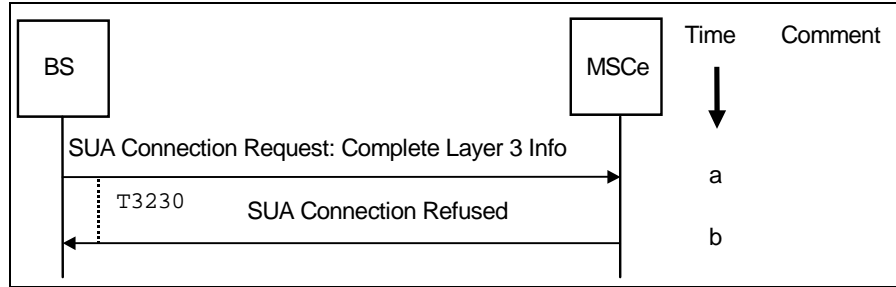


Figure 3.2.2.6.1-2 SUA Connection Establishment Refusal

- a. The BS sends an SUA Connection Request message, including a user data field, to the MSCe. The BS then starts timer T₃₂₃₀.
- b. Upon receipt of the SUA Connection Request message, the MSCe sends an SUA Connection Refused (COREF) message to the BS. Upon receipt of this message, the BS stops timer T₃₂₃₀.

If the user data field of the SUA Connection Request message contains a Complete Layer 3 Info message with a Location Updating Request application message, the MSCe shall respond with an SUA Connection Refused message with a Location Updating Accept, Location Updating Reject, Service Redirection message in the user data field.

3.2.2.6.1.2 Establishment Procedure - Case 2

In this case, the connection establishment is initiated by the MSCe as soon as the MSCe decides to perform an inter-BS handoff.

An SUA Connection Request message is sent to the BS. The user data field of this message shall contain the BSMAP Handoff Request message (refer to [14]). It shall be transferred in the user data field of the SUA Connection Request message to complete the establishment of the relation between the radio channel requested and the SUA connection as soon as possible. The exact structure of the user data field is explained in [14].

When a BS receives an SUA Connection Request message that contains a Handoff Request message in the user data field, the BS performs the necessary checking and reserves, in the successful case, a radio channel for the requested handoff. If the BS fails to reserve a radio channel, it may send an SUA Connection Refused message with a Handoff Failure message in the user data field to the MSCe. Otherwise, an SUA Connection Acknowledge message is returned to the MSCe that may contain the BSMAP Handoff Request Acknowledge message in the user data field.

The diagram in Figure 3.2.2.6.1.2-1 shows a successful SUA connection establishment procedure during handoff.

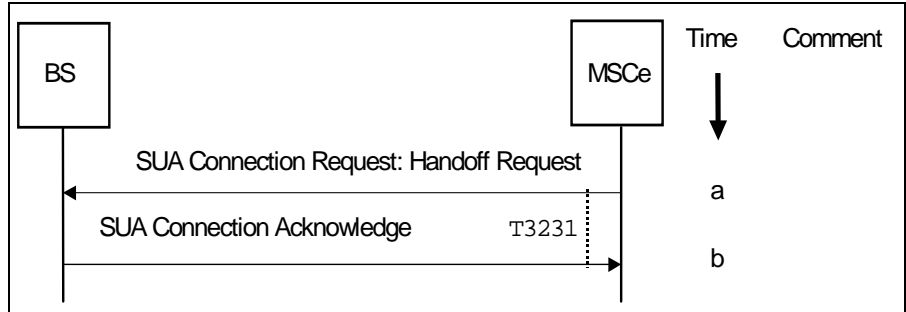


Figure 3.2.2.6.1.2-1 SUA Connection Establishment During Handoff

- a. The MSCe sends an SUA Connection Request message, including a user data field that contains a Handoff Request application message, to the BS. The MSCe starts timer T_{3231} . Refer to [14] for the T_{3231} timer definition.
- b. Upon receipt of the SUA Connection Request message, the BS sends an SUA Connection Acknowledge message, which shall contain the Layer 3 Handoff Request Acknowledge application message, to the MSCe and establishes the connection. Upon receipt of this message, the MSCe stops timer T_{3231} .

The diagram in Figure 3.2.2.6.1.2-2 shows an SUA connection refusal during handoff.

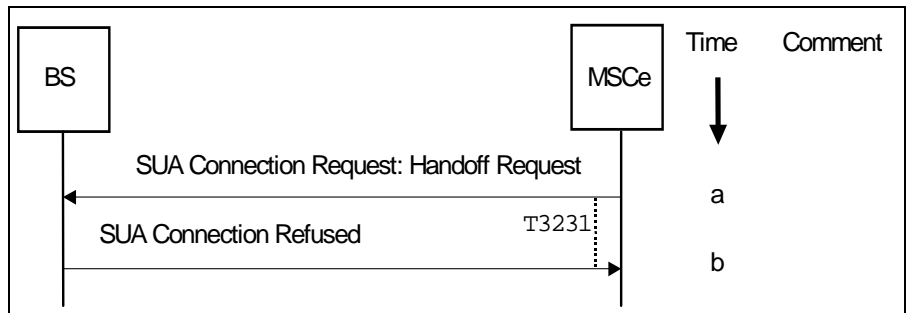


Figure 3.2.2.6.1.2-2 SUA Connection Refusal During Handoff

- a. The MSCe sends an SUA Connection Request message, including a user data field that contains a Handoff Request application message, to the BS. The MSCe starts timer T_{3231} .
- b. Upon receipt of the SUA Connection Request message, the BS sends an SUA Connection Refused message, which contains the Layer 3 Handoff Failure application message, to the MSCe. Upon receipt of this message, the MSCe stops timer T_{3231} .

3.2.2.6.2 Connection Release

This procedure is normally initiated at the MSCe side but in the case of abnormal SUA connection release (refer to section 3.2.2.6.3), the BS may initiate connection clearing.

The MSCe initiates this procedure with respect to the source BS in normal conditions for all calls supported by A1p connections.

1 A connection is released when a given signaling connection is no longer required. This
 2 may occur in normal cases:

- 3 • at the end of a transaction (call, location updating);
- 4 • after completion of a successful hard handoff: the connection with the source BS is
 5 released.

6 When either the MSCe or the BS sends an SUA Release Request (RELRE) message, the
 7 user data field is optional and may contain a transparent layer 3 message (e.g., DTAP) or
 8 be empty. The structure of the user data field, if any, is explained in [14].

