# Wireless Datagram Protocol

Version 14 Jun 2001

Open Mobile Alliance
WAP-259-WDP-20010614-a

Continues the Technical Activities
Originated in the WAP Forum

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

[OMA-Template-SpecWAP-20030912]

EX-1014
U.S. Patent 9,619,578

Use of this document is subject to all of the terms and conditions of the Use Agreement located at http://www.openmobilealliance.org/UseAgreement.html.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the "OMA IPR Declarations" list at http://www.openmobilealliance.org/ipr.html. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE "OMA IPR DECLARATIONS" LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

# Contents


1. SCOPE ..... 5
2. REFERENCES ..... 6
   2.1 NORMATIVE REFERENCES ..... 6
   2.2 INFORMATIVE REFERENCES ..... 8
3. TERMINOLOGY AND CONVENTIONS ..... 9
   3.1 CONVENTIONS ..... 9
   3.2 DEFINITIONS ..... 9
   3.3 GENERAL CONCEPTS ..... 11
   3.4 ABBREVIATIONS ..... 11
4. WDP ARCHITECTURAL OVERVIEW ..... 14
   4.1 REFERENCE MODEL ..... 14
   4.2 GENERAL DESCRIPTION OF THE WDP PROTOCOL ..... 15
      4.2.1 WDP Management Entity ..... 16
      4.2.2 Processing Errors of WDP Datagrams ..... 17
      4.2.3 Security Considerations ..... 17
   4.3 WDP CONFORMANCE ..... 17
      4.3.1 WDP Adaptation Layer Segmentation & Re-assembly ..... 17
   4.4 WDP BEARER DEPENDENT PROFILES ..... 18
      4.4.1 WDP over GSM ..... 18
      4.4.2 WDP over ANSI-136 ..... 20
      4.4.3 WDP over CDPD ..... 23
      4.4.4 WDP over CDMA ..... 23
      4.4.5 WDP over PDC (Japan) ..... 26
      4.4.6 WDP Profile Over iDEN ..... 27
      4.4.7 WDP over FLEX™ and ReFLEX™ ..... 29
      4.4.8 WDP over PHS ..... 30
      4.4.9 WDP over DataTAC ..... 31
      4.4.10 WDP Profile Over TETRA ..... 31
      4.4.11 WDP over DECT ..... 32
      4.4.12 WDP over Mobitex ..... 33
5. ELEMENTS FOR LAYER-TO-LAYER COMMUNICATION ..... 35
   5.1 SERVICE PRIMITIVE NOTATION ..... 35
   5.2 SERVICE PRIMITIVE TYPES ..... 35
   5.3 WDP SERVICE PRIMITIVES ..... 36
      5.3.1 General ..... 36
      5.3.2 T-DUnitdata ..... 36
      5.3.3 T-DError ..... 36
6. WDP PROTOCOL DESCRIPTION ..... 38
   6.1 INTRODUCTION ..... 38
   6.2 MAPPING OF WDP FOR IP ..... 38
   6.3 MAPPING OF WDP FOR GSM SMS, ANSI-136 GHOST AND USSD ..... 38
      6.3.1 Binary Header Format ..... 38
      6.3.2 Segmentation and Reassembly ..... 38
      6.3.3 Mapping of WDP to GSM SMS Phase 1 Text-based Headers ..... 39
      6.3.4 Mapping of WDP to GSM USSD ..... 41
   6.4 MAPPING OF WDP FOR ANSI-136 GUTS/R-DATA ..... 41
   6.5 MAPPING OF WDP TO CDMA SMS ..... 41
      6.5.1 Datagram Structure ..... 42
      6.5.2 SMS User Data ..... 42
      6.5.3 Use of MESSAGE_ID Field ..... 42
      6.5.4 Segmentation and Reassembly ..... 43
      6.5.5 Segmentation Example ..... 43


© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

**6.6 MAPPING OF WDP TO FLEX™ AND REFLEX™ ..... 43**
**6.7 MAPPING OF WDP TO DATATAC ..... 44**
**6.8 MAPPING OF WDP TO GSM CELL BROADCAST ..... 55**
6.8.1 Binary Header Format ..... 55
6.8.2 Source and Destination Port Addressing ..... 55
6.8.3 Segmentation and Reassembly ..... 56
**6.9 MAPPING OF WDP TO TETRA SDS ..... 56**
**6.10 MAPPING OF WDP FOR MOBITEX ..... 57**
6.10.1 Short Datagram Format ..... 57
6.10.2 Long Datagram Format ..... 57
6.10.3 Long Datagram Format with Space Saving Function (SSF) ..... 58
6.10.4 Bit Set for Datagram ..... 58
6.10.5 Encapsulation of WDP Mapping for Mobitex into MPAKs ..... 59
**APPENDIX A. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE) ..... 60**
**APPENDIX B. PORT NUMBER DEFINITIONS (NORMATIVE) ..... 68**
**APPENDIX C. BEARER TYPE ASSIGNMENTS (NORMATIVE) ..... 69**
**APPENDIX D. MAPPING WDP INTO UDH FORMAT (INFORMATIVE) ..... 71**
**APPENDIX E. IMPLEMENTATION NOTES (INFORMATIVE) ..... 74**
**APPENDIX F. CHANGE HISTORY (INFORMATIVE) ..... 75**
**F.1 APPROVED VERSION HISTORY ..... 75**
**F.2 DRAFT/CANDIDATE VERSION 1_0 HISTORY ..... ERROR! BOOKMARK NOT DEFINED.**

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# 1. Scope

The Transport layer protocol in the WAP architecture consists of the Wireless Transaction Protocol (WTP) and the Wireless Datagram Protocol (WDP). The WDP layer operates above the data capable bearer services supported by the various network types. As a general datagram service, WDP offers a consistent service to the upper layer protocol (Security, Transaction and Session) of WAP and communicate transparently over one of the available bearer services.

The protocols in the WAP family are designed for use over narrowband bearers in wireless telecommunications networks.

Since the WDP protocols provide a common interface to the upper layer protocols (Security, Transaction and Session layers) , they are able to function independently of the underlying wireless network. This is accomplished by adapting the transport layer to specific features of the underlying bearer.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# 2. References

## 2.1 Normative References


[ANSI136] ANSI/TIA/EIA-136 Series: TDMA Cellular PCS, Rev B. March 1, 2000. URL:http://www.tiaonline.org/.

[IOPProc] "OMA Interoperability Policy and Process". Open Mobile Alliance™. OMA-IOP-Process-v1_0. URL:http//www.openmobilealliance.org/

[DECT] ETSI norm EN 300 175: DECT Common Interface specification. URL:http://www.etsi.org/

[DECT–D2] ETSI norm EN 301 238: DECT Data Service Profile, service type D, mobility class 2. URL:http://www.etsi.org/

[DECT-FP2] ETSI norm DEN/DECT-020128: CTM Feature package 2. URL:http://www.etsi.org/

[DECT-GSM] ETSI norm ETS 300 764: DECT/GSM interworking profile. URL:http://www.etsi.org/

[DPRS] ETSI norm EN 301 649: DECT Packet Radio Service. URL:http://www.etsi.org/

[DM] *DataTAC Messaging Protocol Specification, Version 1.0*, Document Number 68P04025C10, Motorola

[FLEX] FLEX Protocol Specification Document, Document Number 68P81139B01, Motorola.

[FLEXsuite] FLEXsuite™ of Enabling Protocols, Motorola.

[ETSI GSM] ETSI GSM specifications. URL:http://www.etsi.org/

[GSM0260] ETSI Digital Cellular Telecommunication Systems (phase 2+) : General Packet Radio Service (GPRS) - stage 1 (GSM 02.60). URL:http://www.etsi.org/

[GSM0290] ETSI Digital Cellular Telecommunication Systems (phase 2) : Unstructured Supplementary Service Data(USSD) - stage 1 (GSM 02.90). URL:http://www.etsi.org/

[GSM0332] ETSI Digital cellular telecommunications system (Phase 2+); Universal Geographical Area Description (GAD) (GSM 03.32 version 5.1.0 Release 1996). URL http://www.etsiorg/

[GSM0340] ETSI Digital Cellular Telecommunication Systems (phase 2+); Technical realisation of the Short Message Service (SMS) Point-to-Point (P); (GSM 03.40 version 7.4.0 release 1998). URL:http://www.etsi.org/

[GSM0341] ETSI Digital Cellular Telecommunication Systems (phase 2+); Technical realization of Short Message Service Cell Broadcast (SMSCB) (GSM 03.41). URL http://www.etsi.org/

[GSM0360] ETSI Digital Cellular Telecommunication Systems (phase 2+) : General Packet Radio Service (GPRS) - stage 2 (GSM 03.60). URL:http://www.etsi.org/

[GSM0390] ETSI Digital Cellular Telecommunication Systems (phase 2) : Unstructured Supplementary Service Data(USSD) - stage 2 (GSM 03.90). URL:http://www.etsi.org/

[GSM0490] ETSI Digital Cellular Telecommunication Systems (phase 2) : Unstructured Supplementary Service Data(USSD) - stage 3 (GSM 04.90). URL:http://www.etsi.org/

[GSM0808] ETSI Digital cellular telecommunications system (Phase 2+) Mobile-services Switching Centre - Base Station System (MSC - BSS) interface; Layer 3 specification (GSM 08.08). URL:http://www.etsi.org/

[IDEN] iDEN™ Technical Overview, Motorola Document Number 68P81095E55-A

[ITU E.164] Recommendation E.164/I.331 (05/97) - The international public telecommunication numbering plan. ITU-T. May 1997. URL:http://www.itu.int/

[ITU X.25] Recommendation X.25 (10/96) - Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit. ITU-T. October 1996. URL:http://www.itu.int/

[Mobitex] Mobitex Interface Specification (MIS), rev R4A, document number LZY 232 105, especially the Network Layer section. The MIS can be ordered at http://www.ericsson.se/wireless/products/mobsys/mobitex/subpages/mdown/mdownmi.shtml


© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

| | |
|---|---|
| [NCL] | *Native Control Language Specification, Version 1.2*, Document Number 68P04025C15, Motorola. |
| [PIAFS] | PHS Internet Access Forum Standard URL:http://www.infopro.or.jp/piaf/ |
| [RCR STD-27] | ARIB Standard Personal Digital Cellular RCR STD-27, Association of Radio Industries and Businesses |
| [RCR STD-28] | ARIB Standard Personal Handy Phone System RCR STD-28 , version 3 (Rev.1) , Association of Radio Industries and Businesses |
| [ReFLEX] | ReFLEX Protocol Specification Document, Document Number 68P81139B02-A, Motorola. |
| [RFC768] | "User Datagram Protocol". J. Postel. August 1980. URL:http://www.ietf.org/rfc/rfc768.txt |
| [RFC791] | "Internet Protocol". J. Postel. September 1981. URL:http://www.ietf.org/rfc/rfc791.txt |
| [RFC2119] | "Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. URL:http://www.ietf.org/rfc/rfc2119.txt |
| [RFC2234] | "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997. URL:http://www.ietf.org/rfc/rfc2234.txt |
| [RFC2373] | "IP Version 6 Addressing Architecture". S. Deering(Cisco), R. Hinden(Nokia). July 1998. URL:http://www.ietf.org/rfc/rfc2373.txt |
| [RFC2460] | "Internet Protocol, Version 6 (IPv6) Specification". S. Deering(Cisco), R. Hinden(Nokia). December 1998. URL:http://www.ietf.org/rfc/rfc2460.txt |
| [SCR] | *Standard Context Routing Protocol Specification, Version 1.0*, Document Number 68P04025C20, Motorola. |
| [TET 392-1] | ETSI Radio Equipment and System (RES); Terrestial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General Network Design (ETS 300 392-1). URL:http://www.etsi.org/ |
| [TET 392-2] | ETSI Radio Equipment and System (RES); Terrestial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI) (ETS 300 392-2). December 1999. URL:http://www.etsi.org/ |
| [TET SDSTL] | ETSI Radio Equipment and System (RES); Terrestial Trunked Radio (TETRA); Voice plus Data (V+D); SDS Transport Layer. URL:http://www.etsi.org/ |
| [TIAEIA-95] | TIA/EIA-95-B: Mobile Station-Base Station Compatibility Standard for Wideband Spread Spectrum Cellular Systems |
| [TIAEIA-136-350] | TIA/EIA-136-350: Data-Service Control |
| [TIAEIA-136-370] | TIA/EIA-136-370 |
| [TIAEIA-136-711] | TIA/EIA-136-711 |
| [TIAEIA-136-750] | TIA/EIA-136-750: General UDP Transport Service (GUTS) |
| [TIAEIA-637] | TIA/EIA-637-A: Short Message Service for Spread Spectrum Systems |
| [TIAEIA-707] | TIA/EIA-707-A: Data Service Options for Spread Spectrum Systems |
| [TIAEIA-732] | TIA/EIA/IS-732 series: Cellular Digital Packet Data |
| [TTC JJ-70.10] | Mobile Application Part(MAP) Signaling System of Digital Mobile, Communications Network Inter-Node Interface(DMNI) for PDC, Telecommunication Technology Committee, URL:http://www.ttc.or.jp/ |
| [TTC JT-Q931-b] | PHS Public Cell Station - Digital Network Interface Layer 3 – Specification, Telecommunication Technology Committee URL:http://www.ttc.or.jp/ |
| [TTC JT-Q932-a] | PHS Public Cell Station - Digital Network Interface - PHS Service Control Procedures, Telecommunication Technology Committee URL:http://www.ttc.or.jp/ |
| [TTC JT-Q921-b] | PHS Public Cell Station - Digital Network Interface Layer 2 – Specification, Telecommunication Technology Committee URL:http://www.ttc.or.jp/ |
| [TTC JT-Q1218-a] | Inter-network Interface for PHS Roaming, Telecommunication Technology Committee |


**© 2003 Open Mobile Alliance Ltd. All Rights Reserved.**
**Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.**

URL:http://www.ttc.or.jp/

[TTC JT-Q1218] Inter-network Interface for Intelligent Network, Telecommunication Technology Committee URL:http://www.ttc.or.jp/

[WAPGSMUD] "WAP over GSM USSD". WAP Forum™. WAP-204-WAPOverGSMUSSD. URL:http//www.wapforum.org/

[WCMP] "Wireless Control Message Protocol", Open Mobile Alliance™, WAP-202-WCMP, http://www.openmobilealliance.org/.

