3GPP2 A.S0012-B

Version 1.0

Date: April 2004

3rd Generation Partnership Project 2
"3GPP2"

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

(3G-IOSv4.3.1)

Table of Contents

List of Figures

List of Tables

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

1.2.1 TIA / EIA

For ease of cross-referencing, the Telecommunications Industry Association (TIA) / Electronics Industry Association (EIA) references provided in this section are aligned with the Third Generation Partnership Project 2 (3GPP2) references, provided in section 1.2.2.

[1~7] Reserved.
[8] TIA/EIA/IS-835-A, *cdma2000 Wireless IP Network Standard*, May 2001.
[9] Reserved.
[10] Reserved.
[11] TIA-2001.1-C-1, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 1 Overview*, December 2003.
[12] Reserved.
[13] TIA-2001.3-C-1, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 3 Features*, December 2003.
[14] TIA-2001.4-C-1, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 4 (A1, A2, and A5 Interfaces)*, December 2003.
[15] TIA-2001.5-C-1, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 5 (A3 and A7 Interfaces)*, December 2003.
[16] TIA-2001.6-C-1, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 6 (A8 and A9 Interfaces)*, December 2003.

[17] TIA-2001.7-C-1, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 7 (A10 and A11 Interfaces)*, December 2003.
[18] TIA-923, *Link-Layer Assisted Service Options for Voice-over-IP: Header Removal (SO60) and Robust Header Compression (SO61)*, May 2003.
[19] TIA-728, *Intersystem Link Protocol (ISLP)*, January 1, 2002.

1.2.2 3GPP2

The 3GPP2 references are aligned with the TIA/EIA references of section 1.2.1 and are provided here for information and cross reference purposes.

[1~7] Reserved.
[8] 3GPP2 X.S0011-C, *Wireless IP Network Standard*, six parts, September 2003.
[9] Reserved.
[10] Reserved.
[11] 3GPP2 A.S0011-B, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 1 Overview*, April 2004.
[12] Reserved.
[13] 3GPP2 A.S0013-B, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 3 Features*, April 2004.
[14] 3GPP2 A.S0014-B, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 4 (A1, A2, and A5 Interfaces)*, April 2004.
[15] 3GPP2 A.S0015-B, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 5 (A3 and A7 Interfaces)*, April 2004.
[16] 3GPP2 A.S0016-B, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 6 (A8 and A9 Interfaces)*, April 2004.
[17] 3GPP2 A.S0017-B, *Interoperability Specification (IOS) for cdma2000 Access Network Interfaces – Part 7 (A10 and A11 Interfaces)*, April 2004.
[18] 3GPP2 C.S0047-0, Version 1.0, *Link-Layer Assisted Service Options for Voice-over-IP: Header Removal (SO60) and Robust Header Compression (SO61)*, April 14, 2003.
[19] 3GPP2 N.S0019, *Intersystem Link Protocol*, January 28, 2000

1.2.3 Standards Committee T1

[20] ANSI T1.101-1987, *Synchronization Interface Standards for Digital Networks*, 1987.
[21] ANSI T1.102-1987, *Digital Hierarchy – Electrical Characteristics*, 1987.
[22] ANSI T1.107-1988, *Digital Hierarchy – Formats Specifications*, 1988.
[23] ANSI T1.111-1992, *Signaling System No. 7 (SS7) - Message Transfer Part (MTP)*, June 1992.
[24] ANSI T1.112-1992, *Signaling System No. 7 (SS7) - Signaling Connection Control Part (SCCP)*, October 1992.
[25] ANSI T1.403-1995, *Network to Customer Installation – DS1 Metallic Interface*, 1995.
[26] ANSI T1.627 - 1993, *B-ISDN - ATM Layer Functionality and Specification*, 1993.
[27] ANSI T1.635 – 1995, *Broadband ISDN –Physical Layer Specification for User-Network-Interface Including DS1/ATM*, 1995.
[28] ANSI T1.105 – 1995, *Synchronous Optical Network (SONET) Basic Description Including Multiplex Structure, Rates and Formats*, 1995.

1.2.4 International Telecommunications Union - Telecommunications Sector (ITU-T)

[29] ITU-T Recommendation G.707, *Network Node Interface for the Synchronous Digital Hierarchy (SDH)*, 1996.

[30] ITU-T Recommendation I.366.1, *Segmentation and Reassembly Service Specific Convergence Sublayer for the AAL type 2*, June 1998.

[31] ITU-T Recommendation Q.2931, *Broadband-Integrated Services Digital Network (B-ISDN) Digital Subscriber Signaling No. 2 (DSS2) User-Network Interface Layer 3 Specification for Basic Call/Connection Control*, 1995.

1.2.5 Other

[32] Internet Engineering Task Force, *RFC 768 – User Datagram Protocol (UDP)*, 1980.

[33] Internet Engineering Task Force, *RFC 791 – Internet Protocol (IP)*, 1981.

[34] Internet Engineering Task Force, *RFC 793 – Transmission Control Protocol (TCP)*, 1981.

[35] Internet Engineering Task Force, *RFC 1483 – Multiprotocol Encapsulation over ATM Adaptation Layer 5*, 1993.

[36] Internet Engineering Task Force, *RFC 2002 – IP Mobility Support Specification*, 1996.

[37] Internet Engineering Task Force, *RFC 2225 – Classical IP and ARP over ATM*, 1998.

[38] Internet Engineering Task Force, *RFC 2475, An Architecture for Differentiated Services*, December 1998.

[39] Internet Engineering Task Force, *RFC 2784 - Generic Routing Encapsulation (GRE)*, 2000.

[40] Internet Engineering Task Force, *RFC 2890 - Key and Sequence Number Extensions to GRE*, September 2000.

[41] Internet Engineering Task Force, *RFC 2960, Stream Control Transmission Protocol*, October 2000.

1.3 Terminology

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
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
CIC	Circuit Identity Code
CM	Connection Management
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
IMSI	International Mobile Subscriber Identity

Acronym	**Meaning**
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
L1	Layer 1 (Physical Layer)
L2	Layer 2 (Link Layer)
L3	Layer 3 (Network Layer)
LLC	Logical Link Control
LSB	Least Significant Bit
Mbps	Million Bits per Second
MS	Mobile Station
MSB	Most Significant Bit
MSC	Mobile Switching Center
Msg	Message
MTP	Message Transfer Part
OAMP	Operation Administration Maintenance 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
RFC	Request For Comment
RLC	Release Complete (SCCP)
RLSD	Release (SCCP)
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

Acronym	**Meaning**
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
T1	T1-type Digital Carrier
T3	T3-type Digital Carrier
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
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

1.3.2 Definitions

Refer to [11].

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.

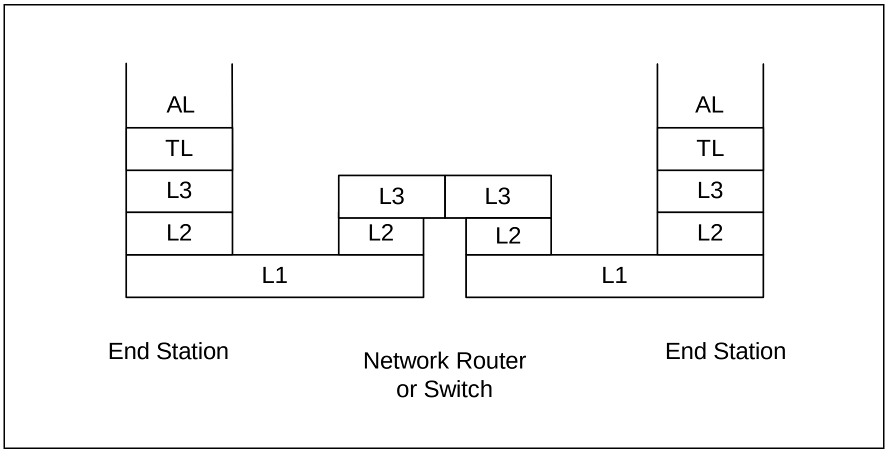

Figure 2-1 Transport Network Reference Model

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. This type of interfaces can be full-duplex or half-duplex when it is used as a clear channel.
- E1 digital transmission interfaces consisting of 30*64 kbps user channels 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.
- Synchronous Transfer Mode 1 (STM1) [29] digital transmission interfaces supporting transmission rates of 155.52 Mbps.