9 When receiving this message, the BS releases or the MSCe initiates release of all the
 10 radio resources allocated to the relevant MS, if there are still any left, and returns an SUA
 11 Release Complete (RELCO) message.

12 For abnormal cases a connection failure may be detected by the connection supervision
 13 service provided by SUA. For other abnormal SUA connection releases, refer to section
 14 3.2.2.6.3, “Abnormal SUA Release”.

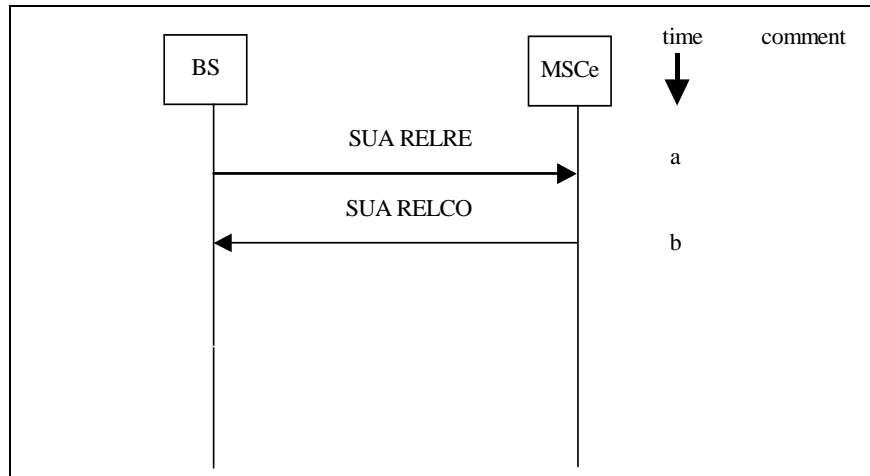
15 **3.2.2.6.3 Abnormal SUA Release**

16 The normal release of SUA A1p connections is initiated by the MSCe. Under abnormal
 17 conditions, an SUA connection may be released by the BS to clear resources.

18 Whenever an SUA connection is abnormally released, all resources associated with that
 19 connection shall be cleared. Abnormal release can result from, for example, resource
 20 failure, protocol error, or unexpected receipt of the SUA RELRE or SUA RELCO
 21 command.

22 **3.2.2.6.3.1 SUA Release by BS: Loss of SUA Connection Information**

23 Figure 3.2.2.6.3.1-1 demonstrates release of an SUA connection by the BS due to loss of
 24 SUA connection information.



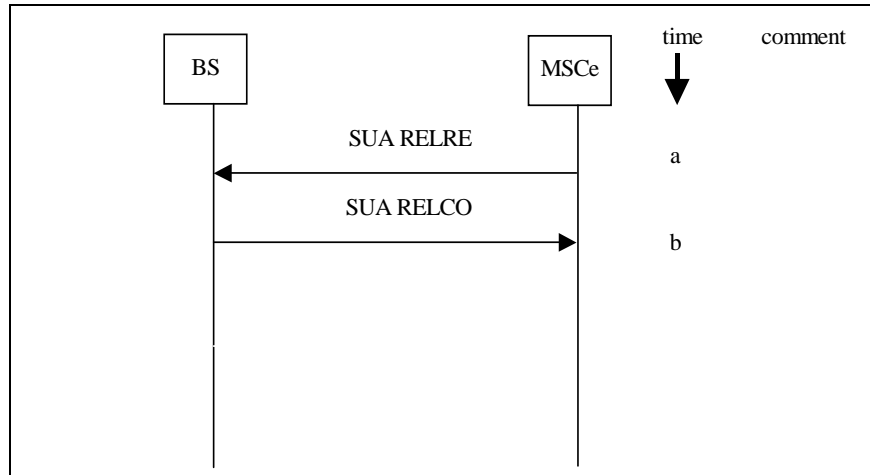
25 **Figure 3.2.2.6.3.1-1 BS Initiated SUA Release: BS Lost SUA Connection Information**

- 26 a. An unexpected SUA RELRE message (under abnormal termination) is received by
 27 the MSCe from the BS.
 28

- 1 b. The MSCe sends an SUA RELCO message to the BS to indicate that the SUA
 2 RELRE message has been received and that the appropriate procedures have been
 3 completed.

4 **3.2.2.6.3.2 SUA Release by MSCe: Loss of SUA Connection Information**

5 Figure 3.2.2.6.3.2-1 demonstrates release of an SUA connection by the MSCe due to loss
 6 of SUA connection information.



7
 8 **Figure 3.2.2.6.3.2-1 MSCe Initiated SUA Release: MSCe Lost SUA Connection Information**

- 9 a. An unexpected SUA RELRE message (under abnormal termination) is received by
 10 the BS from the MSCe.
 11 b. The BS sends an SUA RELCO message to the MSCe to indicate that the SUA
 12 RELRE message has been received and that the appropriate procedures have been
 13 completed.

14 **3.2.2.6.4 SUA Transfer of DTAP and BSMAP Messages**

15 The DTAP and BSMAP messages on the A1p interface are contained in the user data
 16 field of the exchanged SUA frames. Table 3.2.2.6.4-1 below summarizes the use of the
 17 User Data Field in SUA frames.

Table 3.2.2.6.4-1 Use of the User Data Field in SUA Frames

SUA Frame	User Data Field (BSMAP/DTAP)
Connection Oriented Protocol Class 2	
SUA Connection Request (CORE)	Optional
SUA Connection Acknowledge (COAK)	Optional
SUA Connection Refused (COREF)	Optional
SUA Release Request (RELRE)	Optional
SUA Release Complete (RELCO)	Not Applicable
SUA Connection Oriented Data Transfer (CODT)	Mandatory
Connectionless Protocol Class 0	
SUA Connectionless Data Transfer (CLDT)	Mandatory

For connection oriented transactions, a connection is requested, obtained or refused using the following SUA messages (protocol class 2):

- SUA Connection Request (CORE)
- SUA Connection Acknowledge (COAK)
- SUA Connection Refused (COREF)
- SUA Release Request (RELRE) and SUA Release Complete (RELCO) messages are used to break a connection.

The use of the User Data Field in SUA frames in the various establishment and release cases is described in section 3.2.2.6.1 and section 3.2.2.6.2.