## 2.2 Informative References

[IS07498] ISO 7498 OSI Reference Model

[RFC793] "Transmission Control Protocol". J. Postel. September 1981. URL:http://www.ietf.org/rfc/rfc793.txt

[TCP/Ipill3] "TCP/IP Illustrated, Volume 3". W. Richard Stevens. Addison-Wesley Publishing Company Inc. 1996. ISBN 0-201-63495-3

[WAE] "Wireless Application Environment Specification". WAP Forum™. WAP-190-WAESpec. URL:http://www.wapforum.org/

[WAPARCH] "Wireless Application Protocol Architecture Specification". WAP Forum™. WAP-100-WAPArch. URL:http://www.wapforum.org/

[WCMPWDPAdapt] "WDP and WCMP Adaptation Gateway Protocol", Open Mobile Alliance™, WAP-159-WDPWCMPAdapt, http://www.openmobilealliance.org/.

[WSP] "Wireless Session Protocol", Open Mobile Alliance™, -WAP-230-WSP, http://www.openmobilealliance.org/.

[WTLS] "Wireless Transport Layer Security". WAP Forum™. WAP-199-WTLS. URL:http//www.wapforum.org/

[WTP] "Wireless Transaction Protocol", Open Mobile Alliance™, WAP-224-WTP, http://www.openmobilealliance.org/.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# 3. Terminology and Conventions

## 3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope”, are normative, unless they are explicitly indicated to be informative.

## 3.2 Definitions

**ANSI-136 General UDP Transport Service (GUTS)**
GUTS is a general-purpose application data delivery service. GUTS utilises the Internet Standard User Datagram Protocol (UDP) to specify the intended application or port.

**ANSI-136 GSM Hosted SMS Teleservice (GHOST)**
GHOST is an ANSI-136 teleservice used to tunnel GSM SMS PDUs.

**ANSI-136 Packet Data**
ANSI-136 Packet Data provides a packet data radio service in ANSI-136.

**ANSI-136 R-DATA**
ANSI-136 R-Data is a two-way narrowband transport mechanism that is supported on the digital control channel (DCCH) and digital traffic channel (DTC). R-Data can be used to carry GUTS messages or other teleservices messages such as the Cellular Messaging Teleservice (CMT). It is by nature similar to a datagram service.

**Cell Broadcast**
Cell Broadcast permits a number of short messages to be broadcast to all receivers within a particular region.

**Cellular Digital Packet Data (CDPD)**
CDPD is an AMPS overlay packet radio service.

**CS**
Cell Station is similar to Base Station. This term is used in RCR STD-28 ( for PHS).

**CSD**
Circuit-Switched Data provides a point-to-point connection between the device and the network. This service is typically available in cellular and PCS networks.

**DECT**
DECT is the Digital Enhanced Cordless Telecommunications standard, as defined within ETSI.

**Device**
An entity that is capable of sending and/or receiving packets of information via a wireless network and has an unique device address. See [WAP] for further information.

**Device Address**
The address of a device is its unique network address assigned by a carrier and following the format defined by an international standard such as E.164 for MSISDN addresses, X.121 for X.25 addresses or RFC 791 for IPv4 addresses. An address uniquely identifies the sending and/or receiving device.

**DM**
DataTAC Messaging is a protocol that enables two-way communications between wireless terminals.

**DPRS**
The DECT Packet Radio Service profile (EN 301 649) defines packetized data services over the DECT air interface.

**FLEX™**
A one-way paging protocol developed to optimise channel efficiency, battery life, and cost per bit for transmitting messages over a wide geographical area.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

**FLEX™ Suite of Application Enabling Protocols**
A suite of protocols and features which enable applications on FLEX and ReFLEX networks. The FLEX Suite protocols operate at the layer above the FLEX and/or ReFLEX protocol layers.

**GPRS**
General Packet Radio Service as defined in GSM 02.60 and 03.60. GPRS provide a packet data service overlay to GSM networks.

**GPRS-136**
General Packet Radio Service as defined for use in supporting the packet data requirements of ANSI-136 networks by the UWCC (Universal Wireless Communications Consortium http://www.uwcc.org).

**iDEN™**
Integrated Digital Enhanced Network.

**iDEN™ Circuit Switched Data**
iDEN Circuit-Switched Data provides a point-to-point connection between the device and the network.

**iDEN™ Packet Data**
iDEN Packet Data provides a packet data radio service to the iDEN system. This packet data service utilises mobile IP as the mechanism to enable mobile devices to roam within iDEN.

**IS-637 SMS**
IS-637 SMS [TIAEIA-637] provides a short message service in IS-95 CDMA networks.

**IS-707 Circuit Switching Data**
IS-707 Circuit Data Service [TIAEIA-707] provides a circuit data radio service in IS-95 CDMA networks.

**IS-707 Packet Data**
IS-707 Packet Data [TIAEIA-707] provides a packet data radio service in IS-95 CDMA networks.

**IS-95 CDMA**
Wireless network technology defined in [TIAEIA-95].

**Maximum Packet Lifetime, MPL**
MPL is fixed by the used carrier (the network system).

**Mobitex**
A narrow-band wireless technology, for dedicated two-way packet-data networks, that uses cellular radio technology.

**MSC**
Mobile-services Switching Center provides controls for call connection and service to support mobile communications services for PDC.

**NCL**
Native Command Language is a protocol that enables two-way communications between a DTE and a wireless modem.

**Network Type**
Network type refers to any network, which is classified by a common set of characteristics (i.e. air interface) and standards. Examples of network types include GSM, CDMA, ANSI-136, iDEN, FLEX and Mobitex. Each network type may contain multiple underlying bearer services suitable for transporting WDP.

**Packet**
A packet is a set of bytes being transmitted over the network as an undivided entity. Each packet contains a header, which describes the context of the packet, its position in the packet group, its position in the transmission, and other pertinent information. The WDP header is positioned into the packet according to the features of the underlying bearer.

**Port**
Ports are used as a sub-addressing mechanism inside a device. A port number identifies the higher layer entity (such as a protocol or application) directly above the WDP layer.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

**ReFLEX™**
A two-way paging protocol developed to enable the efficient delivery of messages and content over-the-air in both the outbound (system to pager) and inbound (pager to system) directions.

**SDS**
Point-to-Point short data service is a narrow bandwidth data transport mechanism available in TETRA network.

**SMS**
Point-to-Point Short Message Service is a narrow bandwidth data transport mechanism typically available in cellular and PCS networks.

**SCR**
Standard Context Routing is a protocol that enables two-way communications between fixed host computers and wireless terminal fleets.

**TETRA**
Terrestrial Trunked Radio

**TETRA Packet Data**
TETRA Packet Data provides a packet data radio services in TETRA.

**Transmission**
Transmission is a collection of one or more packet from a source to a destination.

**UAR**
Uniform Addressing and Routing

**Underlying Bearer**
An underlying bearer is a data transport mechanism used to carry the WDP protocols between two devices. Examples of underlying bearers include CDPD, GSM SMS, GSM USSD, GSM CSD, GSM GPRS, ANSI-136 GUTS, ANSI-136 GHOST, CSD, and Packet Data. During a data exchange between two devices, more than one underlying bearer may be used.

**USSD**
Unstructured Supplementary Service Data is narrow bandwidth transport mechanism. USSD is a GSM supplementary service. It uses the signalling channels as a bearer, and is half-duplex (only one of the parties are allowed to send at any one moment). It is by nature similar to circuit switched data service.

## 3.3 General Concepts

This chapter describes the industry terminology related to the specifications.

**Client and Server**
The terms client and server are used in order to map the WAP environment to well known and existing systems. A client is a device (or application) which initiates requests for data. The server is a device which passively waits for data requests from client devices or actively pushes data to client devices. The server can either accept the request or reject it. A device can simultaneously act both as client and server for different applications, or even in the context of one application. An application can serve a number of clients (as a server), but act as a client towards another server.

## 3.4 Abbreviations

| | |
|---|---|
| API | Application Programming Interface |
| BMI | Base Station, MSC, Interworking Function (IWF) |
| BS | Base Station |
| BSD | Berkeley Software Distribution |
| CBC-IF | Cell Broadcast Centre Interface |
| CBS | Cell Broadcast short message service |
| CDMA | Code Division Multiple Access |
| CDPD | Cellular Digital Packet Data |
| DECT DSP | DECT Data Service Profile |
| DM | DataTAC Messaging |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

| | |
|---|---|
| CS | Cell Station |
| CSD | Circuit Switched Data |
| DCS | Data Coding Scheme |
| ETSI | European Telecommunication Standardisation Institute |
| GHOST | GSM Hosted SMS Teleservice |
| GPRS | General Packet Radio Service |
| GSM | Global System for Mobile Communication |
| GUTS | General UDP Transport Service |
| HLR | Home Location Register |
| iDEN | Integrated Digital Enhanced Network |
| IE | Information Element |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| ITSI | Individual TETRA Subscriber Identity |
| IWF | Interworking Function |
| LAPi | Link Access Protocol iDEN |
| LSB | Least significant bits |
| MAC | Medium Access Control |
| MAN | Mobitex Subscription Number |
| MAP | Mobile Application Part |
| MDBS | Mobile Data Base Station |
| MDG | Mobile Data Gateway |
| MD-IS | Mobile Data – Intermediate System |
| MDLP | Mobile Data Link Protocol |
| MIS | Mobitex Interface Specification |
| MPAK | Mobitex Network Layer Packets |
| MPL | Maximum Packet Lifetime (constant) |
| MSISDN | Mobile Subscriber ISDN (Telephone number or address of device) |
| MS | Mobile Station |
| MSB | Most significant bits |
| MSC | Mobile Switching Centre |
| MSC | Mobile-services Switching Center (for PDC) |
| MTU | Maximum Transfer Unit |
| NCL | Native Command Language |
| PCS | Personal Communication Services |
| PDC | Personal Digital Cellular |
| PDLP | Packet Data Link Protocol |
| PHS | Personal Handy Phone System |
| PLMN | Public Land Mobile Network |
| PPP | Point-to-Point Protocol |
| RAS | Remote Access Server |
| R-Data | Relay Data |
| RFCL | Radio Frequency Convergence Layer |
| RLP | Radio Link Protocol |
| SAR | Segmentation and Reassembly |
| SCR | Standard Context Routing |
| SDS | Short Data Service |
| SDS-TL | Short Data Service Transport Layer |
| SMSC | Short Message Service Centre |
| SMSCB | Short Message Service Cell Broadcast |
| SMS | Short Message Service |
| SNDCP | SubNetwork Dependent Convergence Protocol |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

| | |
|---|---|
| SPT | Server Processing Time |
| SS7 | Signalling System 7 |
| SSAR | Simplified Segmentation and Reassembly |
| SSF | Space Saving Function (Mobitex) |
| SwMI | TETRA Switching and Management Infrastructure |
| TCAP | Transaction Capability Application Part |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TDMA | Time Division Multiple Access |
| TETRA | Terrestrial Trunked Radio |
| TIA/EIA | Telecommunications Industry Association/Electronic Industry Association |
| TSALP | TETRA SDS Adaptation Layer Protocol |
| TSAP | Transport Service Access Point |
| UDH | User-Data Header (see GSM 03.40) |
| UDHL | User-Data Header Length |
| UDL | User-Data Length |
| UDP | User Datagram Protocol |
| UDCP | USSD Dialogue Control Protocol |
| USSD | Unstructured Supplementary Service Data |
| USSDC | Unstructured Supplementary Service Data Center |
| VLR | Visitor Location Registry |
| VPLMN | Visitor Public Land Mobile Network |
| WAE | Wireless Application Environment |
| WAP | Wireless Application Protocol |
| WDP | Wireless Datagram Protocol |
| WORM-ARQ | WORM-Auto Repeat Request |
| WSP | Wireless Session Protocol |
| WTP | Wireless Transaction Protocol |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# 4. WDP Architectural Overview

The WDP protocol operates above the data capable bearer services supported by multiple network types. WDP offers a consistent service to the upper protocols (Security, Transaction and Session) of WAP and communicate transparently over one of the available bearer services.