Asynchronous layer 1 protocols (e.g. 10/100BaseT) 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 [26] 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 [29], 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 [37]. Specification of either Logical Link Control (LLC) and Sub Network Attachment Point encapsulation or Virtual Channel (VC) multiplexing as per [35] is left to the discretion of operators and manufacturers.

2.4 IP Transport Considerations

The standard IP protocol, as defined in [33], 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 translation and other functions specific to the type of network they are connected to. There is no restriction on the number or types of topologies or devices that can be used to implement this RAN transport network.

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

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

2.4.2.1 Addressing

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

2.4.2.2 Routing

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

2.4.2.3 Flow Association

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

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

2.4.3 IP Performance Specifications

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

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

2.4.4 IP Quality of Service (QoS) Framework

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

Differentiated Services (DiffServ) framework as specified in [38], with the following clarifications:

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

2.4.5 IP Security Framework Specifications

The IOS RAN is realized as a managed network. In this network, it is assumed that all interfaces are physically secured as a minimum. For security measures specific to particular IOS interfaces, refer to [13]. Any additional security measures are beyond the scope of this standard.

2.5 Use of TCP

The standard TCP protocol, as described in [34], shall be used for establishing, using, and clearing TCP connections.

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

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

2.5.1 Message Delimiting in TCP

TCP provides a reliable byte stream between two application entities. Because the protocol in this standard uses messages to communicate, these messages shall be delimited in the TCP byte stream. Such delimitation shall be done by means of a two byte flag field and a two byte length field inserted at the beginning of each message sent over a TCP connection. The flag field shall contain the hex value "F634". The purpose of the flag field is to facilitate verification of message boundaries and to speed up reestablishment of synchronization if synchronization of message boundaries is lost. Refer to Figure 2.5.1-1.

	7	6	5	4	3	2	1	0
Flag	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**0**
Flag	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**0**
Length	(MSB)							
Length								(LSB)
Msg	First Octet of IOS Application Message							
	Second Octet of IOS Application Message							
	Third Octet of IOS Application Message							
	…							
	Last Octet of IOS Application Message							
Flag	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**0**
Flag	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**0**
Length	(MSB)							
Length								(LSB)
Msg	First Octet of IOS Application Message							
	Second Octet of IOS Application Message							
	Third Octet of IOS Application Message							
	…							
	Last Octet of IOS Application Message							
Flag	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**0**
Flag	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**0**
Length	(MSB)							
Length								(LSB)
Msg	First Octet of IOS Application Message							
	Second Octet of IOS Application Message							
	Third Octet of IOS Application Message							
	…							

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

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 [39] and extended in [35].

The A10 connection and A8 connection 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. 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 which A10 connection a particular payload packet belongs to.

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

When the PDSN SID is unique within the PDSN, the PDSN can use it to identify which A10 connection the packet belongs to. 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 which A8 connection a particular payload packet belongs to.

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 which A8 connection a particular payload packet belongs to.

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

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

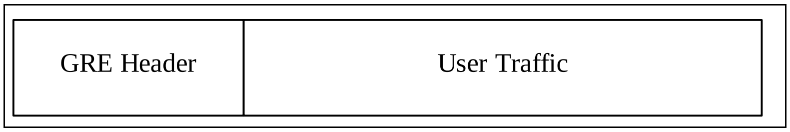

Figure 2.6-1 GRE Encapsulated User Traffic

Figure 2.6-2 shows the structure of the GRE header.

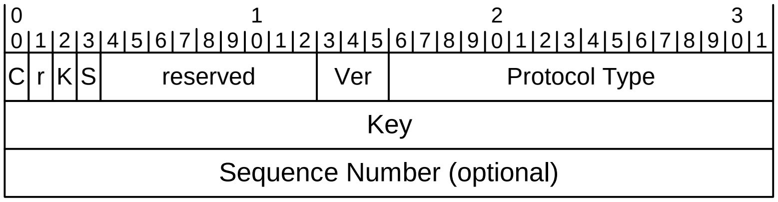

Figure 2.6-2 GRE Header

The GRE header shall be encoded as follows:

C (Checksum Present)	‘0’
r (reserved)	‘0’
K (Key Present)	‘1’
S (Sequence Number Present)	‘0 or 1’
reserved	‘000000000’
Ver (Version Number)	‘000’
Protocol Type	Hex ‘88 81’ for Unstructured Byte Stream.

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

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

If the link layer/network layer protocol requires that the GRE packets be delivered in sequence (e.g. if a state-full compression mechanism is in use) over the connection, the S indicator shall be set to ‘1’ and the sequence number field shall be included in each GRE packet sent over the connection. The sequence number field is used by the BS and PDSN to deliver the GRE packets to the destination entity in sequence (e.g. over-the-air to the MS, from the GRE to PPP layer in the PDSN). When the sequence number field is included, the sender and receiver shall perform the following:

- The sequence numbers shall be set to zero after the connection is established.
- The sequence number shall be incremented according to [40] in each subsequent packet sent on the same connection
- Receipt of an out-of-sequence packet on a connection shall be handled according to [40].

2.6.1 Relationship of GRE tunnel to Quality of Service

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

To support QoS on the A8/A9 and A10/A11 interfaces, the RAN shall have a local RAN transport network QoS policy which indicates which outer DSCP values can be used by the PDSN, PCF and BS for traffic. These DSCP values shall be made available to the PDSN (e.g. via O&M functions) to enable QoS for the RAN transport network.

When QoS is required for GRE tunnels across the A8/A9/A10/A11 transport network, the IOS shall implement Diffserv as described in section 2.4.4 to support intra-network QoS requirements. In addition, the BS, PCF and PDSN shall follow specific mapping rules as follows:

1. The PDSN shall mark packets in the GRE tunnel (outer DSCP value) according to the policy in use by the RAN transport network (refer to section 24.4) connecting the PDSN to the PCF. This policy is local and specifies the DSCP values for use on each GRE tunnel (i.e. service instance) instantiated on the PDSN.
2. The PCF and BS shall use the local QoS policy (refer to section 2.4.4) to set the outer DSCP value of the packets in the GRE tunnels (i.e. service instance). Since the PCF and BS are not required to inspect the encapsulated IP packets to derive the inner DSCP value, the PCF and BS may mark all GRE packets in the same service instance (SI) with the same DSCP value. The PCF and BS may also set the DSCP value of all GRE packets associated with the same user to the same value if this is the local policy.
3. The BS may use the outer DSCP value for RAN QoS functions (e.g. RLP frame prioritization). However, the BS is not required to differentiate between packets in the same SI or between users.

2.6.2 GRE Protocol Usage for VoIP SOs

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

(This page intentionally left blank.)

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

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 section 2.1.

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 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 Base Station Application Part

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

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

Refer to Figure 3.1.1-1 “A1 Interface Signaling Protocol Reference Model” for an illustration of this structure.