For connection oriented (protocol class 2) transactions, once the signaling connection is confirmed between the MSCe and the BS, all A1p interface messages are transported in the SUA Connection Oriented Data Transfer (CODT) message until the connection is to be dropped.

For Connectionless (protocol class 0) transactions, where there is no SUA connection, A1p interface messages are transported in the SUA Connectionless Data Transfer (CLDT) message.

Table 3.2.2.6.4-2 below indicates which SUA messages shall be used to transport each of the application messages on the A1p interface.

Table 3.2.2.6.4-2 Use of SUA for BSMAP and DTAP Messages

Application Message	Message Discriminator	SUA Message
Call Processing Messages		
Bearer Update Request	BSMAP	CODT
Bearer Update Required	BSMAP	CODT
Bearer Update Response	BSMAP	CODT

Table 3.2.2.6.4-2 Use of SUA for BSMAP and DTAP Messages

Application Message	Message Discriminator	SUA Message
Complete Layer 3 Information	BSMAP	CORE ^a
CM Service Request	DTAP	CORE ^{a,b}
Event Notification	BSMAP	CLDT, COREF
Event Notification Ack	BSMAP	CLDT
Paging Request	BSMAP	CLDT ^a
Paging Response	DTAP	CORE ^{a,b}
CM Service Request Continuation	DTAP	CODT ^c
Connect	DTAP	CODT
Progress	DTAP	CODT
Service Release	DTAP	CODT
Service Release Complete	DTAP	CODT
Assignment Request	BSMAP	COAK ^d , CODT
Assignment Complete	BSMAP	CODT
Assignment Failure	BSMAP	CODT
Clear Request	BSMAP	CODT
Clear Command	BSMAP	CODT
Clear Complete	BSMAP	CODT
Alert With Information	DTAP	CODT
BS Service Request	BSMAP	CLDT
BS Service Response	BSMAP	CLDT
Additional Service Request	DTAP	CODT
Additional Service Notification	BSMAP	CODT
Supplementary Services Messages		
Flash with Information	DTAP	CODT
Flash with Information Ack	DTAP	CODT
Feature Notification	BSMAP	CLDT ^a
Feature Notification Ack	BSMAP	CLDT ^a
Priority Access Channel Assignment (PACA) Command	BSMAP	COAK ^d , CODT
PACA Command Ack	BSMAP	CODT
PACA Update	BSMAP	CLDT
PACA Update Ack	BSMAP	CLDT
Radio Measurements for Position Request	BSMAP	CODT
Radio Measurements for Position Response	BSMAP	CODT
Mobility Management Messages		

Table 3.2.2.6.4-2 Use of SUA for BSMAP and DTAP Messages

Application Message	Message Discriminator	SUA Message
Authentication Request	DTAP/BSMAP	CODT, CLDT ^c
Authentication Response	DTAP/BSMAP	CODT, CLDT ^c
SSD Update Request	DTAP	CODT
Base Station Challenge	DTAP	CODT
Base Station Challenge Response	DTAP	CODT
BS Authentication Request	BSMAP	CODT
BS Authentication Request Ack	BSMAP	CODT
Status Request	DTAP/BSMAP	CODT, CLDT ^c
Status Response	DTAP/BSMAP	CODT, CLDT ^c
SSD Update Response	DTAP	CODT
Location Updating Request	DTAP	CORE ^{a,b}
Location Updating Accept	DTAP	COREF
Location Updating Reject	DTAP	COREF
Mobile Station Registered Notification	BSMAP	CODT
Parameter Update Request	DTAP	CODT
Parameter Update Confirm	DTAP	CODT
Privacy Mode Command	BSMAP	CODT
Privacy Mode Complete	BSMAP	CODT
Registration Request	BSMAP	CLDT
User Zone Reject	DTAP/BSMAP	CODT, CLDT ^c
User Zone Update	DTAP	CODT
User Zone Update Request	DTAP	CODT
Handoff Messages		
Handoff Required	BSMAP	CODT
Handoff Request	BSMAP	CORE
Handoff Request Acknowledge	BSMAP	COAK
Handoff Failure	BSMAP	COREF ^f
Handoff Command	BSMAP	CODT
Handoff Required Reject	BSMAP	CODT
Handoff Commenced	BSMAP	CODT
Handoff Complete	BSMAP	CODT
Handoff Performed	BSMAP	CODT
Facilities Management Messages		
Reset	BSMAP	CLDT
Reset Acknowledge	BSMAP	CLDT
Service Redirection	DTAP	CODT, COREF

Table 3.2.2.6.4-2 Use of SUA for BSMAP and DTAP Messages

Application Message	Message Discriminator	SUA Message
Application Data Delivery Service (ADDS) Messages		
ADDS Page	BSMAP	CLDT
ADDS Transfer	BSMAP	CLDT
ADDS Deliver	DTAP	CODT
ADDS Page Ack	BSMAP	CLDT
ADDS Deliver Ack	DTAP	CODT
ADDS Transfer Ack	BSMAP	CLDT
Error Handling Messages		
Rejection	DTAP/BSMAP	CODT, CLDT ^e

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

- Following are the footnotes referred to in Table 3.2.2.6.4-2.
- a. Required, SUA CODT is not an option.
 - b. Sent within Complete Layer 3 Information, which is a BSMAP message.
 - c. This message may be used in addition to the CM Service Request.
 - d. May be used if responding to a CM Service Request or Paging Response.
 - e. Used only when the procedure is done on a paging channel.
 - f. May be used if responding to an SUA Connection Request/Handoff Request.

3.2.2.7 Base Station Application Part on A1p

The Base Station Application Part is specified in section 2.9.

3.2.2.8 Use of SCTP

The A1p interface shall use SCTP as specified in section 2.10.

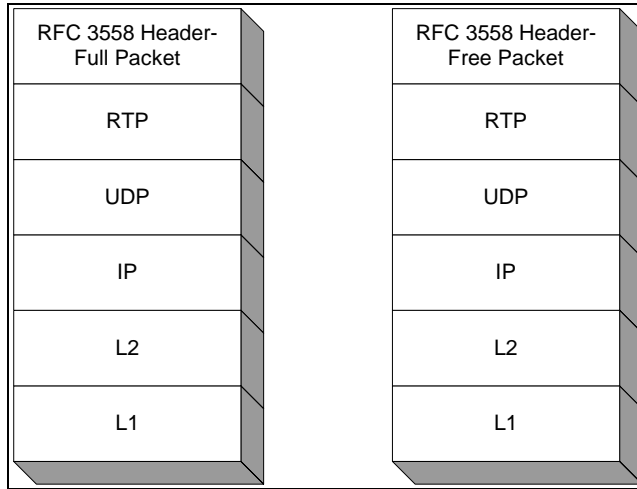
SCTP port value 14001 is used for SUA on the A1p interface.