## 4.1 Reference Model

The model of protocol architecture for the Wireless Datagram Protocol is given in Figure 4-1.

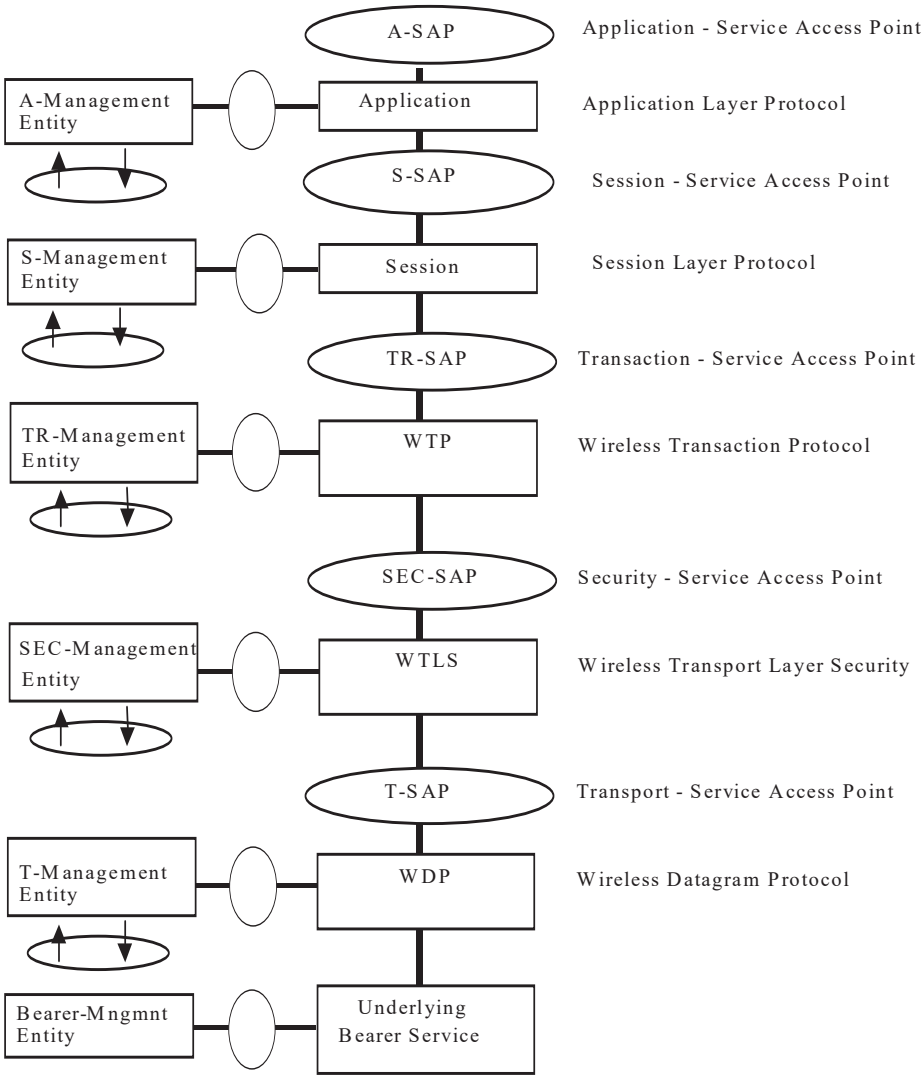



**Figure 4-1 WAP Reference Architecture**

The services offered by WDP include application addressing by port numbers, optional segmentation and reassembly and optional error detection. The services allow for applications to operate transparently over different available bearer services.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

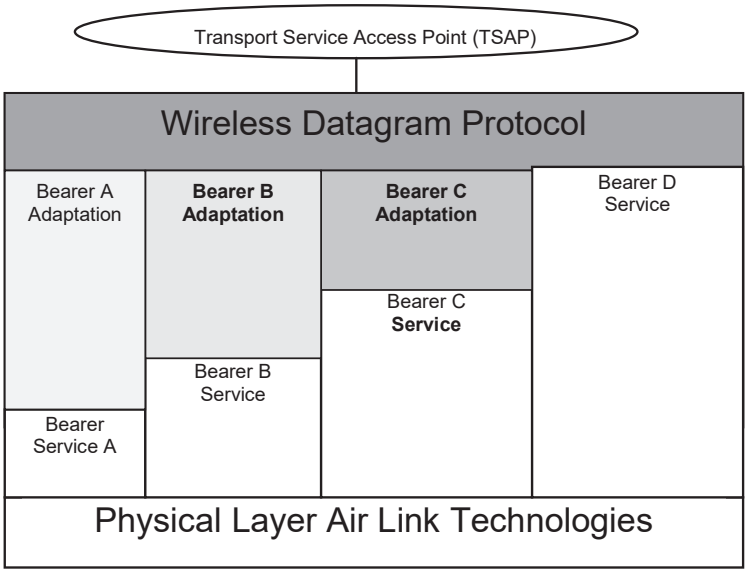



**Figure 4-2: Wireless Datagram Protocol Architecture**

The model of protocol architecture for the Wireless Transport Protocol is given in Figure 4-2.

WDP offers a consistent service at the Transport Service Access Point to the upper layer protocol of WAP. This consistency of service allows for applications to operate transparently over different available bearer services. The varying heights of each of the bearer services shown in Figure 4-2 illustrates the difference in functions provided by the bearers and thus the difference in WDP protocol necessary to operate over those bearers to maintain the same service offering at the Transport Service Access Point is accomplished by a bearer adaptation.

WDP can be mapped onto different bearers, with different characteristics. In order to optimise the protocol with respect to memory usage and radio transmission efficiency, the protocol performance over each bearer may vary. However, the WDP service and service primitives will remain the same, providing a consistent interface to the higher layers.

## 4.2 General Description of the WDP Protocol

The WDP layer operates above the data capable bearer services supported by the various network types. As a general datagram service, WDP offers a consistent service to the upper layer protocol (Security, Transaction and Session) of WAP and communicate transparently over one of the available bearer services.

WDP supports several simultaneous communication instances from a higher layer over a single underlying WDP bearer service. The port number identifies the higher layer entity above WDP. This may be another protocol layer such as the Wireless Transaction Protocol (WTP) or the Wireless Session Protocol (WSP) or an application such as electronic mail. By reusing the elements of the underlying bearers, WDP can be implemented to support multiple bearers and yet be optimised for efficient operation within the limited resources of a mobile device.

Figure 4-3 shows a general model of the WAP protocol architecture and how WDP fits into that architecture.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

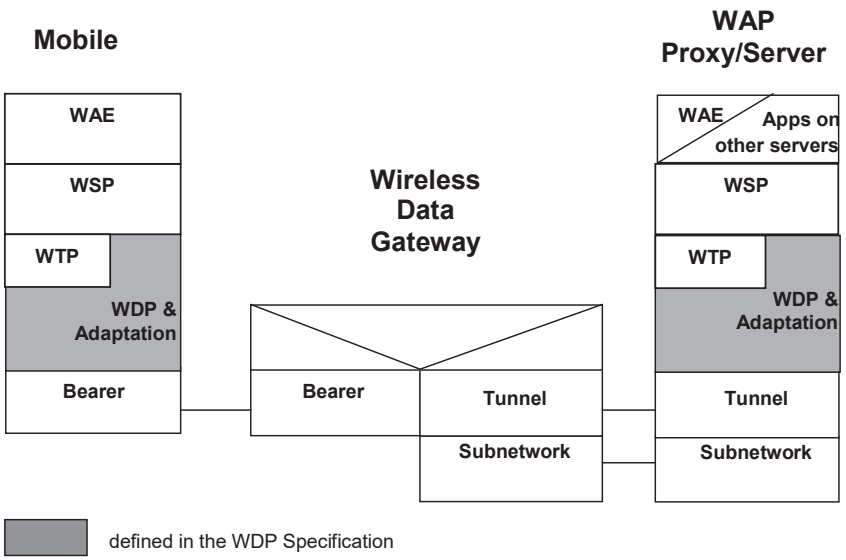



**Figure 4-3 General WDP Architecture**

In Figure 4-3 the shaded areas are the layers of protocol which the WDP Specification is specifically applicable. At the Mobile the WDP protocol consists of the common WDP elements shown by the layer labelled WDP. The Adaptation Layer is the layer of the WDP protocol that maps the WDP protocol functions directly onto a specific bearer. The Adaptation Layer is different for each bearer and deals with the specific capabilities and characteristics of that bearer service. The Bearer Layer is the bearer service such as GSM SMS, or USSD, or ANSI-136 R-Data, or CDMA Packet Data. At the Gateway the Adaptation Layer terminates and passes the WDP packets on to a WAP Proxy/Server via a Tunnelling protocol, which is the interface between the Gateway that supports the bearer service and the WAP Proxy/Server. For example if the bearer were GSM SMS, the Gateway would be a GSM SMSC and would support a specific protocol (the Tunnelling protocol) to interface the SMSC to other servers. The SubNetwork is any common networking technology that can be used to connect two communicating devices, examples are wide-area networks based on TCP/IP or X.25, or LANs operating TCP/IP over Ethernet. The WAP Proxy/Server may offer application content or may act as a gateway between the wireless WTP protocol suites and the wired Internet.

## 4.2.1 WDP Management Entity

The WDP Management Entity is used as an interface between the WDP layer and the environment of the device. The WDP Management Entity provides information to the WDP layer about changes in the devices environment, which may impact the correct operation of WDP.

The WDP protocol is designed around an assumption that the operating environment is capable of transmitting and receiving data.

For example, this assumption includes the following basic capabilities that must be provided by the mobile:

- the mobile is within a coverage area applicable to the bearer service being invoked;
- the mobile having sufficient power and the power being on;
- sufficient resources (processing and memory) within the mobile are available to WDP;
- the WDP protocol is correctly configured, and ;
- the user is willing to receive/transmit data.

The WDP Management Entity would monitor the state of the above services/capabilities of the mobile's environment and would notify the WDP layer if one or more of the assumed services were not available.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

For example if the mobile roamed out of coverage for a bearer service, the Bearer Management Entity should report to the WDP Management Entity that transmission/reception over that bearer is no longer possible. In turn the WDP Management Entity would indicate to the WDP layer to close all active connections over that bearer. Other examples such as low battery power would be handled in a similar way by the WDP Management Entity.

In addition to monitoring the state of the mobile environment the WDP Management Entity may be used as the interface to the user for setting various configuration parameters used by WDP, such as device address. It could also be used to implement functions available to the user such as a "drop all data connections" feature. In general the WDP Management Entity will deal with all issues related to initialisation, configuration, dynamic re-configuration, and resources, as they pertain to the WDP layer.

Since the WDP Management Entity must interact with various components of a device which are manufacturer specific, the design and implementation of the WDP Management Entity is considered outside the scope of the WDP Specification and is an implementation issue.

### 4.2.2 Processing Errors of WDP Datagrams

Processing errors can happen when WDP datagrams are sent from a WDP provider to another. For example, a Wireless Data Gateway may not be able to send the datagram to the WAP Gateway, or there is no application listening to the destination port, or the receiver might not have enough buffer space to receive a large message.

The Wireless Control Message Protocol (WCMP) provides an efficient error handling mechanism for WDP, resulting in improved performance for WAP protocols and applications. Therefore the WCMP protocol SHOULD be implemented. See the [WCMP] specification.

WDP is expected not to pass up corrupted messages. If a particular bearer does not provide this service, then the WDP bearer adaptation MUST provide payload protection.

### 4.2.3 Security Considerations

WDP has no authentication mechanisms.

## 4.3 WDP Conformance

There is a minimum set of WDP features that need to be implemented to ensure that implementations from multiple vendors will be able to interoperate.

The WDP protocol operates over various bearer services. Each bearer service for which WDP is specified supports a datagram service. It is this datagram service which WDP uses to support the abstract service primitives defined in this specification. For bearer services supporting IP the WDP protocol MUST be UDP. For bearer services not supporting IP the WDP protocol defined in this specification MUST be used. Appendix A lists the features required from WDP implementations.