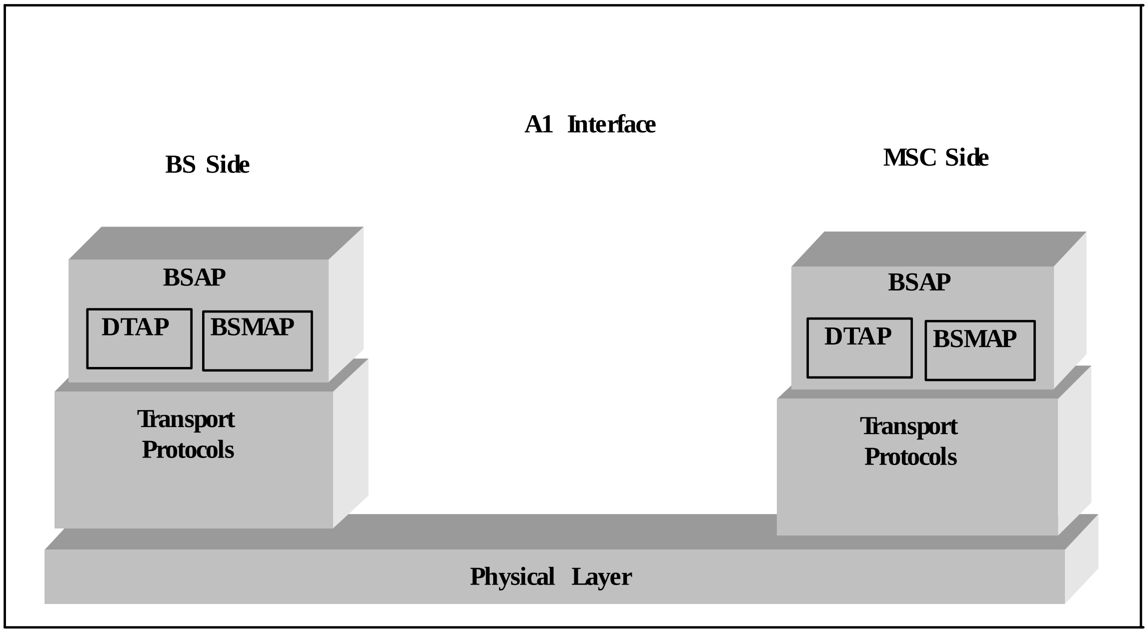

Figure 3.1.1-1 A1 Interface Signaling Protocol Reference Model

3.1.1.1 The BS Management Application Part

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

The A1 messages that are considered BSMAP are listed in Table 3.1.4.4.5-2 and specified in [14].

3.1.1.2 The Direct Transfer Application Part

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

The A1 messages that are considered DTAP are listed in Table 3.1.4.4.5-2 and specified in [14].

3.1.2 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 3.1.2-1.

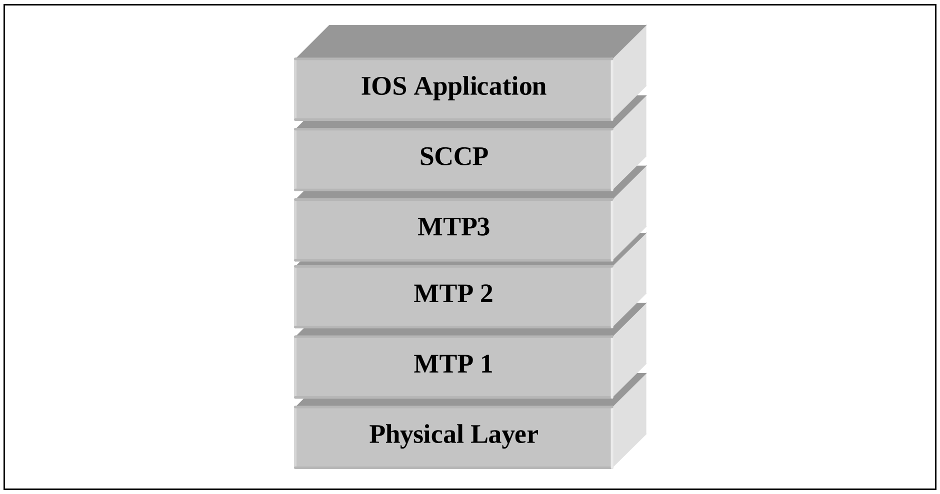

Figure 3.1.2-1 A1 Signaling Protocol Stack

3.1.3 User Traffic Connection Transport Protocol Options

The protocol stack options for transport of user traffic that are available to operators and manufacturers are shown in Figure 3.1.3-1 and Figure 3.1.3-2. The link layer for the A5 interface uses the Intersystem Link Protocol (ISLP) [19].

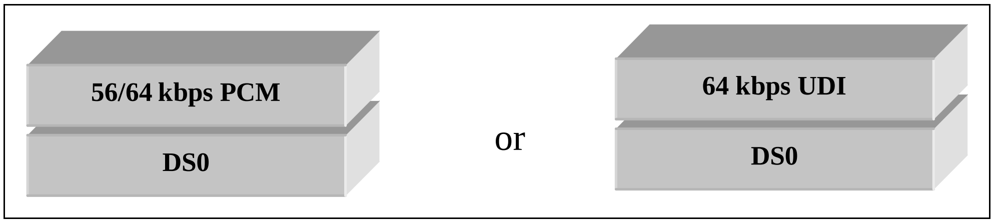

Figure 3.1.3-1 A2 User Traffic Protocol Stacks

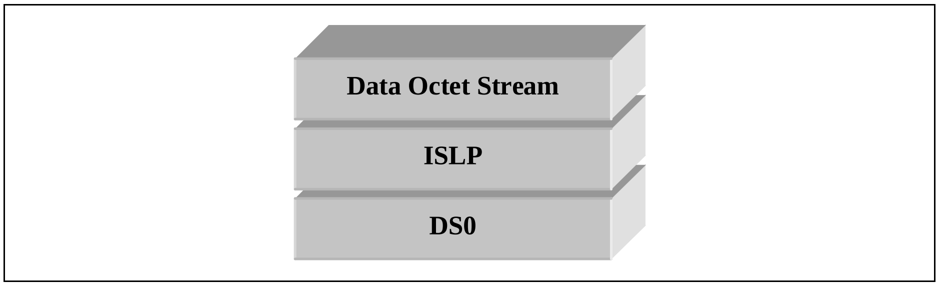

Figure 3.1.3-2 A5 User Traffic Protocol Stacks

3.1.4 Use of ANSI SS7 Transport (Layer 2)

This standard specifies multiple protocols for the transport of signaling and user information. Refer to sections 3.1.2 and 3.1.3.

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

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

Information for this section was excerpted from [23] and [24]. Section 3.1.4.2 deals with the MTP. Section 3.1.4.3 deals with SCCP and its use.

The MTP provides a mechanism giving reliable transfer of signaling messages. Section 3.1.4.2 deals with the subset of the MTP that can be used between a BS and a MSC, which is compatible with a full MTP.

SCCP is used to provide a referencing mechanism to identify a particular transaction relating to, for instance, a particular call. Section 3.1.4.3 identifies the SCCP subset that shall be used between a BS and an MSC. SCCP can also be used to enhance the message routing for operations and maintenance information.

3.1.4.1 Field of Application

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

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

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

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

3.1.4.2 Message Transfer Part

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

3.1.4.2.1 General

The MTP functions as specified in [23] are applicable. However, the following exceptions and modifications to those recommendations may be applied for the MSC to BS signaling. Refer to section 3.1.4.2.2 through section 3.1.4.2.4.