3.2.3 A2p User Traffic Transport Protocol

The protocol stack options for transport of user traffic over A2p that are available to operators and manufacturers are shown in Figure 3.2.3-1 to Figure 3.2.3-7.

- a. Figure 3.2.3-1 is used for EVRC or SMV. Refer to [41].
- b. Figure 3.2.3-2 is used for PCM (G.711). Refer to [40].
- c. Figure 3.2.3-3 is used for 13k. Refer to [34].
- d. Figure 3.2.3-4 is used for DTMF. Refer to [36].
- e. Figure 3.2.3-5 is used for EVRC-B. Refer to [44].
- f. Figure 3.2.3-6 is used for EVRC-WB. Refer to [45].
- g. Figure 3.2.3-7 is used for EVRC-NW. Refer to [46].

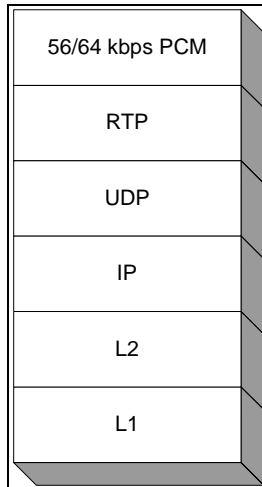
1



2

3

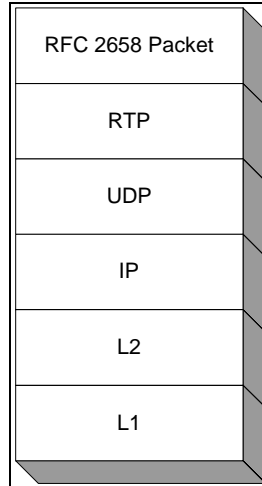
Figure 3.2.3-1 Protocol stack for EVRC and SMV



4

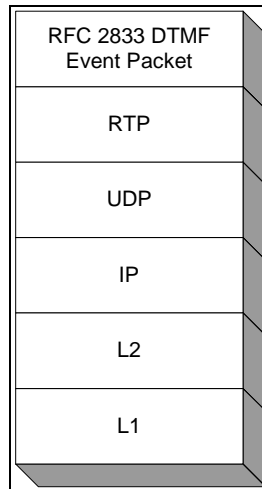
5

Figure 3.2.3-2 Protocol stack for PCM (G.711)



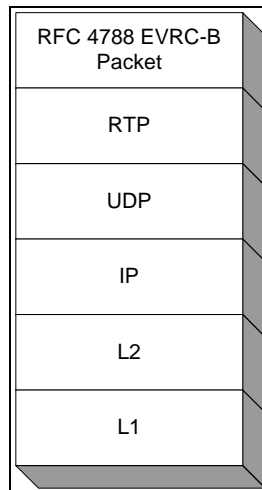
1
2

Figure 3.2.3-3 Protocol Stack for 13k



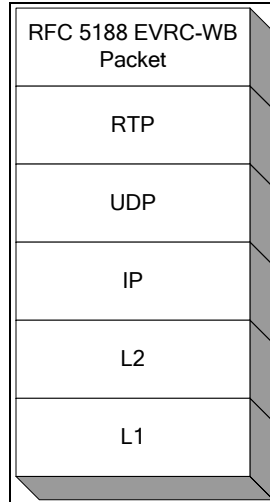
3
4

Figure 3.2.3-4 Protocol Stack for DTMF



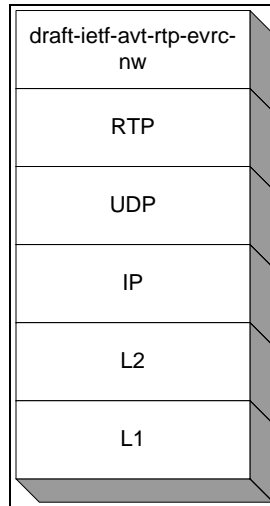
5
6

Figure 3.2.3-5 Protocol Stack for EVRC-B



1
2

Figure 3.2.3-6 Protocol Stack for EVRC-WB



3
4

Figure 3.2.3-7 Protocol Stack for EVRC-NW

- 5 **3.2.3.1 Physical Layer (L1) Specification for A2p**

- 6 The A2p interface shall use one of the L1 specifications in section 2.1.
- 7 **3.2.3.2 Layer 2 Specification for A2p**

- 8 The A2p L2 requirements as specified in section 2.2 may apply as per inter-vendor
- 9 agreements.
- 10 **3.2.3.3 Use of IP for A2p**

- 11 The requirements for 2.4.1 and 2.4.2 may apply as per inter-vendor agreements.
- 12 **3.2.3.4 QoS Specifications for A2p**

- 13 The A2p QoS requirements are for further study.

3.2.3.5 Security Specifications for A2p

The A2p Security Framework requirements are specified in section 2.4.5.

3.3 A3 and A7 Interfaces

Two protocol stacks are defined for the A3 and A7 signaling interface, and two protocol stacks are defined in this standard for the A3 user traffic interface.

As a mandatory requirement, the BS shall implement the ATM-based protocol stack. As an option, the IP-based protocol stack may be implemented at the BS.

3.3.1 Performance Specifications

The following parameters shall be specified by the required performance specifications on the A3/A7 interfaces:

- **ISD:** This is composed of the cumulative queuing, transmission, and propagation delays across the transport network between nodes supporting the A3/A7 interface. ISD is specified as a statistical variable (e.g. 99.9th percentile) allowing for delay variation (e.g. jitter). The delay budget for each hop in the transport network is not specified but rather each deployment or implementation should be engineered to meet the ISD using, for example, the link rate and technology at L1/L2.
- **ISL:** This is the packet loss across the transport network between nodes supporting the A3/A7 interface. ISL includes two components of packet loss in IP transport networks, queue overflow and errors on the transmission media. An implementation may choose to specify a packet loss rate that does not significantly impact the overall performance of the system while enabling a practical physical layer transmission network to be employed.