### 4.3.1 WDP Adaptation Layer Segmentation & Re-assembly

When introducing a new bearer service, considerations should be given to the potential inclusion of the Segmentation & Re-Assembly (SAR) functionality in the adaptation layer of that new bearer service.

The following criteria should be considered when evaluating the need for the SAR functionality of a new bearer service:

- the applications (or higher communication layers) that are likely to use the bearer service: to estimate if the typical payload of those applications can be handled by the new bearer service (for example, when using X.509 certificates with WTLS, typical session establishment message can be up to 1500 bytes in size); and
- the bearer service Maximum Transfer Unit (MTU).

If the applications typical payload exceed the bearer MTU, support for SAR SHOULD be included in the new bearer service specification. When SAR is defined for a bearer, the bearer service must be able at least to recognise and discard segmented messages, if it is not able to receive and re-assemble them.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-SpecWAP-20030912]

The support for SAR in a bearer service does not guarantee the application that transport of data to user will be done in a timely manner. Therefore, applications need to be aware that user experience may be bad if large volumes of data are sent over certain bearer services.

## 4.4 WDP Bearer Dependent Profiles

The following figures illustrate the protocol profiles for operating WDP between a mobile device and server over a specific RF technology and a specific bearer within that technology.

### 4.4.1 WDP over GSM

#### 4.4.1.1 GSM SMS Profile

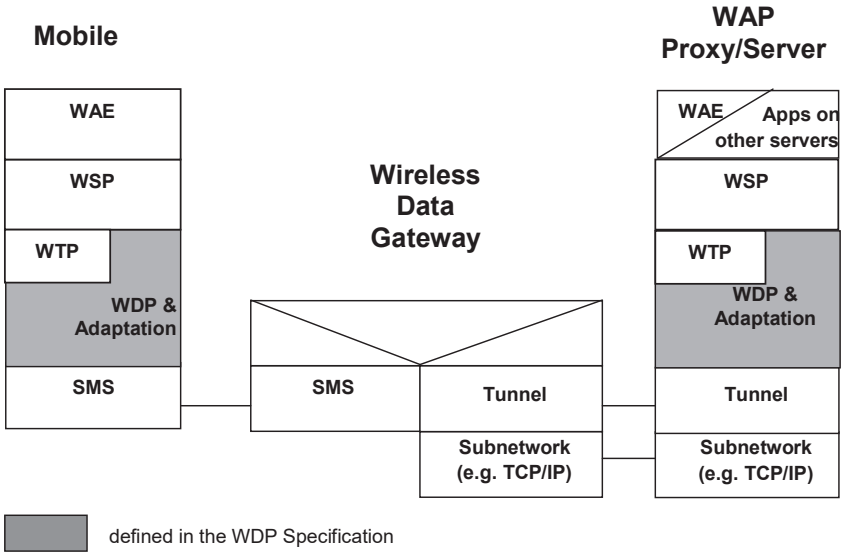



**Figure 4-4 WDP over GSM SMS**

Figure 4-4 illustrates the protocol profile for the WDP layer when operating over the SMS bearer service.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

### 4.4.1.2 GSM USSD Profile

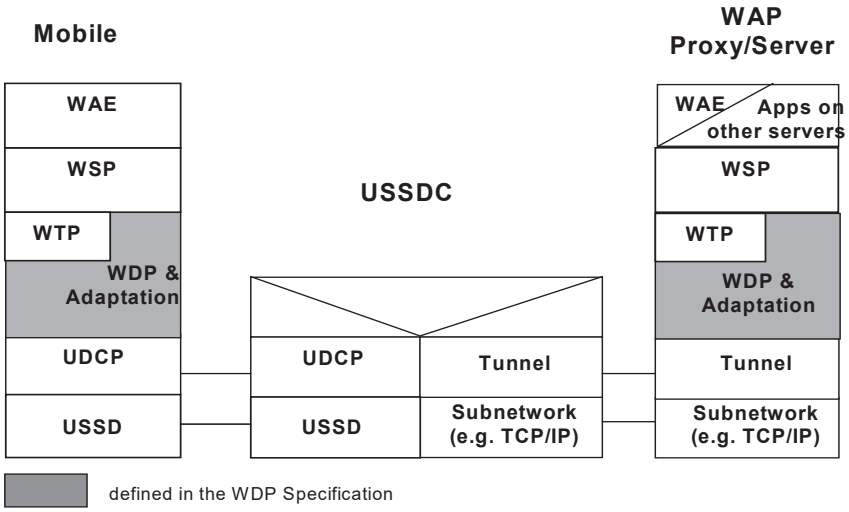



**Figure 4-5 WDP over GSM USSD**

Figure 4-5 illustrates the protocol profile for the WTP layer when operating over the USSD bearer service.

The USSD Dialogue Control Protocol (UDCP) is responsible for managing the half-duplex USSD dialogue and providing the upper layer with the address to the WAP Proxy/Server.

### 4.4.1.3 GSM Circuit-Switched Data

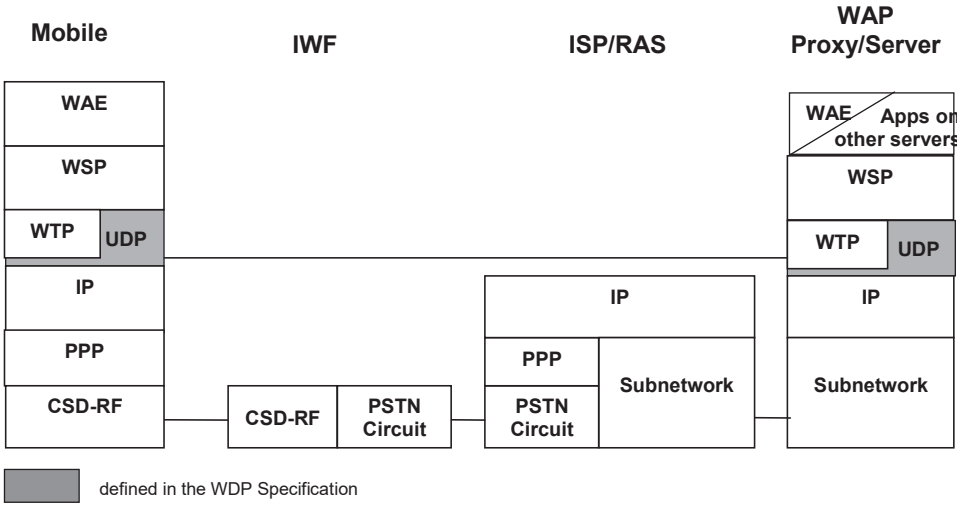



**Figure 4-6 WDP over GSM Circuit Switched Data Channel**

Figure 4-6 illustrates the protocol profile for the WDP layer when operating over a Circuit-Switched Data connection. The IWF provides non-transparent CSD services and is not present in transparent circuit data calls. The Remote Access Server (RAS) or the Internet Service Provider (ISP) provides connectivity to the Internet network so that the mobile and WAP proxy server can address each other. The WAP Proxy/Server can terminate the WAE or serve as a proxy to other applications on the Internet.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

#### 4.4.1.4 GSM GPRS Profile

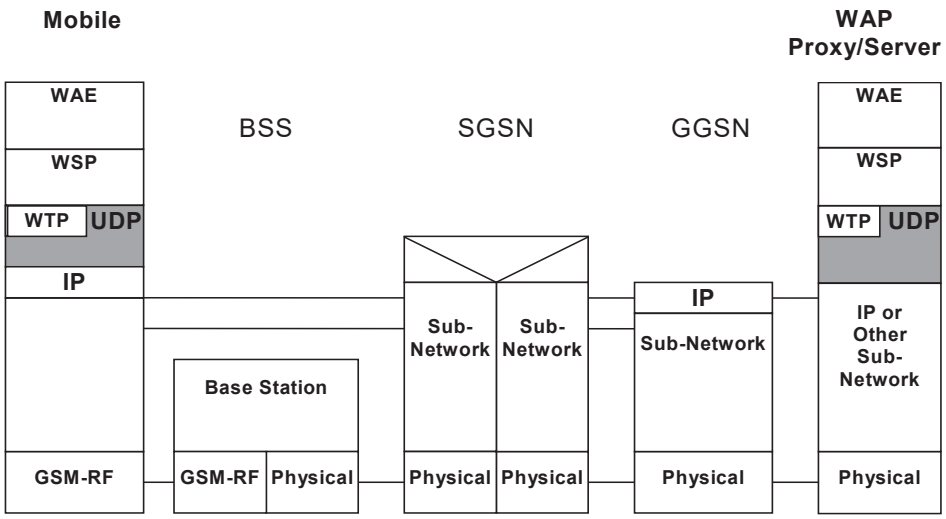



**Figure 4-7 WDP over GSM GPRS**

Figure 4-7 illustrates the protocol profile for the WDP layer when operating over the GPRS bearer service. GPRS supports IP to the mobile therefore UDP/IP will provide datagram services.

#### 4.4.1.5 GSM Cell Broadcast

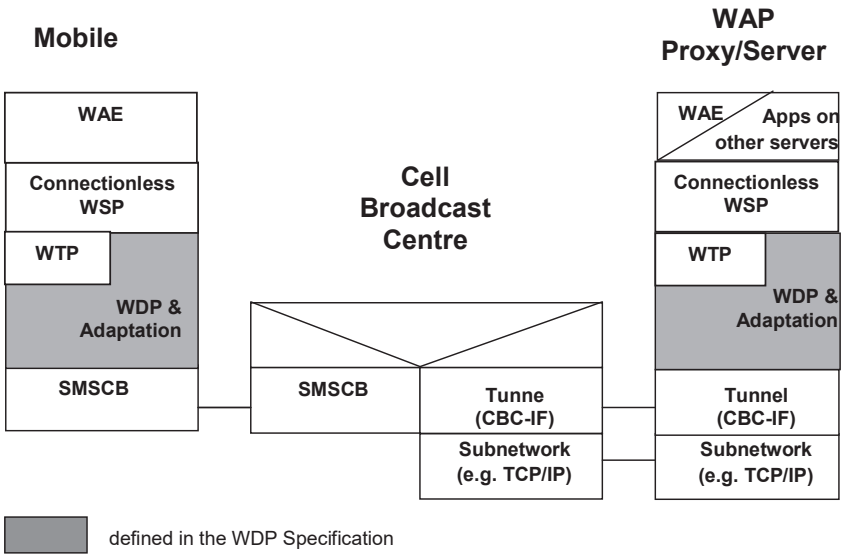



**Figure 4-8 WDP over GSM Cell Broadcast**

Figure 4-8 illustrates the protocol profile for the WDP layer when operating over the GSM Cell Broadcast bearer service.

### 4.4.2 WDP over ANSI-136

The WDP layer operates above the data capable bearer services supported by ANSI-136.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

#### 4.4.2.1.1 ANSI-136 R-Data Profile using GUTS

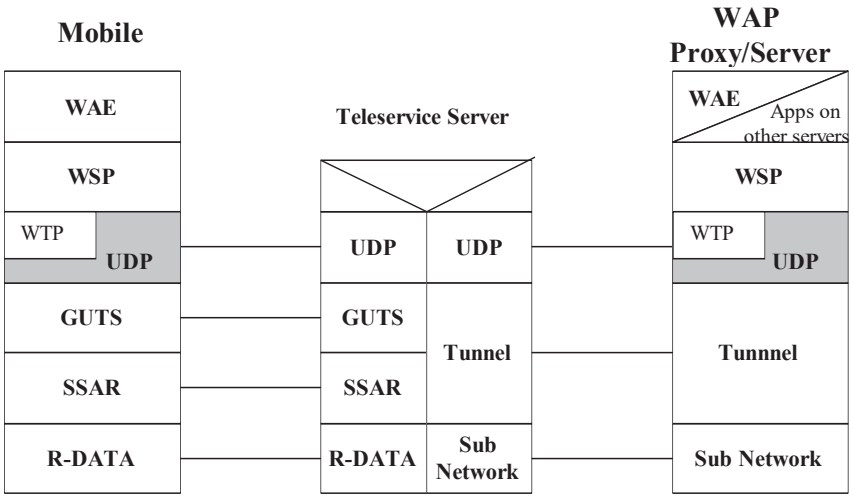



**Figure 4-9: WDP over ANSI-136 R-DATA using GUTS**

Figure 4-9 illustrates the protocol profile for the WDP layer when operating over the ANSI-136 GUTS and R-DATA bearer service. For efficiency WDP can be supported directly on GUTS. A GUTS protocol discriminator would be needed for this purpose. The ANSI-136 Teleservice Server interface protocol is SubNetwork dependent and not specified in the WAP specifications.