3.1.4.2.2 Level 1 (Chapter 2 of [23])

Chapter 2, Figure 2

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

Chapter 2, Section 1.4 Analog Signaling Link

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

Chapter 2, Section 2 General

A signaling rate of 56/64 kbps is assumed.

Chapter 2, Section 3 Error Characteristics and Availability

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

Chapter 2, Section 5 Digital Signaling Link

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

Chapter 2, Section 6 Analog Signaling Data Link

Only digital signaling data links are supported.

3.1.4.2.3 Level 2 (Chapter 3 of [23])

Chapter 3, Section 1.4 Signal Unit Error Correction

Only the basic error correction protocol is required.

Chapter 3, Section 7 Signaling Link Initial Alignment Procedure

In the initial alignment procedure specified in Chapter 3 of [23], only the emergency proving period is applicable for the BS. Thus, in states 02 and 03 of the initial alignment procedure status indication “N” is not sent from the BS. The BS should be capable of recognizing status indication “N” if received in order for the alignment procedure to complete.

3.1.4.2.4 Level 3 (Chapter 4 of [23])

Chapter 4, Section 1.1.2 End Point of a Signaling Link

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

Chapter 4, Section 2

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

Chapter 4, Section 2.2 Routing Label

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

Chapter 4, Section 2.3 Message Routing Function

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

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

The procedures for handling message congestion priority levels as defined for U. S. Signaling Networks in Chapter 4, section 2.3.5.2 of [23] shall be followed. The message priorities given in Appendix B (of Chapter 5 of [23]) for SCCP and MTP messages shall be used. The remaining message priorities for BSMAP and DTAP messages are provided in [14].

Chapter 4, Section 2.4 Message Discrimination

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

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

Chapter 4, Section 3 Signaling Network Management

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

Chapter 4, Section 3.8 Signaling Network Congestion

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

Chapter 4, Section 4 Signaling Traffic Management

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

Chapter 4, Section 4.2

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

Chapter 4, Section 4.3.3

There is no alternative link set.

Chapter 4, Section 5 Changeover

Changeover between link sets is not applicable.

Chapter 4, Section 6 Change back

Change back between link sets is not applicable.

Chapter 4, Section 7 Forced Rerouting

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

Chapter 4, Section 8 Controlled Rerouting

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

Chapter 4, Section 9 MTP Restart

The MTP Restart procedure is not required.

Chapter 4, Section 11 Signaling Traffic Flow Control

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

Chapter 4, Section 12 Signaling Link Management

Only basic link management procedures are applicable.

Chapter 4, Section 13 Signaling Link Management

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

Chapter 4, Section 14.2.1

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

Chapter 4, Section 14.2.2

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

Chapter 4, Section 15

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

3.1.4.2.5 Testing and Maintenance (Chapter 7 of [23])

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.

3.1.4.2.6 Interface Functions

The method of interfacing to the higher layers is by the primitives defined in Chapter 1 of [23].

The primitives defined are:

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

3.1.4.2.7 Overload Control (Message Throughput Congestion)

MTP overload control is not required.

3.1.4.3 SCCP Transport Layer Specification (SCCP Functions)

3.1.4.3.1 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.

- Chapters 1 through 4 of [24] are considered as the basis for elaboration of this document.

3.1.4.3.2 Primitives (Chapter 1 of [24])

Chapter 1, Table 1

Two primitives of the table are not used:

N-INFORM DATA
N-RESET

Chapter 1, Table 2

The following parameters of the N-CONNECT primitive are not used:

Responding address
Receipt confirmation selection
Expedited data selection

Chapter 1, Table 3

The following parameter of the N-DATA primitive is not used:

Confirmation request

Chapter 1, Table 6

The following parameter of the N-DISCONNECT primitive is not used:

Responding address

Chapter 1, Section 2.1.2

Permanent signaling connections are not applicable.

Chapter 1, Table 8

The primitive N-NOTICE is not used.

Chapter 1, Table 8A

The following parameter of the N-UNITDATA primitive is not used:

Return option

Chapter 1, Section 4.1.2

Functions for permanent signaling connections are not applicable.

3.1.4.3.3 SCCP Messages (Chapter 2 of [24])

Chapter 2, Section 2.4

The Data Acknowledgment message is not used.

Chapter 2, Section 2.6

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

Chapter 2, Section 2.7

The Expedited Data message is not used.

Chapter 2, Section 2.8

The Expedited Data Acknowledgment message is not used.

Chapter 2, Section 2.10

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

Chapter 2, Section 2.13

The Reset Confirm message is not used.

Chapter 2, Section 2.14

The Reset Request message is not used.

Chapter 2, Section 3.5

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

Chapter 2, Section 3.4

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

Chapter 2, Section 2.16

The Unit Data Service message is not used.

Chapter 2, Section 4.2

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

Chapter 2, Section 4.6

The “error cause” parameter field is not used.

Chapter 2, Section 4.10

The “receive sequence number” parameter is not used.

Chapter 2, Section 4.13

The “reset cause” parameter field shall not be used.

Chapter 2, Section 4.16

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

3.1.4.3.4 SCCP Formats and Codes (Chapter 3 of [24])

Chapter 3, Section 3.4

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

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

Chapter 3, Section 3.4.2.2

SSN Values: BSAP = 11111100, (252)

Use of alternative values is an administrative concern.

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

Chapter 3, Section 3.4.2.3

Global title: refer to Chapter 3, section 3.4 of [24].

Chapter 3, Section 3.6

Protocol Class: the classes 1 and 3 are not used.

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

Parameters are not used.

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

Messages are not used.

Chapter 3, Section 5.1.1

SOR and SOG are not needed.

3.1.4.3.5 SCCP Procedures (Chapter 4 of [24])

Chapter 4, Sections 1.1.2.2, 1.1.2.4

Protocol classes 1 and 3 are not used.

Chapter 4, Section 1.1.3

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

The use of multiple connections sections is an administrative concern.

Chapter 4, Section 1.2.1 (b)

Not applicable for single connections.

Chapter 4, Section 2.1 (1.)

Global title not used for single connections.

Chapter 4, Section 2.2.1

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

Chapter 4, Section 2.2.2

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

Chapter 4, Section 2.2.2.2

No SCCP translation function is required for single connections.

Chapter 4, Section 2.3.1 (3)

Not applicable for single connections.

Chapter 4, Section 2.3.2 (4)

Not applicable for single connections.

Chapter 4, Section 3.1.3

Not applicable: no protocol class and flow control negotiations.

Chapter 4, Section 3.1.5

Not applicable.

Chapter 4, Section 3.2.2

Not applicable.

Chapter 4, Section 3.3.4

Not applicable.

Chapter 4, Section 3.5.1.2

Not applicable.

Chapter 4, Section 3.5.2

Not applicable.

Chapter 4, Sections 3.6, 3.7, 3.9, 3.10

Not applicable.

Chapter 4, Section 4.2

Message return is not applicable.

Chapter 4, Section 5

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

3.1.4.4 Use of the SCCP

The SCCP is used to support signaling messages between the MSC and the BS. BSAP (refer to section 3.1.1) uses one SCCP signaling connection for the transfer of layer 3 (A1) messages per MS.

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

3.1.4.4.1 Connection Establishment

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

Two connection establishment cases are distinguished:

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

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

3.1.4.4.1.1 Establishment Procedure - Case 1

In this case, the connection establishment is initiated at the reception by the BS of the first layer 3 message from the MS. Generally, such a message contains the Mobile Identity parameter (Electronic Serial Number (ESN), or International Mobile Subscriber Identity (IMSI)). The BS then constructs the first A1 interface BSMAP message (Complete Layer 3 Information), which includes one of the appropriate DTAP messages (Location Updating Request, Connection Management (CM) Service Request, or Paging Response) depending on whether the MS is accessing the network for the purpose of registration, call origination, or termination. The Complete Layer 3 Information message is sent to the MSC in the user data field of the SCCP Connection Request message (refer to [14]). The Complete Layer 3 Information message includes the cell identity and the layer 3 message that was received from the MS. The exact coding of the BSMAP message is specified in [14].