The performance of the A3/A7 interfaces has a significant impact on a subscriber's service quality. The RAN components supporting the fundamental channel (FCH), dedicated control channel (DCCH), and supplemental channel (SCH), on the A3/A7 interface shall conform to the delay budget requirements in Table 3.3.1-1.

The delay between the source BS and target BS (channel element) includes the ISD and network entity processing delays. The forward delay is the 99.9 percentile delay measured from the time the first bit of the frame is transmitted from the source BS to the time the first bit of the frame is transmitted over the air interface at the channel element for any soft handoff leg. The reverse delay is the 99.9 percentile delay measured from the time the last bit of the frame is received on the air interface at the channel element of any soft handoff leg to the time the last bit of the frame is received at the source BS.

Table 3.3.1-1 Delay Budget Requirements

Traffic type	IOS BSC-BTS	IOS BSC-BTS w/Turbo coding	A3 ISD
IS-95/IS-2000 FCH/DCCH forward	50 ms	N/A	10 ms
IS-95/IS-2000 FCH/DCCH reverse	60 ms	N/A	10 ms
IS-2000 SCH forward	55 ms	55 ms	15 ms

Traffic type	IOS BSC-BTS	IOS BSC-BTS w/Turbo coding	A3 ISD
IS-2000 SCH reverse	65 ms	75 ms	15 ms

1 **3.3.1.1 Performance Specification for IP Protocol Stacks**

2 If QoS is required (refer to section 2.4.4), the BSs on the A3/A7 interfaces shall employ
 3 Diffserv [33] marking for traffic as per the classes in Table 3.3.1.1-1. The transport
 4 network shall use this class information to meet the specified ISD and ISL on the
 5 particular interface, as given in Table 3.3.1.1-1.

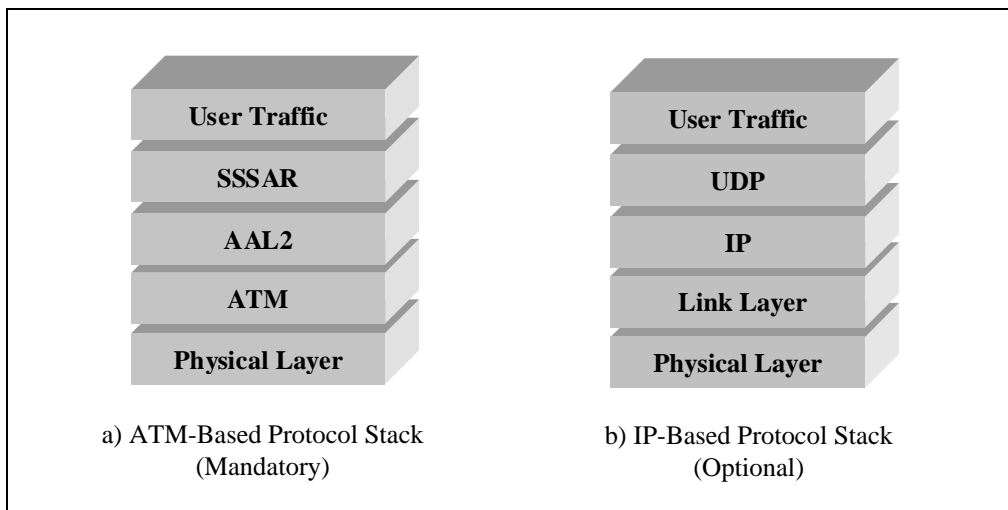
6
 7 **Table 3.3.1.1-1 A3/A7 Mapping Between Traffic Classes and Service-Level QoS**

Traffic Classes	Mandatory Traffic Types	Optional Traffic Types	99.9 %-tile Interface Service Delay (includes jitter)	Interface Service Packet Loss Rate
Class 1	FCH and DCCH frame protocols	Very low latency control and/or signaling messages	10 ms	1.e-5
Class 2	SCH frame protocol	Low latency control and/or signaling messages	15 ms	1.e-4
Class 3 ^a	None.	Normal signaling Messages	100 ms	1.e-4
Class 4 ^a	None.	OAM&P messages	2 sec	1.e-3

8 a. The ISD and ISL values for these classes are suggested values.

9 **3.3.2 A3 User Traffic Transport Requirements**

10 The protocol stack options for transport of user traffic that are available to operators and
 11 manufactures are shown in Figure 3.3.2-1.



12
 13 **Figure 3.3.2-1 A3 User Traffic Protocol Stack**

1	3.3.2.1	ATM-Based User Traffic Transport
2		The A3 user traffic interface, when implementing an ATM-based protocol stack, shall
3		contain the layers shown in a) of Figure 3.3.2-1.
4	3.3.2.1.1	Physical Layer (L1) Specification
5		The A3 user traffic interface shall use one of the L1 specifications in section 2.1.
6	3.3.2.1.2	Use of ATM
7		For this specification only ATM PVCs shall be required for the A3 user traffic interface.
8		These virtual circuits shall be configured through administrative procedures and no
9		special signaling interface procedures, e.g., ATM User Network Interface (UNI) [26],
10		shall be required.
11	3.3.2.1.3	Use of AAL2
12		When ATM is used to provide user traffic (voice/data) transport, the AAL2 protocol is
13		used. The procedures defined in [15] determine the allocation and use of the logical
14		channels, i.e., the connection identifiers (CIDs) that AAL2 provides over an ATM virtual
15		circuit.
16		Each BS has one or more ATM virtual circuits that connect it to other BSs (regardless of
17		whether switched or permanent virtual circuits are used). These virtual circuits are
18		comprised of one or more virtual circuits using AAL2 for the user traffic connections.
19	3.3.2.2	IP-Based User Traffic Transport
20		The A3 user traffic interface, when implementing an IP-based protocol stack, shall
21		contain the protocol layers shown in b) of Figure 3.3.2-1.
22		The requirements of this section shall apply to the transport layer for the A3 user traffic
23		frames.
24	3.3.2.2.1	Physical Layer (L1) Specification
25		The A3 user traffic interface shall use one of the L1 specifications in section 2.1.
26	3.3.2.2.2	Layer 2 Specification
27		The A3 user traffic L2 requirements as specified in section 2.2 shall apply for the
28		following areas:
29		• Bandwidth efficiency
30		• Delay/jitter control
31		• Multiplexing
32		• Compression
33		• Segmentation and re-assembly (SAR)
34		• Error detection
35		• Addressing