#### 4.4.2.1.2 ANSI-136 R-Data Profile using GHOST

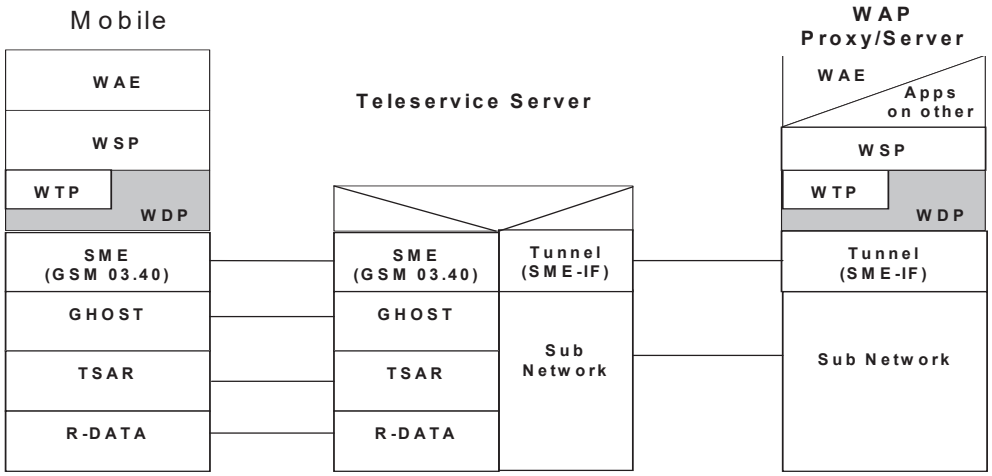



**Figure 4-10 WDP over ANSI-136 R-DATA using GHOST**

Figure 4-10 illustrates the protocol profile for the WDP layer when operating over the ANSI-136 GHOST and R-DATA bearer service. Note that Teleservice Segmentation and Reassembly (TSAR) is optional.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

#### 4.4.2.2 ANSI-136 Circuit-Switched Data Profile

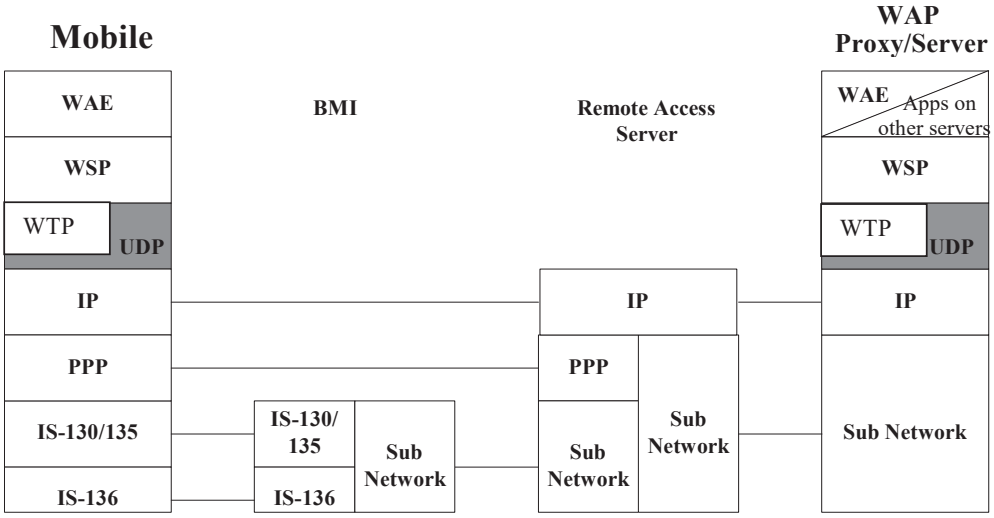



**Figure 4-11: WDP over ANSI-136 Circuit-Switched Data**

Figure 4-11 illustrates the protocol profile for the WDP layer when operating over an ANSI-136 Circuit-Switched Data connection. A remote access or an Internet service provider (ISP) provides connectivity to a WAP proxy server. The WAP Proxy/Server can terminate the WAE or serve as a proxy to other applications on the Internet.

#### 4.4.2.3 ANSI-136 Packet Data Profile

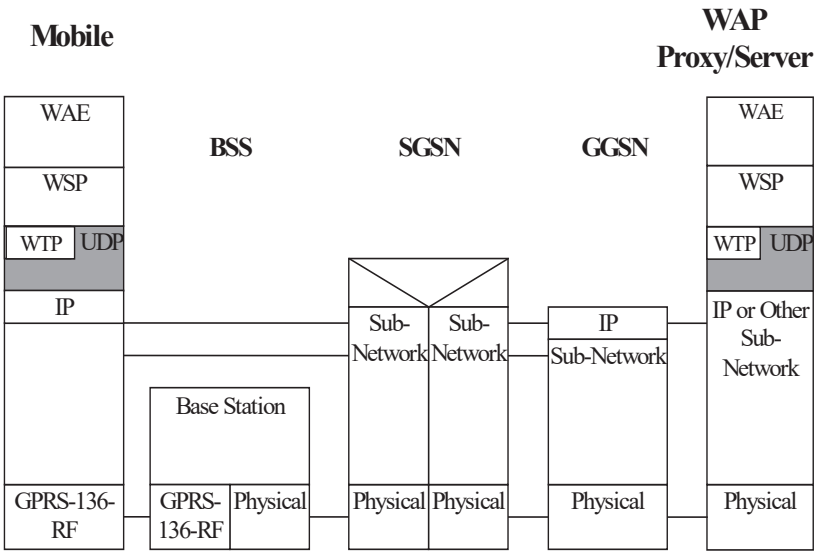



**Figure 4-12: WDP over ANSI-136 Packet data**

Figure 4-12 illustrates the protocol profile for the WDP layer when operating over the ANSI-136 Packet Data bearer service. ANSI-136 uses GPRS to support its packet data requirements. GPRS supports IP to the mobile therefore UDP/IP will provide datagram services.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

*Note:* The term GPRS-136 RF denotes both the GPRS-136 (30 kHz channel spacing) and GPRS-136HS (200 kHz channel spacing).

### 4.4.3 WDP over CDPD

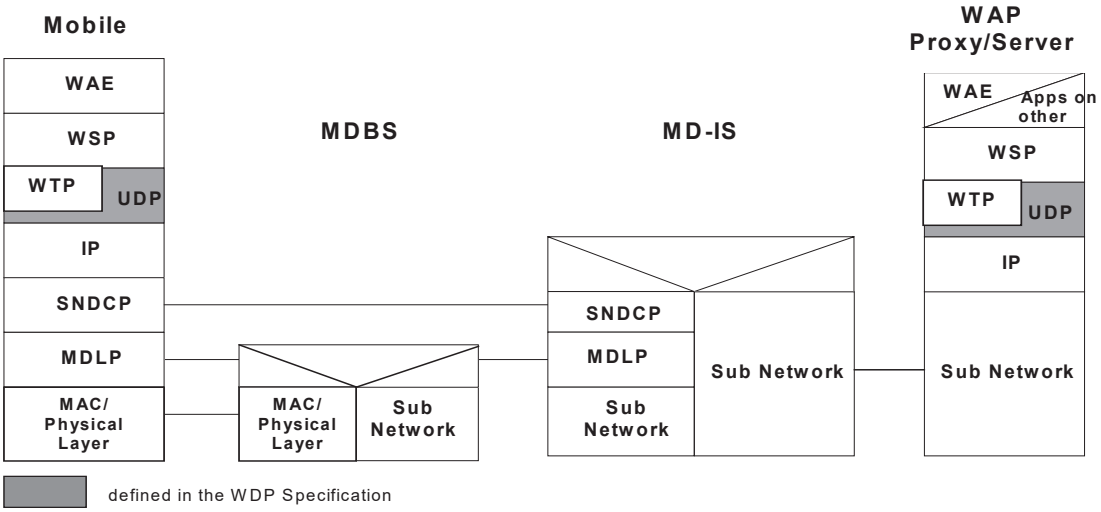



**Figure 4-13 WDP over CDPD**

Figure 4-13 illustrates the protocol profile for the WDP layer when operating over the CDPD bearer service. CDPD supports IP to the mobile therefore UDP/IP will provide the datagram services.

### 4.4.4 WDP over CDMA

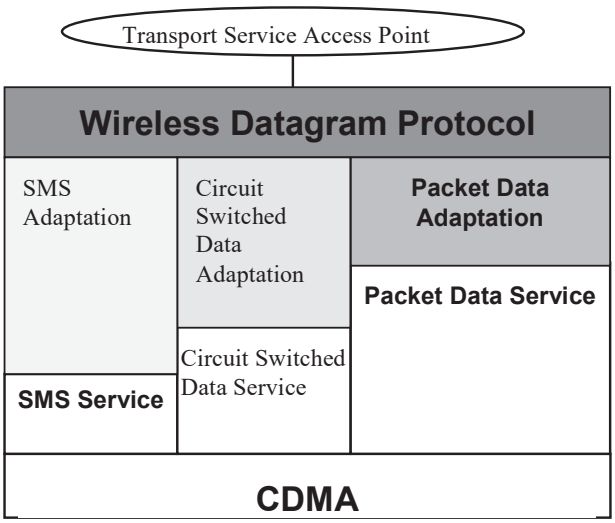



**Figure 4-14: WDP over CDMA Bearer Services**

The WDP layer operates above the data capable bearer services supported by CDMA. Figure 4-14 identifies the CDMA bearer services presented in this specification.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

#### 4.4.4.1 CDMA Circuit-Switched Data Profile

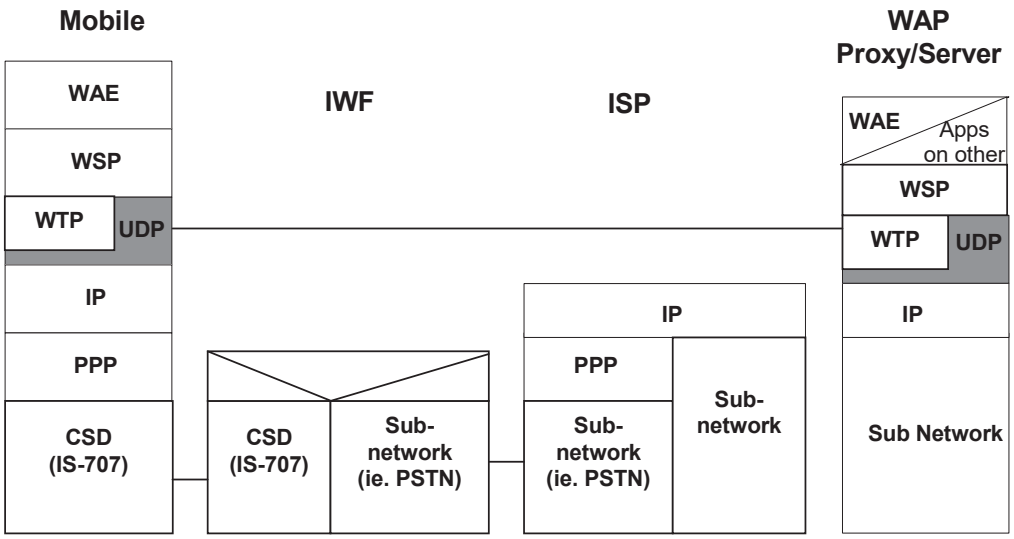



**Figure 4-15 WDP over CDMA Circuit-Switched Data Channel**

Figure 4-15 illustrates the protocol profile for the WDP layer when operating over the CDMA Circuit-Switched Bearer Service. The Internet Service Provider (ISP) provides connectivity to the Internet network so that the mobile and WAP proxy server can address each other. The WAP proxy/server can terminate the WAE or serve as a proxy to other applications on the Internet. The CDMA Circuit-Switched Data protocol consists of TCP, IP, PPP & RLP layer as defined in [TIAEIA-707] over IS-95 air interface.

The IS-707 Circuit Switching Data layer in Figure 4-15 includes a TCP/IP/PPP stack, which is used only between the mobile station and the IWF.