Upon the reception of the SCCP Connection Request message, the MSC may check, based on the received identity, whether another association already exists for the same MS. If this is the case, the connection establishment is refused. Otherwise, an SCCP Connection Confirm message is sent back to the BS. This message may optionally contain a BSMAP or DTAP message in the user data field.

The diagram in Figure 3.1.4.4.1.1-1 shows a successful SCCP connection establishment procedure.

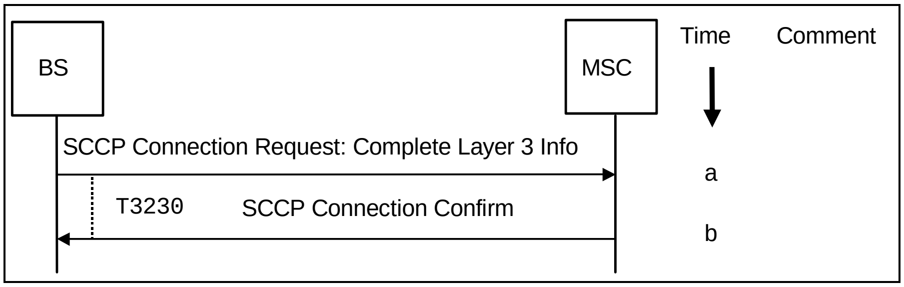

Figure 3.1.4.4.1.1-1 SCCP Connection Establishment

a. The BS sends an SCCP Connection Request message, including a user data field, to the MSC. The BS starts timer T_{3230}. Refer to [14] for the T_{3230} timer definition.

b. Upon receipt of the SCCP Connection Request message, the MSC sends an SCCP Connection Confirm message, which may contain a Layer 3 application message, to the BS. Upon receipt of this message, the BS stops timer T_{3230} and establishes the connection.

The procedures in case of connection establishment refusal are shown in Figure 3.1.4.4.1.1-2.

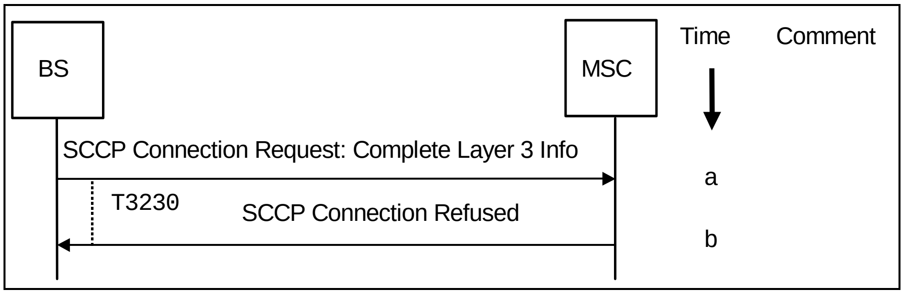

Figure 3.1.4.4.1.1-2 SCCP Connection Establishment Refusal

a. The BS sends an SCCP Connection Request message, including a user data field, to the MSC. The BS then starts timer T_{3230}.

b. Upon receipt of the SCCP Connection Request message, the MSC sends an SCCP Connection Refused message to the BS. Upon receipt of this message, the BS stops timer T_{3230}.

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

3.1.4.4.1.2 Establishment Procedure - Case 2

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

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

When a BS receives an SCCP 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 SCCP Connection Refuse message with a Handoff Failure message in the user data field to the MSC. Otherwise, an SCCP Connection Confirm message is returned to the MSC that may contain the BSMAP Handoff Request Acknowledge message in the user data field.

The diagram in Figure 3.1.4.4.1.2-1 shows a successful SCCP connection establishment procedure during handoff.

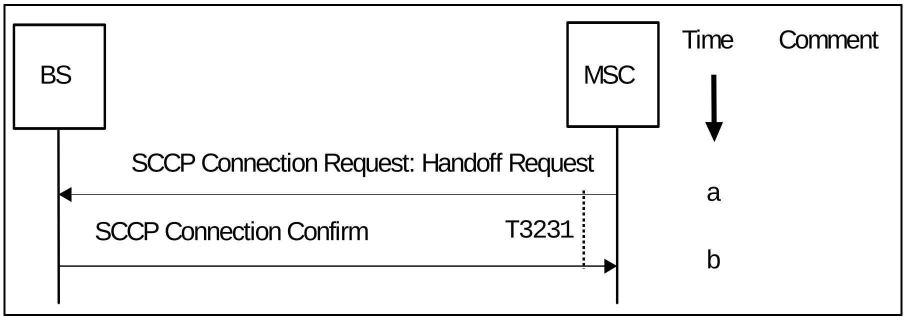

Figure 3.1.4.4.1.2-1 SCCP Connection Establishment During Handoff

a. The MSC sends an SCCP Connection Request message, including a user data field that contains a Handoff Request application message, to the BS. The MSC starts timer T_{3231}. Refer to [14] for the T_{3231} timer definition.

b. Upon receipt of the SCCP Connection Request message, the BS sends an SCCP Connection Confirm message, which shall contain the Layer 3 application message Handoff Request Acknowledge, to the MSC and establishes the connection. Upon receipt of this message, the MSC stops timer T_{3231}.

The diagram in Figure 3.1.4.4.1.2-2 shows an SCCP connection refusal during handoff.

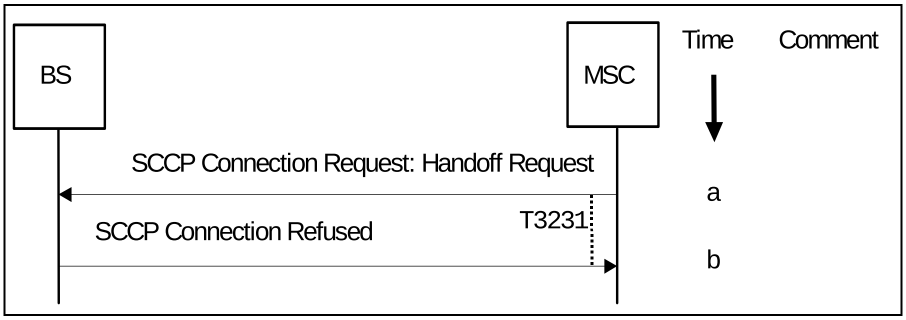

Figure 3.1.4.4.1.2-2 SCCP Connection Refusal During Handoff

a. The MSC sends an SCCP Connection Request message, including a user data field that contains a Handoff Request application message, to the BS. The MSC starts timer T_{3231}.

b. Upon receipt of the SCCP Connection Request message, the BS sends an SCCP Connection Refused message, which contains the Layer 3 application message Handoff Failure, to the MSC. Upon receipt of this message, the MSC stops timer T_{3231}.

3.1.4.4.2 Connection Release

This procedure is normally initiated at the MSC side but in the case of abnormal SCCP connection release (refer to 3.1.4.4.3), the BS may initiate connection clearing.

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

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

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

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

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

For abnormal cases a connection failure may be detected by the connection supervision service provided by SCCP. If so, the Reset Circuit procedure described in [14] is used. For other abnormal SCCP connection releases, refer to section 3.1.4.4.3, “Abnormal SCCP Release”.