3.3.2.2.3 Use of IP

The following requirements are valid for the IP network, when it is used for A3 user traffic:

- The A3 bearer transport topology options are specified in section 2.4.1.
- The standard IP protocol, as defined in [28], shall be used for routing A3 user traffic.
- The A3 bearer transport network addressing shall support a class-less IP addressing scheme as specified in section 2.4.2.1.
- The A3 bearer transport network routing requirements are specified in section 2.4.2.2.
- The A3 bearer flow association guidelines are specified in section 2.4.2.3. Specific flow association requirements for A3 bearer frames are as follows:
 - Every unidirectional soft handoff leg (i.e., logical A3 bearer path between a Selector/Distribution Unit (SDU) frame selector and a BTS channel element) shall be addressed via an IP address and a UDP port number.
 - Unique IP addresses and UDP port numbers may be assigned in the forward and reverse directions.
 - The target side IP address and UDP port number pair shall uniquely identify a connection.

3.3.2.2.4 QoS Specifications

The A3 bearer QoS requirements are specified in sections 2.4.4 and 3.3.1.1.

The A3 bearer mapping between Traffic Classes and Service-Level QoS requirements are specified in Table 3.3.1.1-1.

3.3.2.2.5 Security Specifications

The A3 bearer Security Framework requirements are specified in section 2.4.5.

3.3.3 A3/A7 Signaling Transport Requirements

The two signaling protocol stack options that are available to operators and manufacturers for the A3 and A7 signaling interfaces include:

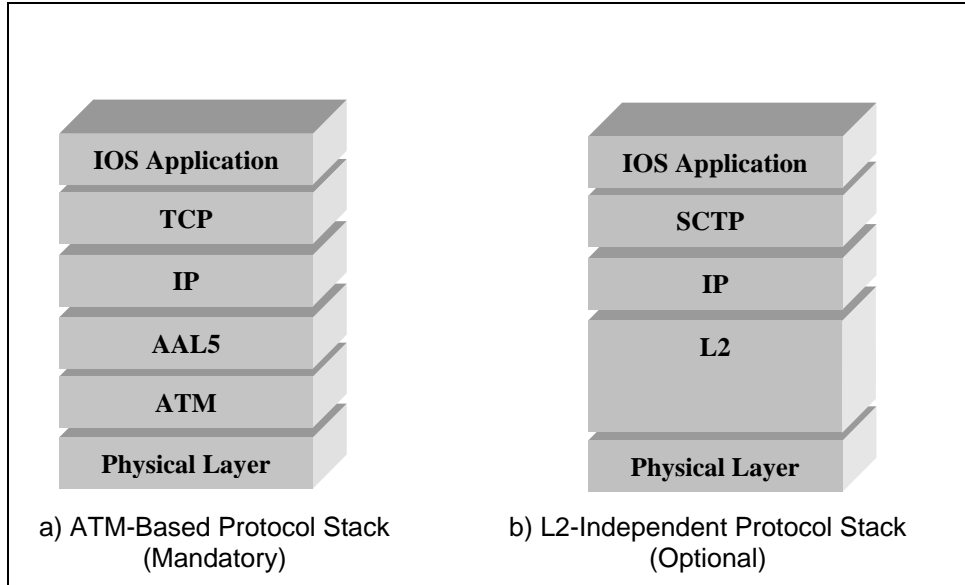


Figure 3.3.3-1 A3 and A7 Signaling Protocol Stack

3.3.3.1 ATM-Based Signaling Protocol Stack

The A3/A7 Signaling interfaces, when using an ATM-based protocol stack, shall contain the layers shown in a) of Figure 3.3.3-1.

3.3.3.1.1 Use of Physical Layer

The A3/A7 signaling interfaces shall use one of the specification defined in section 2.1.

3.3.3.1.2 Use of ATM

For this specification only ATM PVC shall be required for the A3 and A7 signaling interfaces. These virtual circuits shall be configured through administrative procedures and no special signaling interface procedures, e.g., ATM UNI [26], shall be required.

When ATM is used to provide signaling transport, the AAL5 protocol is employed.

Each BS has one or more ATM virtual circuits that connect it to other BSs (regardless of whether switched or permanent virtual circuits are used). These virtual circuits are comprised of one or more virtual circuits using the AAL5 protocol for signaling.

3.3.3.1.3 Use of AAL5

The AAL5 requirements are specified in section 2.3.1.

3.3.3.1.4 Use of IP

The IP requirements are specified in section 2.3.2.

3.3.3.1.5 Use of TCP

The standard TCP, as described in [29] and shown in section 2.5 shall be used on the A3 (signaling subchannel) and A7 interfaces.

All response messages associated with the handoff procedures shall be sent back to the same TCP connection where the first A3 or A7 message initiating the procedure is received. For example, the A3-Connect Ack (refer to [15]) message is sent back to the same TCP connection from which the A3-Connect message is received.

Any A3 or A7 signaling link disconnection during a handoff procedure may result in a failure of the handoff procedure. Optionally, a connection recovery may be performed for continuation of the handoff procedures. If a connection recovery is performed, the same active-passive TCP establishment procedure shall be used.

The following TCP port values are reserved for signaling across A7 interfaces:

- A7: (BS-to-BS) 5602 — This is the registered TCP port at a BS used for signaling interconnection to another BS.

3.3.3.2 IP-Based Signaling Protocol Stack

The A3/A7 Signaling interfaces, when implementing the L2-independent protocol stack, shall contain the layers shown in b) of Figure 3.3.3-1.

3.3.3.2.1 Use of Physical Layer

The A3/A7 signaling interface shall use one of the L1 specifications in section 2.1.

3.3.3.2.2 Layer 2 Specification

The A3/A7 signaling transport L2 requirements are specified in section 2.2 shall apply for the following areas:

- Bandwidth efficiency
- Delay/jitter control
- Multiplexing
- Compression
- Segmentation and re-assembly (SAR)
- Error detection
- Addressing

3.3.3.2.3 Use of IP

The following requirements are valid for the IP network, when used for A3/A7 signaling transport:

- The A3/A7 signaling transport topology options are described in section 2.4.1.
- The standard IP protocol, as defined in [28], shall be used for routing A3/A7 signaling.
- The A3/A7 signaling transport IP network shall support a class-less IP addressing scheme as specified in section 2.4.2.1.