The profile defined here does not preclude the use of other non-standard data services that modify IS-707 Circuit Switching Data to provide a direct connection from the IWF to the Internet. Such a service may provide a way to route IP packets between the mobile station and the WAP gateway via the Internet, without using the PSTN, and it may be used at the discretion of the mobile station manufacturer and network operator. The WAP stack is not affected by this change in the bearer service, as WDP will still use UDP datagrams to communicate with its peer.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

#### 4.4.4.2 CDMA Packet Data Profile

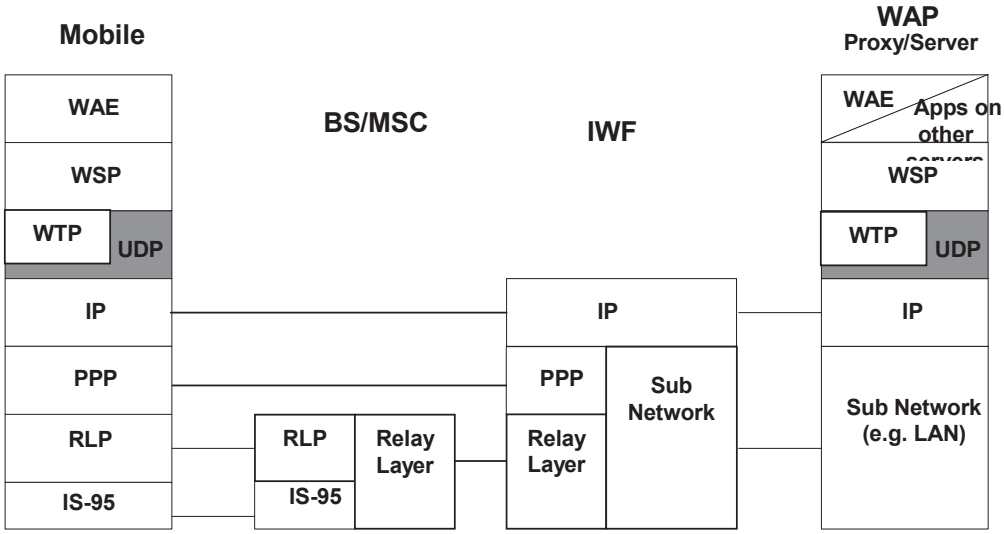



**Figure 4-16 WDP over CDMA Packet Data Channel**

Figure 4-16 illustrates the protocol profile for the WDP layer when operating over the CDMA Packet Data bearer service. CDMA Packet Data supports IP to the mobile. WTP over UDP and UDP/IP provide transaction-oriented and datagram services respectively. The WAP Proxy/Server can terminate the WAE or serve as a proxy to other applications on the Internet.

#### 4.4.4.3 CDMA SMS

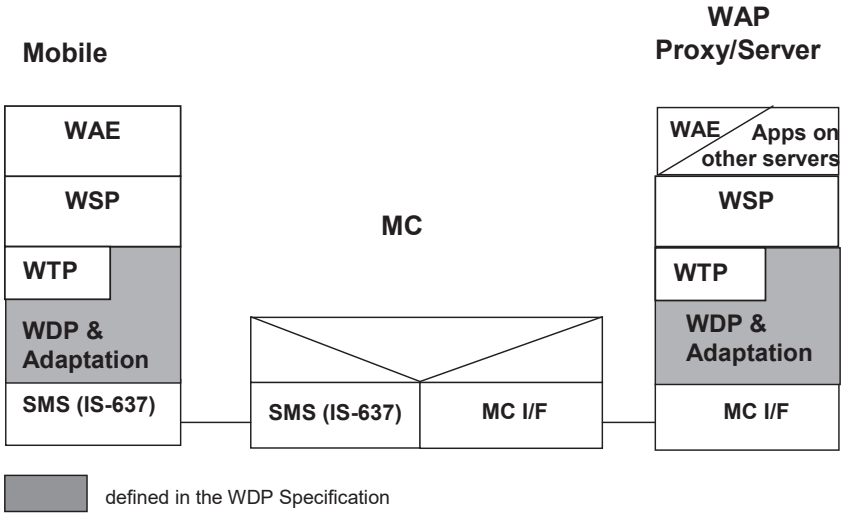



**Figure 4-17 WDP over CDMA SMS**

Figure 4-17 illustrates the protocol profile for the WDP layer when operating over the IS-637 SMS bearer service. The WAP Proxy/Server is Terminal Equipment, as defined in the reference model in [TIAEIA-637], section 1.4.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

## 4.4.5 WDP over PDC (Japan)

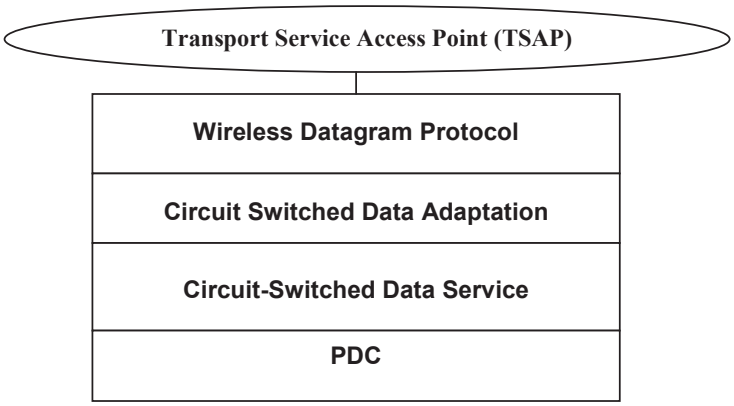



**Figure 4-18: WDP over PDC Bearer Services**

PDC is a digital cellular network, for which air interface is defined in [RCR STD-27] and network inter-node interface is defined in [TTC JJ-70.10]. The WDP layer operates above the data capable bearer services supported by PDC. Figure 4-18 identifies the PDC bearer services presented in this specification. PDC provides Circuit Switched Data Service.

### 4.4.5.1 PDC Circuit-Switched Data

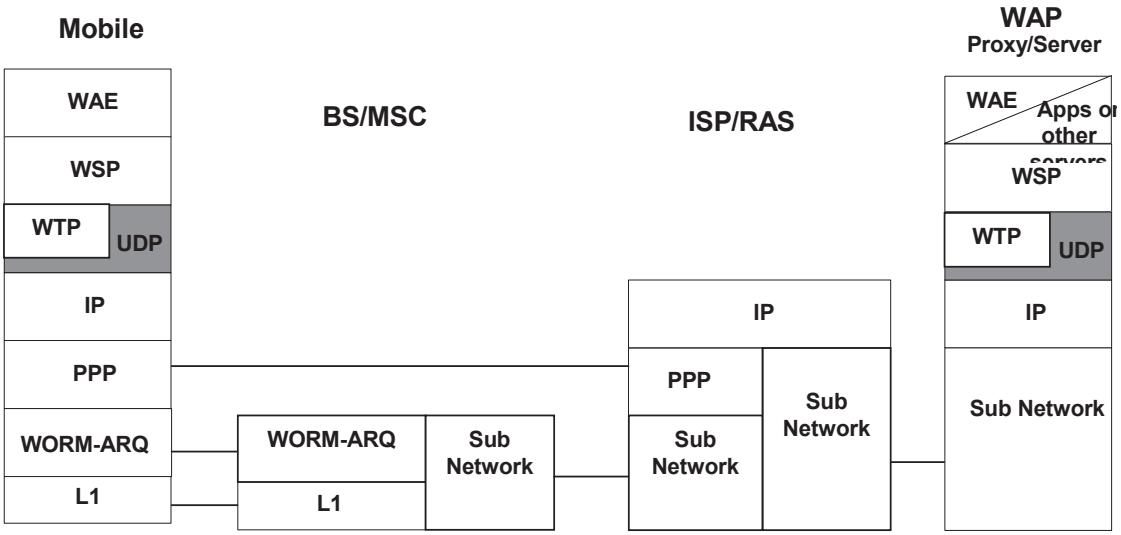



**Figure 4-19 WDP over PDC Circuit-Switched Data Channel**

Figure 4-19 illustrates the protocol profile for the WDP layer when operating over a PDC Circuit-Switched Data connection. The MSC terminates air protocol for PDC. The Internet Service Provider (ISP) Provides Internet connectivity to the Internet network so that the mobile and the WAP Proxy/Server can address each other. The WAP Proxy/Server can terminate the WAE or serve as a proxy to other applications on the Internet.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

#### 4.4.5.2 PDC Packet Data Profile

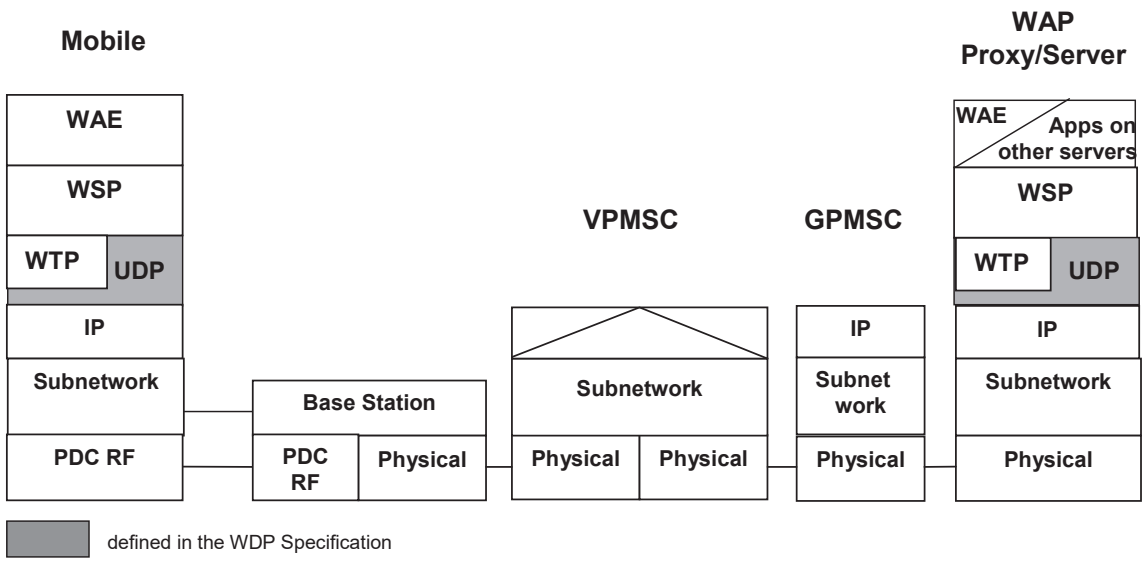



**Figure 4-20 WDP over PDC Packet Data Channel**

Figure 4-20 illustrates the protocol profile for the WDP layer when operating over a PDC Packet Data bearer service. PDC Packet Data supports IP to the mobile. WTP over UDP and UDP/IP provide transaction-oriented and datagram services respectively to WTP. The WAP Proxy/Server can terminate the WAE or serve as a proxy to other applications on the Internet.

### 4.4.6 WDP Profile Over iDEN

iDEN provides three data services, Short Message Service, Circuit Switched and iDEN Packet Data.. Both the Circuit Switched and Packet Data services provide IP connectivity to the mobile device. Therefore the datagram protocol used for iDEN's data bearer services is UDP. This section provides a high-level protocol architecture description of these two bearer services.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

### 4.4.6.1 iDEN Circuit-Switched Data

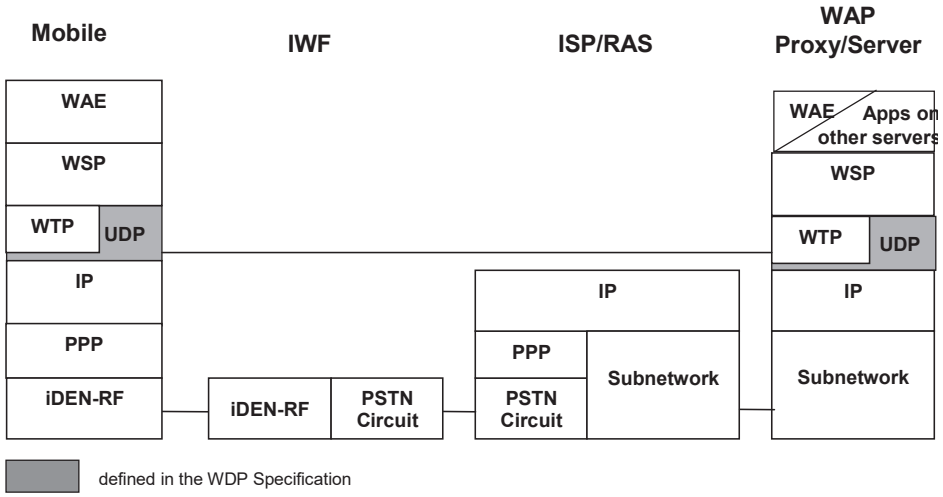



**Figure 4-21 WDP over iDEN Circuit-Switched Data Channel**

Figure 4-21 illustrates the protocol profile for the datagram layer when operating over an iDEN Circuit-Switched Data connection. The IWF provides non-transparent Circuit Switched Data services for all CSD calls within iDEN. The iDEN CSD service is very similar to the GSM CSD service. The Remote Access Server (RAS) or the Internet Service Provider (ISP) provides connectivity to the Internet network so that the mobile and WAP proxy server can address each other. The WAP Proxy/Server can terminate the WAE or serve as a proxy to other applications on the Internet.