3.1.4.4.3 Abnormal SCCP Release

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

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

3.1.4.4.3.1 SCCP Release by BS: Loss of SCCP Connection Information

Figure 3.1.4.4.3.1-1 demonstrates release of an SCCP connection by the BS due to loss of SCCP connection information. Note that when a circuit(s) is associated with the call at the MSC, Reset Circuit/Reset Circuit Ack [14] messages need to be exchanged between the MSC and BS to guarantee release of the circuit by both the MSC and BS.

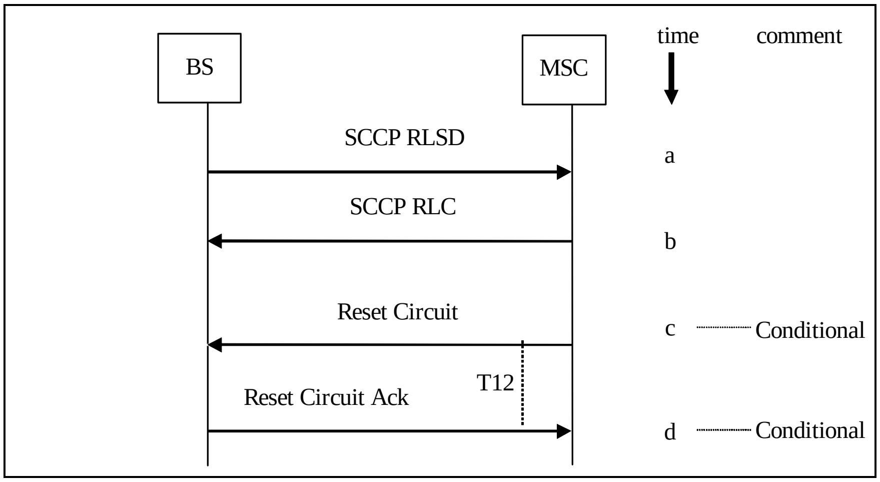

Figure 3.1.4.4.3.1-1 BS Initiated SCCP Release: BS Lost SCCP Connection Information

a. An unexpected SCCP RLSD message (under abnormal termination) is received by the MSC from the BS.

b. The MSC sends an SCCP RLC message to the BS to indicate that the SCCP RLSD message has been received and that the appropriate procedures have been completed.

c. If a circuit was involved with the call at the MSC, the MSC sends a Reset Circuit message to inform the BS that had sent the SCCP RLSD to clear its call data and starts timer T_{12}. Refer to [14] for the T_{3231} timer definition. The Reset Circuit message carries the Circuit Identity Code (CIC) of the trunk whose corrupted connection was 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}.

3.1.4.4.3.2 SCCP Release by MSC: Loss of SCCP Connection Information

Figure 3.1.4.4.3.2-1 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.

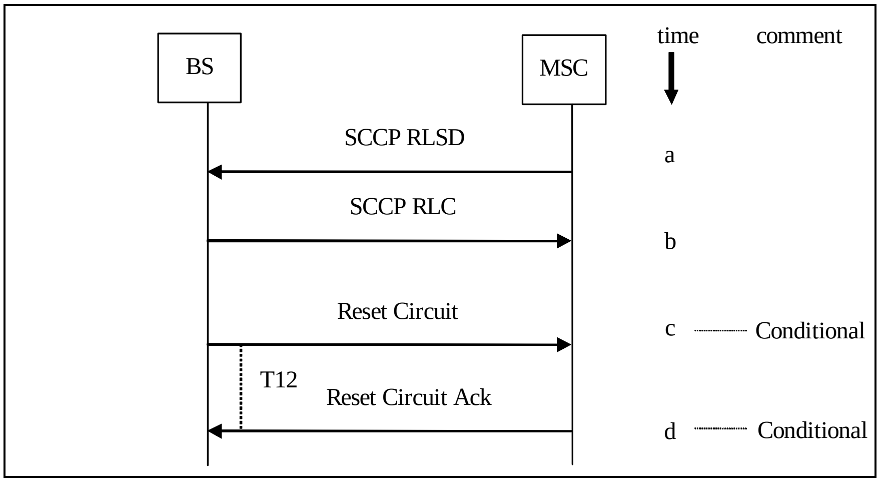

Figure 3.1.4.4.3.2-1 MSC Initiated SCCP Release: MSC Lost SCCP Connection Information

a. An unexpected SCCP RLSD message (under abnormal termination) is received by the BS from the MSC.

b. 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.

c. 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.

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

3.1.4.4.4 SCCP Reference Generation Philosophy

Referring to Figure 3.1.4.4.4-1 “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.

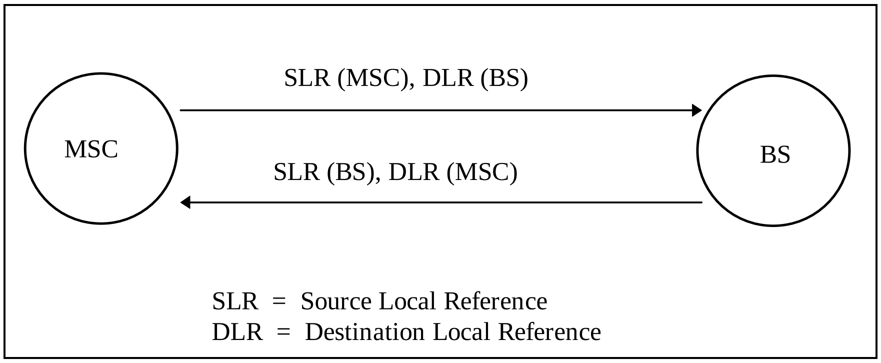

Figure 3.1.4.4.4-1 SLR/DLR Usage

MSC generation of SCCP local reference numbers shall conform to [24].

3.1.4.4.5 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 3.1.4.4.5-1 below summarizes the use of the User Data Field in SCCP frames.

Table 3.1.4.4.5-1 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 3.1.4.4.1, “Connection Establishment” and section 3.1.4.4.2, “Connection Release”.

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

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

Table 3.1.4.4.5-2 below indicates which SCCP messages shall be used to transport each of the application messages on the A1 interface.

Table 3.1.4.4.5-2 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
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]
Priority Access Channel	BSMAP	CC[d], DT1

Table 3.1.4.4.5-2 Use of SCCP for BSMAP and DTAP Messages

Application Message	Message Discriminator	SCCP Message
Assignment (PACA) Command		
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
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]
Handoff Command	BSMAP	DT1
Handoff Required Reject	BSMAP	DT1

Table 3.1.4.4.5-2 Use of SCCP for BSMAP and DTAP Messages

Application Message	Message Discriminator	SCCP Message
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 3.1.4.4.5-2.

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.

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

3.2 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.

3.2.1 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 3.2.1-1.

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 3.2.1-1 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
IS-2000 SCH reverse	65 ms	75 ms	15 ms

3.2.1.1 Performance Specification for IP Protocol Stacks

If QoS is required (refer to section 2.4.4), the BSs on the A3/A7 interfaces shall employ Diffserv [38] marking for traffic as per the classes in Table 3.2.1.1-1. The transport network shall use this class information to meet the specified ISD and ISL on the particular interface, as given in Table 3.2.1.1-1.

Table 3.2.1.1-1 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.	OAMP messages	2 sec	1.e-3

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

3.2.2 A3 User Traffic Transport Requirements

The protocol stack options for transport of user traffic that are available to operators and manufactures are shown in Figure 3.2.2-1.