- 1 • The A3/A7 signaling transport network routing requirements are specified in section
2 2.4.2.2.
- 3 • The A3/A7 signaling transport flow association guidelines are specified in section
4 2.4.2.3. Specific flow association requirements for A3/A7 signaling are as follows:
- 5 – Every logical signaling (i.e., BS) point defined in A3 or A7 interfaces that may
6 be a signaling source or target (e.g., BS source or target) shall be individually
7 addressable via an IP address and TCP or SCTP port number.
- 8 – When using the SCTP-based protocol, messages associated with individual
9 traffic connections shall contain unique SCTP stream identifiers.

10 3.3.3.2.4 QoS Specifications

11 The A3/A7 signaling transport QoS requirements are specified in sections 2.4.4 and
12 3.3.1.1.

13 The A3/A7 signaling transport mapping between Traffic Classes and Service-Level QoS
14 requirements are specified in Table 3.3.1.1-1.

15 3.3.3.2.5 Security Specifications

16 The A3/A7 signaling transport security Framework requirements are specified in section
17 2.4.5.

18 3.3.3.2.6 Use of SCTP

19 The L2-Independent Protocol Stack on the A3 and A7 signaling interface shall use SCTP
20 as specified in section 2.10.

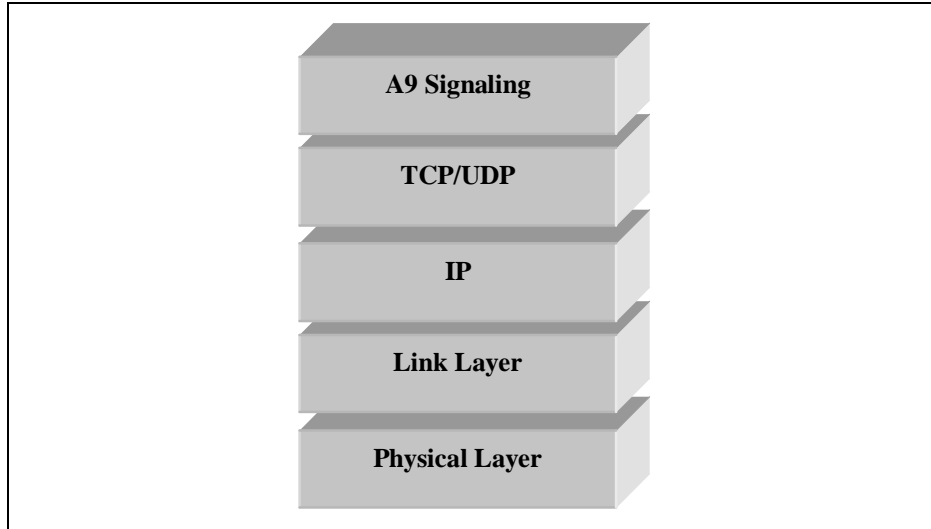
21 Between BSs (e.g., A3 and A7), one or several SCTP associations may exist. A BS may
22 select an SCTP association at creation of a user session context. However, it may not be
23 very efficient to consider each association as a signaling connection because typical
24 requirements of signaling application transport can be fulfilled by an SCTP stream pair.
25 Therefore, it should be assumed that one SCTP association is an aggregation of signaling
26 application connections. As such, each signaling application connection shall be mapped
27 to a pair of SCTP streams (one in downlink and one in uplink). The choice of stream
28 identifiers should be a function of the user application. One simple solution is to choose
29 the same stream identifier for each of the two streams comprising the connection.

30 SCTP port value 5604 is used for A7 signaling.

31 3.4 A8 and A9 Interfaces

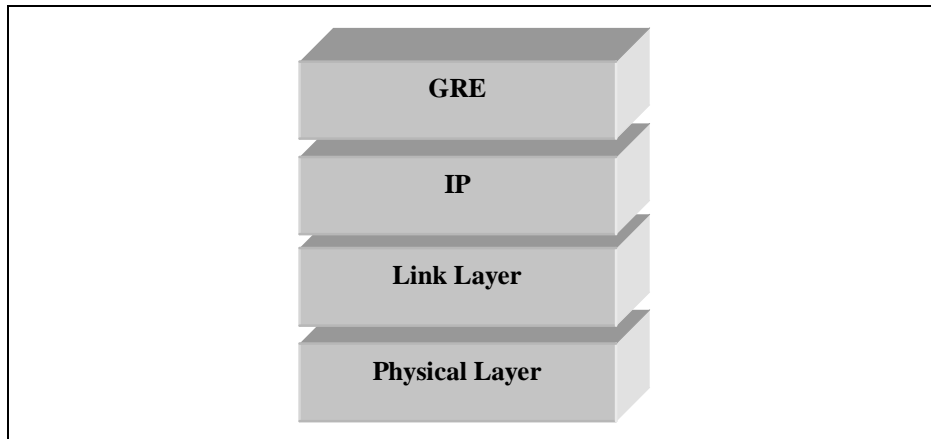
32 The A8 and A9 interfaces are based on the use of IP. IP can operate across various
33 physical layer media. The specific layer 1 media and layer 2 link protocols to be used for
34 these interfaces are not specified in this standard.

35 Signaling over the A9 interface requires a reliable transport protocol and appropriate
36 addressing and routing mechanisms to deliver messages from source to destination. The
37 signaling protocol stack option available to operators and manufacturers for the A9
38 interface is shown in Figure 3.4-1.



1
2 **Figure 3.4-1 A9 Signaling Protocol Stack**

3 The protocol stack options for transport of user traffic that are available to operators and
4 manufacturers are shown in Figure 3.4-2.



5
6 **Figure 3.4-2 A8 User Traffic Protocol Stack**

7 **3.4.1 Use of TCP**

8 When TCP is used for transferring the A9 interface messages, the standard TCP, as
9 described in [29] and shown in section 2.5, shall be used. The following TCP port value
10 is reserved for signaling across the A9 interface:

- 11 • A9: (BS-to-PCF) 5603 — This is the registered TCP/UDP port at a BS used for
12 signaling interconnection to a PCF.

13 **3.4.2 Use of UDP**

14 When UDP is used for transferring the A9 interface messages, the standard UDP, as
15 described in [27], shall be used.