### 4.4.6.2 iDEN Packet Data

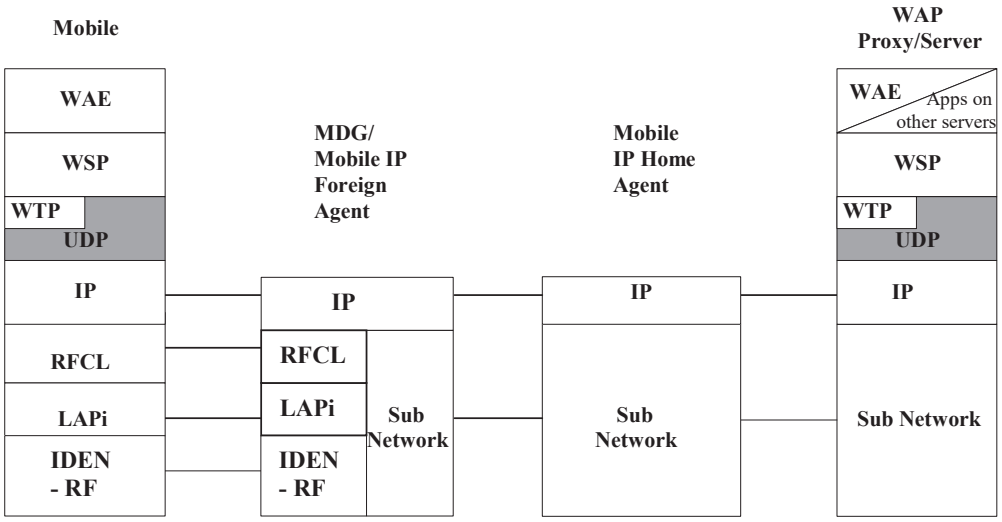



**Figure 4-22: WTP over iDEN Packet Data**

Figure 4-22 illustrates the protocol profile for the WTP layer when operating over the iDEN Packet Data bearer service. The iDEN packet data network utilises the IETF defined mobile IP tunnelling protocol to route data to the mobile device. A Home Agent router on the mobile's home network forwards datagrams to an iDEN Mobile Data Gateway. The MDG acts as a mobile IP Foreign Agent that transfers IP between the wired IP network and the wireless device via the iDEN RF protocols.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

### 4.4.7 WDP over FLEX™ and ReFLEX™

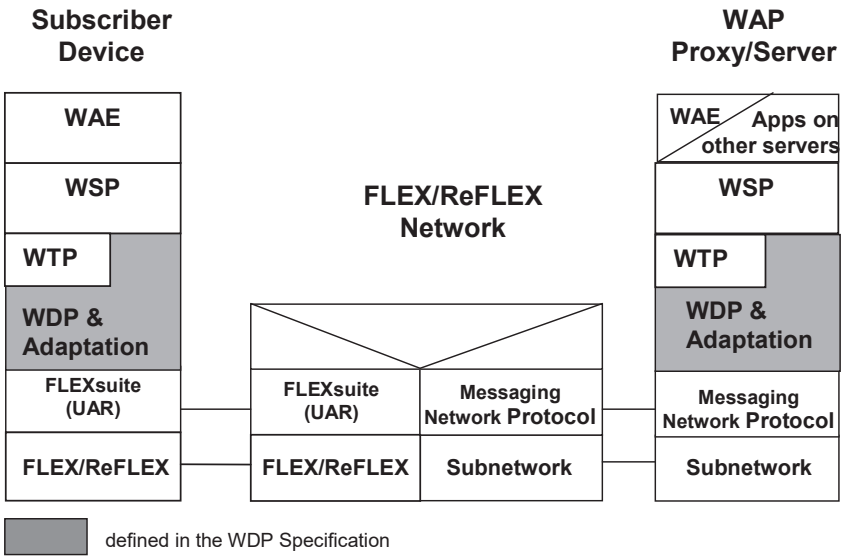



**Figure 4-23 WDP over FLEX and ReFLEX**

Figure 4-23 illustrates the protocol profile for the WDP layer when operating with the FLEX and ReFLEX paging protocols. For the communications between the FLEX/ReFLEX network and the subscriber device, WDP packets MUST be transferred using the FLEXsuite™ Uniform Addressing and Routing (UAR) protocol. (Further description of the UAR protocol can be found in Section 6.6.) The choice of network protocol used for the communications between WAP Proxy/Servers and FLEX/ReFLEX networks is negotiated between each WAP Proxy/Server and FLEX/ReFLEX network and is not specified here. The UAR protocol MAY be used to transfer the WDP packet between the FLEX/ReFLEX network and the WAP Proxy/Server. The WAP Proxy/Server MAY terminate the WAE or serve as a proxy to other applications on the Internet or other networks.

Note that ReFLEX supports message segmentation. Also note that network operators sometimes impose limits on the lengths of accepted messages. It is expected that the network operator will not limit the maximum message size to less than the minimum allowed by WTP and, therefore, no segmentation and re-assembly will be required by WDP.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

## 4.4.8 WDP over PHS

PHS is a digital cordless network, for which air interface is defined in [RCR STD-28] and CS – digital network interface is defined in [TTC JT-Q931-b], [TTC JT-Q932-a] and [TTC JT-Q921-b].

The WDP layer operates above the data capable bearer services supported by PHS. Figure 4-24 identifies the PHS bearer services presented in this specification. PHS provides Circuit-Switched Data.

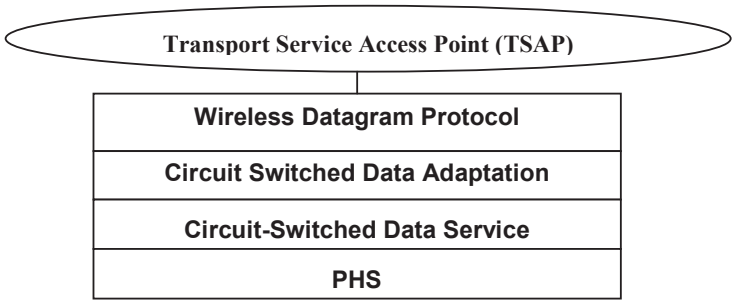



**Figure 4-24 WDP over PHS Bearer Services**

### 4.4.8.1 PHS Circuit-Switched data

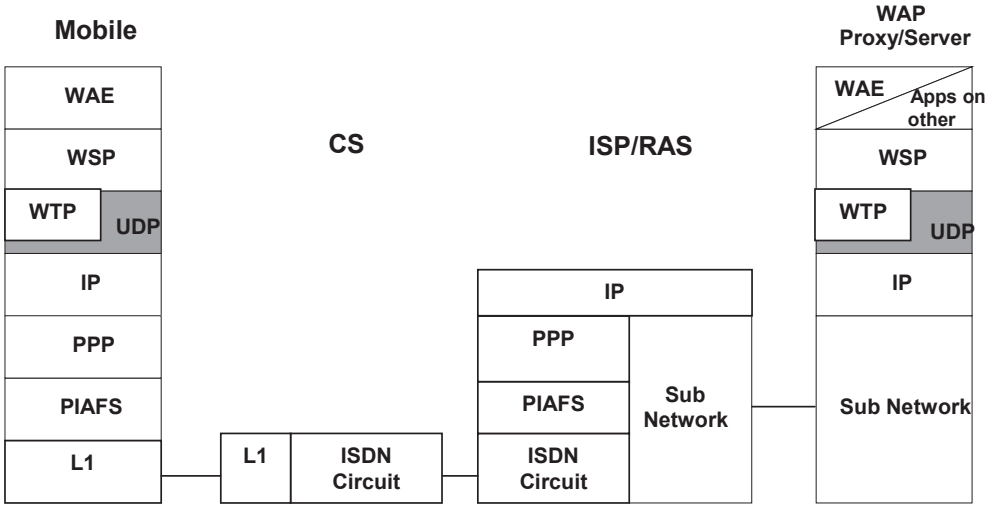



**Figure 4-25 WDP over PHS Circuit-Switched Data Channel**

Figure 4-25 illustrates the protocol profile for the WDP layer when operating over the PHS Circuit-Switched Data connection. The Internet Service Provider (ISP) Provides Internet connectivity to the Internet network so that the mobile and the WAP Proxy/Server can address each other. The WAP Proxy/Server can terminate the WAE or serve as a proxy to other applications on the Internet.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

### 4.4.9 WDP over DataTAC

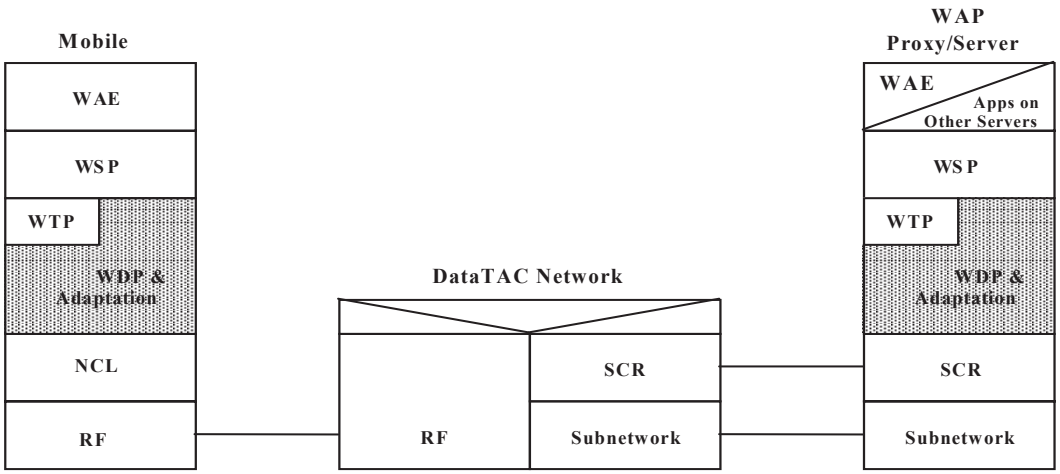



**Figure 4-26: DataTAC Profile**

Figure 4-26 illustrates the protocol profile for the WDP layer when operating over the DataTAC SCR bearer service.

### 4.4.10 WDP Profile Over TETRA

TETRA provides two data services: Short Data Service and TETRA Packet Data. The TETRA Packet Data bearer is the Internet Protocol defined in [RFC791].

#### 4.4.10.1 TETRA Short Data Service

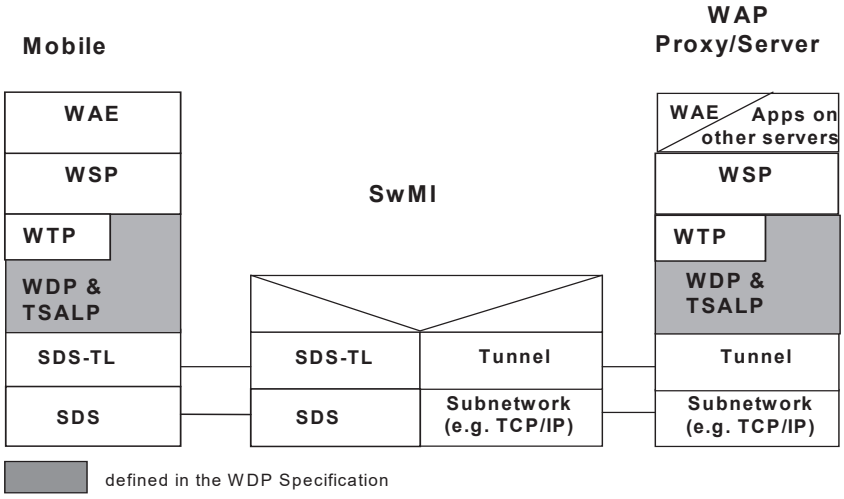



**Figure 4-27 WDP over TETRA SDS; WAP Proxy/Server is External to SwMI**

Figure 4-27 illustrates the protocol profile for the WDP layer when operating over the SDS bearer service. In this figure, the WAP Proxy/Server resides outside the SwMI. However, the WAP Proxy/Server can be also co-located with SDS node inside the SwMI.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

### 4.4.10.2 TETRA Packet Data

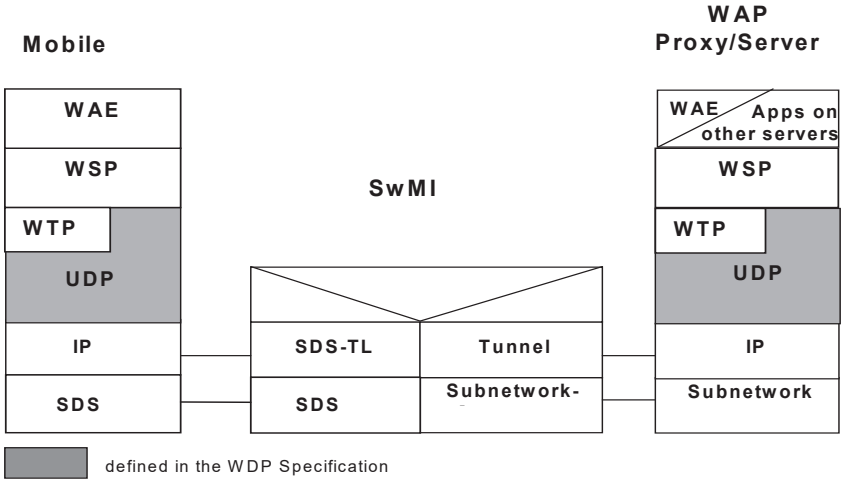



**Figure 4-28 WDP over TETRA Packet Data**

Figure 4-28 illustrates the protocol profile for WTP layer when operating over the TETRA Packet Data bearer service. The TETRA Packet Data bearer service routes IP datagrams from the mobile device to the WAP Proxy/Server and vice versa. The TETRA-specific protocols are defined in [TET 392-2].