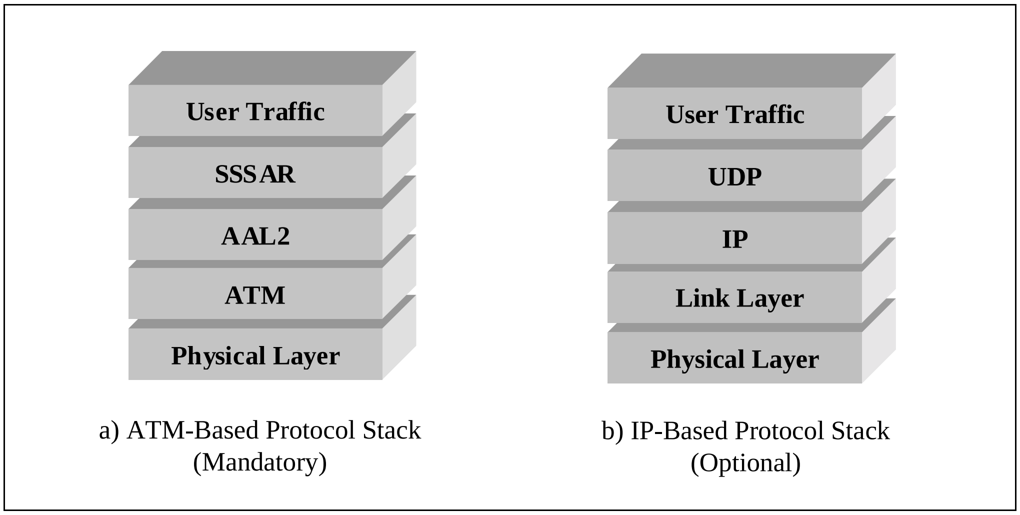

Figure 3.2.2-1 A3 User Traffic Protocol Stack

3.2.2.1 ATM-Based User Traffic Transport

The A3 user traffic interface, when implementing an ATM-based protocol stack, shall contain the layers shown in a) of Figure 3.2.2-1.

3.2.2.1.1 Physical Layer (L1) Specification

The A3 user traffic interface shall use one of the L1 specifications in section 2.1.

3.2.2.1.2 Use of ATM

For this specification only ATM PVCs shall be required for the A3 user traffic interface. These virtual circuits shall be configured through administrative procedures and no special signaling interface procedures, e.g., ATM User Network Interface (UNI) [31], shall be required.

3.2.2.1.3 Use of AAL2

When ATM is used to provide user traffic (voice/data) transport, the AAL2 protocol is used. The procedures defined in [15] determine the allocation and use of the logical channels, i.e., the connection identifiers (CIDs) that AAL2 provides over an ATM virtual circuit.

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 AAL2 for the user traffic connections.

3.2.2.2 IP-Based User Traffic Transport

The A3 user traffic interface, when implementing an IP-based protocol stack, shall contain the protocol layers shown in b) of Figure 3.2.2-1.

The requirements of this section shall apply to the transport layer for the A3 user traffic frames.

3.2.2.2.1 Physical Layer (L1) Specification

The A3 user traffic interface shall use one of the L1 specifications in section 2.1.

3.2.2.2.2 Layer 2 Specification

The A3 user traffic L2 requirements as 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

3.2.2.2.3 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 [33], 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.

3.2.2.2.4 Performance Specifications

The A3 bearer performance requirements are specified in sections 3.2.1.

The A3 bearer source BS-target BS (channel element) delay budget requirements are specified in Table 3.2.1-1.

3.2.2.2.5 QoS Specifications

The A3 bearer QoS requirements are specified in sections 2.4.4 and 3.2.1.1.

The A3 bearer mapping between Traffic Classes and Service-Level QoS requirements are specified in Table 3.2.1.1-1.

3.2.2.2.6 Security Specifications

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

3.2.3 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:

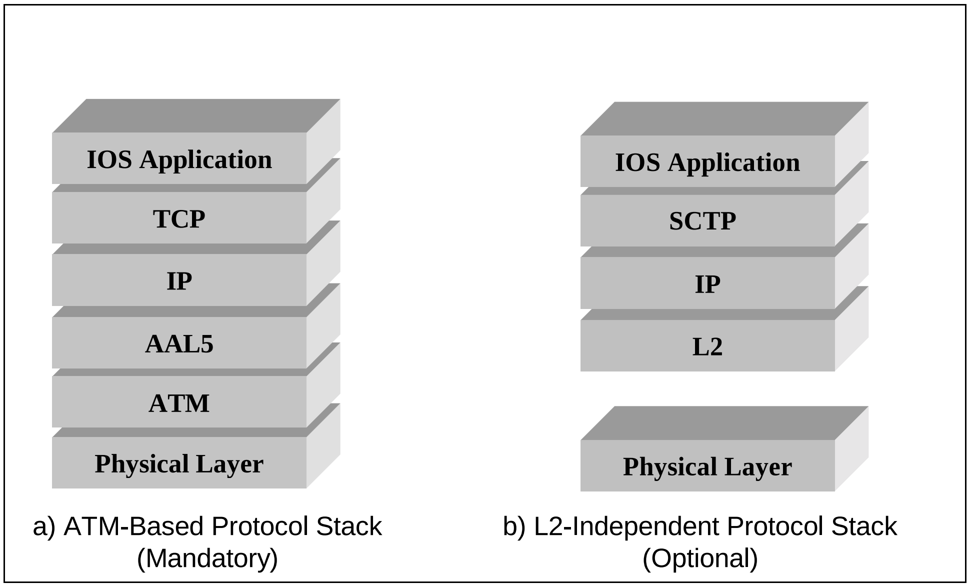

Figure 3.2.3-1 A3 and A7 Signaling Protocol Stack

3.2.3.1 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 3.2.3-1.

3.2.3.1.1 Use of Physical Layer

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

3.2.3.1.2 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 [31], 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.

3.2.3.1.3 Use of AAL5

The AAL5 requirements are specified in section 2.3.1.

3.2.3.1.4 Use of IP

The IP requirements are specified in section 2.3.2.

3.2.3.1.5 Use of TCP

The standard TCP, as described in [34] 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.

3.2.3.2 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 3.2.3-1.

3.2.3.2.1 Use of Physical Layer

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

3.2.3.2.2 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

3.2.3.2.3 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 [33], 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.

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

3.2.3.2.4 QoS Specifications

The A3/A7 signaling transport QoS requirements are specified in sections 2.4.4 and 3.2.1.1.

The A3/A7 signaling transport mapping between Traffic Classes and Service-Level QoS requirements are specified in Table 3.2.1.1-1.

3.2.3.2.5 Security Specifications

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

3.2.3.2.6 Use of SCTP

SCTP provides a reliable message transport in IP networks. SCTP is used without any modifications and is defined in [41].

An SCTP connection between two endpoints is called an association. One SCTP association can be considered as a logical aggregation of streams. A stream is a unidirectional logical channel between two endpoints. To achieve bi-directional communications, two streams are necessary, one in each direction. Each user message (i.e., a message originated from the user application above SCTP) handled by SCTP has to specify the stream to which it is attached. A stream identifier exists for each stream within an association. Therefore, each SCTP stream can be considered as an independent flow of user messages from one node to another. This stream independence characteristic provides a mechanism to avoid and/or manage blocking between streams.

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

SCTP port value 5604 is used for A7 signaling.

3.2.3.2.7 Use of TCP

Refer to section 3.2.3.1.5.

3.3 A8 and A9 Interfaces

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

Signaling over the A9 interface requires a reliable transport protocol and appropriate addressing and routing mechanisms to deliver messages from source to destination. The signaling protocol stack option available to operators and manufacturers for the A9 interface is shown in Figure 3.3-1.