1 UDP Port value '5603' is reserved for signaling use on the A9 interface. The initiator
2 (BS) of an A9 link picks an available source UDP port, and sends an A9-Setup-A8
3 message (refer to [16]) to the destination (PCF) at port 5603. The PCF responds with an
4 A9-Connect-A8 message to the UDP port of the BS that initiated the A9-Setup-A8
5 message (refer to [16]).

6 **3.4.3 Use of GRE**

7 For general use of GRE, refer to section 2.6.

8 The BS shall set the Key field in the GRE header to the value in the Key field in the A8
9 Traffic ID element in the A9-Connect-A8 message received from the PCF indicating that
10 the PCF accepts the A8 connection. The PCF shall set the Key field in the GRE header to
11 the value in the Key field in the A8 Traffic ID element in the A9-Setup-A8 message
12 received from the BS requesting the establishment of the A8 connection. Refer to [16] for
13 details on these A9 messages.

14 On the A8 interface, valid attributes (refer to section 2.6.1) that may be included in the
15 GRE frames when the Protocol Type field is set to "3GPP2 Packet" include:

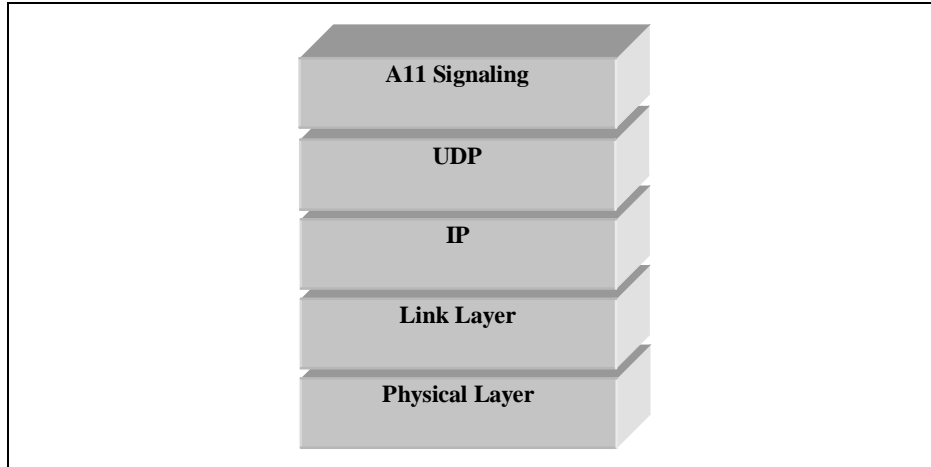
- 16 • IP Flow Discriminator (HRPD)
- 17 • Segmentation Indication

18 **3.5 A10 and A11 Interface**

19 The A10 and A11 interfaces are based on the use of IP. IP can operate across various
20 physical layer media. The specific layer 1 media and layer 2 link protocols to be used for
21 these interfaces are not specified in this standard.

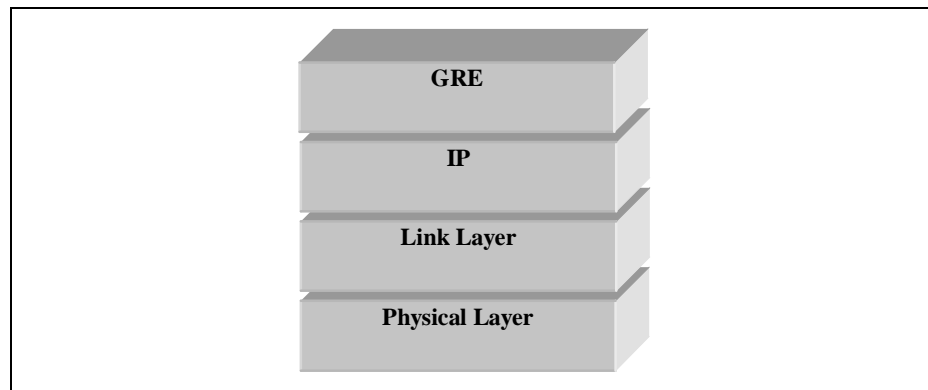
22 Mobile IP based messages are used for A11 interface call control signaling and for
23 passing accounting related and other information from the PCF to the PDSN (refer to [17]
24 for details). Each signaling exchange consists of a request message and a reply message.
25 When a message is sent by the PCF, the PCF's A11 IP address shall be used as the IP
26 Source Address and the PDSN's A11 IP shall be used as the IP Destination Address.
27 When a message is sent by the PDSN, the PDSN's A11 IP address shall be used as the IP
28 Source Address and the PCF's A11 IP address shall be used as the IP Destination
29 Address. Each message is transported within a UDP datagram. The initiator of the request
30 message shall pick an available UDP source port, and set the UDP destination port to 699
31 in the request message it sends to the selected receiver. In the reply message it sends to
32 the initiator, the receiver shall pick an available UDP source port (it can use the UDP
33 destination port in the request message) and set the UDP destination port to the UDP
34 source port in the request message.

35 Signaling over the A11 interface requires a reliable transport protocol and appropriate
36 addressing and routing mechanisms to deliver messages from source to destination. The
37 signaling protocol stack option available to operators and manufacturers for the A11
38 interface is shown in Figure 3.5-1.



1
2 **Figure 3.5-1 A11 Signaling Protocol Stack**

3 The protocol stack option for transport of user traffic that is available to operators and
4 manufacturers is shown in Figure 3.5-2.



5
6 **Figure 3.5-2 A10 User Traffic Protocol Stack**

7 **3.5.1 Use of UDP**

8 The use of UDP over the A11 interface conforms to the use of UDP for Mobile IP, as
9 specified in [31] with the exception of the UDP port number.

10 **3.5.2 Use of GRE**

11 For general use of GRE, refer to section 2.6.

12 The PCF shall set the Key field in the GRE header to the value in the Key field in the
13 Session Specific Extension in the A11-Registration Reply message received from the
14 PDSN indicating that the PDSN accepts the A10 connection. The PDSN shall set the Key
15 field in the GRE header to the value in the Key field in the Session Specific Extension in
16 the A11-Registration Request message received from the PCF requesting the
17 establishment of the A10 connection. Refer to [17] for details on these A11 messages.

1
2
3
4
5
6
7
8

On the A10 interface, valid attributes (refer to section 2.6.1) that may be included in the GRE frames when the Protocol Type field is set to “3GPP2 Packet” include:

- Short Data Indicator
- Flow Control Indication
- IP Flow Discriminator (HRPD)
- Segmentation Indication