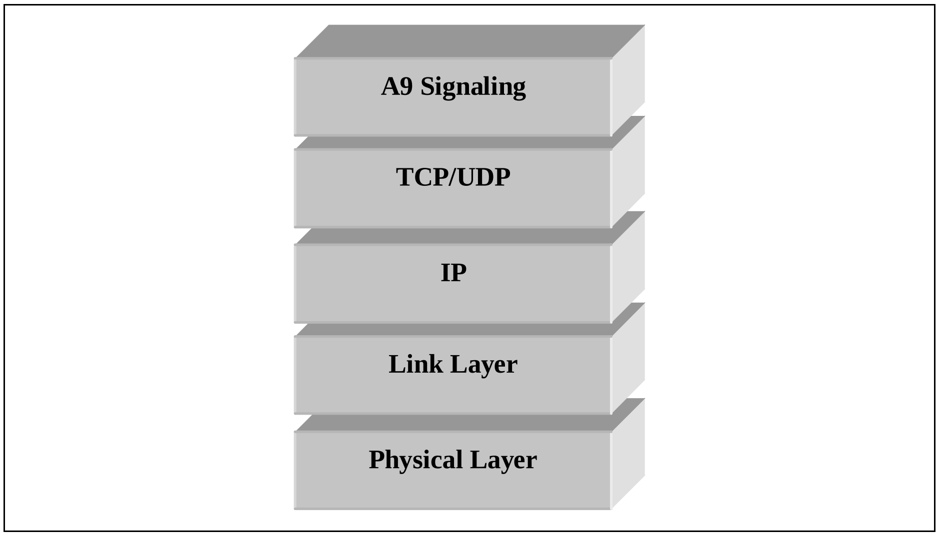

Figure 3.3-1 A9 Signaling Protocol Stack

The protocol stack options for transport of user traffic that are available to operators and manufacturers is shown in Figure 3.3-2.

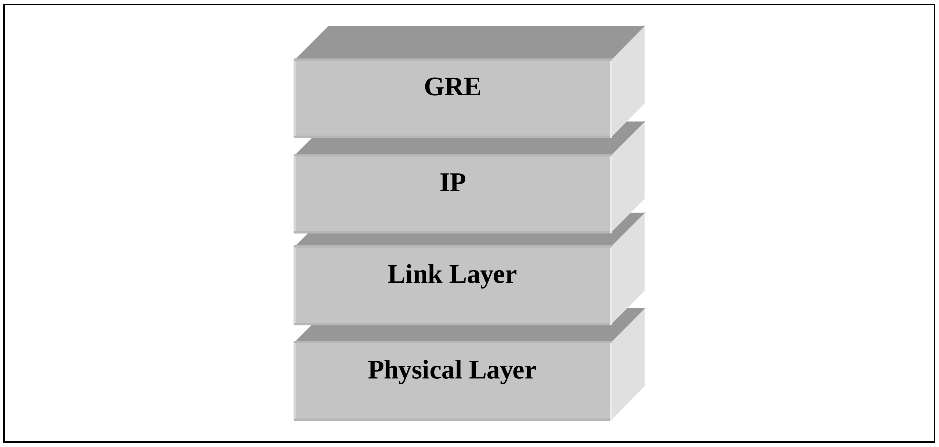

Figure 3.3-2 A8 User Traffic Protocol Stack

3.3.1 Use of TCP

When TCP is used for transferring the A9 interface messages, the standard TCP, as described in [34] and shown in section 2.5, shall be used. The following TCP port value is reserved for signaling across the A9 interface:

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

3.3.2 Use of UDP

When UDP is used for transferring the A9 interface messages, the standard UDP, as described in [32], shall be used.

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

3.3.3 Use of GRE

The BS shall set the Key field in the GRE header to the value in the Key field in the A8 Traffic ID element in the A9-Connect-A8 message received from the PCF indicating that the PCF accepts the A8 connection. The PCF shall set the Key field in the GRE header to the value in the Key field in the A8 Traffic ID element in the A9-Setup-A8 message received from the BS requesting the establishment of the A8 connection.

3.4 A10 and A11 Interface

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

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

Signaling over the A11 interface requires a reliable transport protocol and appropriate addressing and routing mechanisms to deliver messages from source to destination. The signaling protocol stack option available to operators and manufacturers for the A11 interface is shown in Figure 3.4-1.

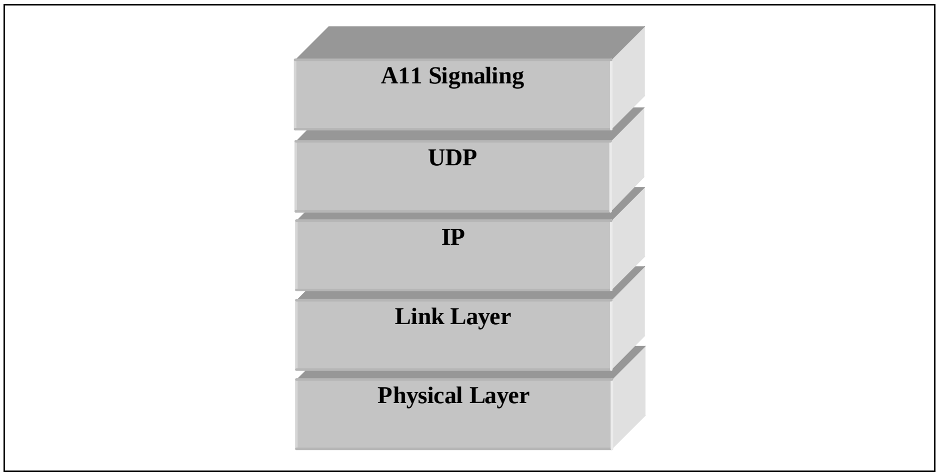

Figure 3.4-1 A11 Signaling Protocol Stack

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

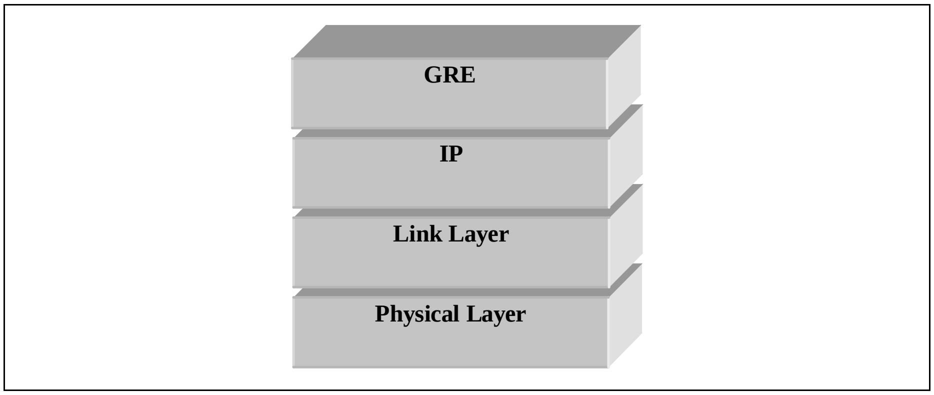

Figure 3.4-2 A10 User Traffic Protocol Stack

3.4.1 Use of UDP

The use of UDP over the A11 interface conforms to the use of UDP for Mobile IP, as specified in [36] with the exception of the UDP port number.

3.4.2 Use of GRE

The PCF shall set the Key field in the GRE header to value in the Key field in the Session Specific Extension in the A11-Registration Reply message received from the PDSN indicating that the PDSN accepts the A10 connection. The PDSN shall set the Key field in the GRE header to the value in the Key field in the Session Specific Extension in the A11-Registration Request message received from the PCF requesting the establishment of the A10 connection.