## 4.4.11 WDP over DECT

### 4.4.11.1 DECT short message service

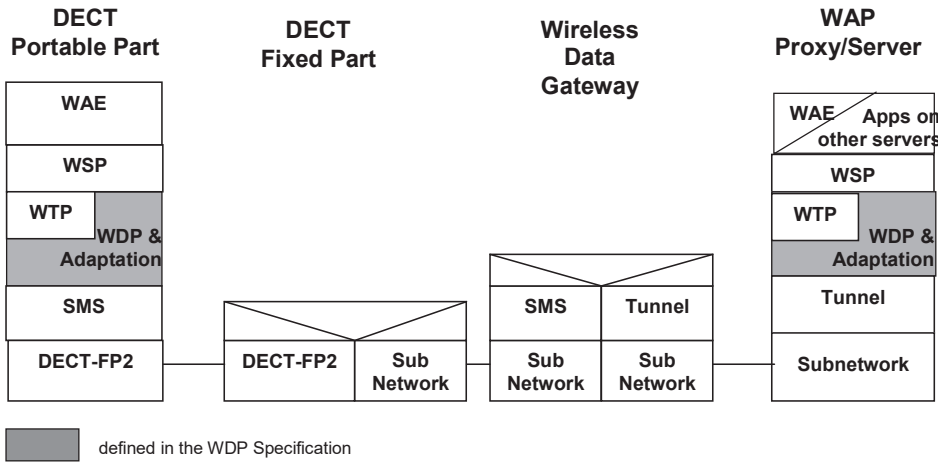



**Figure 4-29: WDP over DECT short message service.**

Figure 4-29 illustrates the protocol profile for the WDP layer when tunneling GSM-SMS over the DECT Short Message Service, as defined in [DECT-FP2]. The specifications for the adaptation layer are equal to those for GSM-SMS. Please refer to [DECT-GSM] for specification of the DECT interworking to GSM.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-SpecWAP-20030912]

### 4.4.11.2 DECT connection oriented services

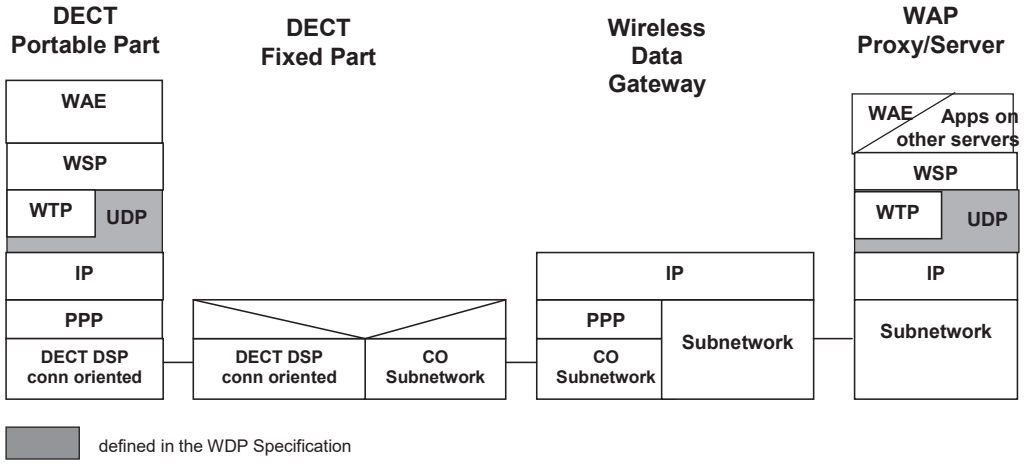



**Figure 4-30 WDP over DECT Connection Oriented Services**

Figure 4-30 illustrates the protocol profile for the WDP layer when operating over DECT connection oriented services,. The connection oriented bearer service can be provided alternatively by

- DPRS connection oriented, refer to [DPRS]
- DECT Data Service Profile D2, refer to [DECT-D2]

### 4.4.11.3 DECT packet switched services

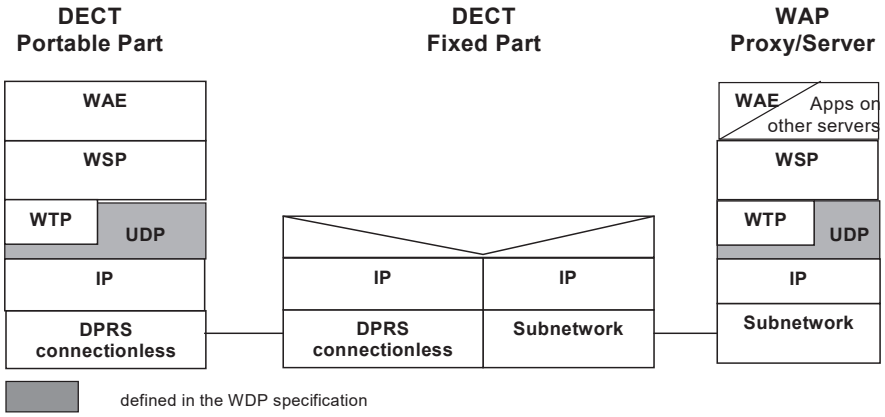



**Figure 4-31: WDP over DECT packet switched services.**

Figure 4-31 illustrates the protocol profile for the WDP layer when operating over DECT connectionless services, refer to [DPRS].

## 4.4.12 WDP over Mobitex

A WAP server gateway can connect to a Mobitex network using MPAK over a tunnel to a Mobitex Area Exchange in the Mobitex network.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

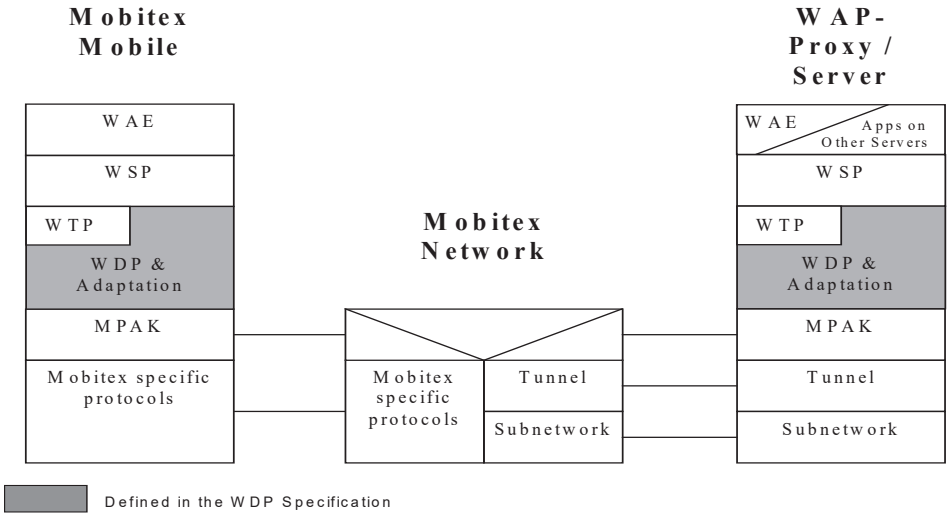



**Figure 4-32 WDP over Mobitex**

Figure 4-32 illustrates the protocol profile for the WDP layer when the WAP server gateway is connected to Mobitex.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# 5. Elements for Layer-to-layer Communication

## 5.1 Service Primitive Notation

Communications between layers and between entities within the transport layer are accomplished by means of service primitives. Service primitives represent, in an abstract way, the logical exchange of information and control between the transport layer and adjacent layers. They do not specify or constrain implementations.

Service primitives consist of commands and their respective responses associated with the services requested of another layer. The general syntax of a primitive is:

X - Generic name . Type (Parameters)

Where X designates the layer providing the service. For this specification X is

"T" for the Transport Layer.

An example of a service primitive for the WDP layer would be T-Dunitdata.Request.

Service primitives are not the same as an application programming interface (API) and are not meant to imply any specific method of implementing an API. Service primitives are an abstract means of illustrating the services provided by the protocol layer to the layer above. The mapping of these concepts to a real API and the semantics associated with a real API are an implementation issue and are beyond the scope of this specification.

## 5.2 Service Primitive Types

The primitive types used in this specification are:

**Request (.Req)**
The Request primitive type is used when a higher layer is requesting a service from the next lower layer.

**Indication (.Ind)**
The Indication primitive type is used by a layer providing a service to notify the next higher layer of activities related to the Request primitive type of the peer.

**Response (.Res)**
The Response primitive type is used by a layer to acknowledge receipt, from the next lower layer, of the Indication primitive type.

**Confirm (.Cnf)**
The Confirm primitive type is used by the layer providing the requested service to confirm that the activity has been completed (successfully or unsuccessfully).

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-SpecWAP-20030912]

# 5.3 WDP Service Primitives

## 5.3.1 General

The following notation is used in the description of the service primitives:

| Abbreviation | Meaning |
|---|---|
| M | Presence of the parameter is mandatory |
| C | Presence of the parameter is conditional |
| O | Presence of the parameter is a user option |
| * | Presence of the parameter is determined by the lower layer protocol |
| blank | The parameter is absent |
| (=) | The value of the parameter is identical to the value of the corresponding parameter of the preceding primitive |

The WDP protocol uses a single service primitive T-DUnitdata. WDP user may also receive a T-DError primitive, if the WDP protocol layer cannot execute the requested transmission.

## 5.3.2 T-DUnitdata

T-DUnitdata is the primitive used to transmit data as a datagram. T-DUnitdata does not require an existing connection to be established. A T-DUnitdata.Req can be sent to the WDP layer at any time.

| Primitive / Parameter | T-DUnitdata | | | |
|---|---|---|---|---|
| | *REQ* | *IND* | *RES* | *CNF* |
| Source Address | M | M(=) | | |
| Source Port | M | M(=) | | |
| Destination Address | M | O(=) | | |
| Destination Port | M | O(=) | | |
| User Data | M | M(=) | | |

**Destination Address**

The destination address of the user data submitted to the WDP layer. The destination address may be an MSISDN number, IP address, X.25 address or other identifier.

**Destination Port**

The application address associated with the destination address for the requested communication instance.

**Source Address**

The source address is the unique address of the device making a request to the WDP layer. The source address may be an MSISDN number, IP address, X.25 address or other identifier.

**Source Port**

The application address associated with the source address of the requesting communication instance.

**User Data**

The user data carried by the WDP protocol. The unit of data submitted to or received from the WDP layer is also referred to as the Service Data Unit. This is the complete unit (message, packet, package) of data which the higher layer has submitted to the WDP layer for transmission. The WDP layer will transmit the Service Data Unit and deliver it to its destination without any manipulation of its content.

## 5.3.3 T-DError

The T-DError primitive is used to provide information to the higher layer when an error occurs which may impact the requested service. A T-DError Indication may be issued by the WDP layer only after the higher layer has made a request to the WDP layer, such as by issuing a T-DUnitdata Request. The T-DError primitive is used when the WDP layer is unable to

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-SpecWAP-20030912]

complete the requested service due to a local problem. It is not used to inform the upper layer of networking errors external to the device/server.

An example would be if the upper layer issues a D-Unitdata Request containing an SDU which is larger than the maximum size SDU allowed by the specific WDP implementation. In this case a T-DError Indication would be returned to the upper layer with an error code indicating the SDU size is too large.

| Primitive | T-DError | | | |
|---|---|---|---|---|
| **Parameter** | ***REQ*** | ***IND*** | ***RES*** | ***CNF*** |
| Source Address | | O | | |
| Source Port | | O | | |
| Destination Address | | O | | |
| Destination Port | | O | | |
| Error Code | | M | | |

**Error Code**

An error return code carried by the D-Error primitive to the higher layer. The error codes are of local significance only.

The other parameters have the same definitions as for T-DUnitdata

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# 6. WDP Protocol Description

## 6.1 Introduction

In order to implement the WDP datagram protocol the following fields are necessary:

- Destination Port
- Source Port
- If the underlying bearer does not provide Segmentation and Reassembly the feature is implemented by the WDP provider in a bearer dependent way.

## 6.2 Mapping of WDP for IP

The User Datagram Protocol (UDP) is adopted as the WDP protocol definition for any wireless bearer network where IP is used as a routing protocol. UDP provides port based addressing and IP provides the segmentation and reassembly in a connectionless datagram service. There is no value in defining a new datagram protocol to operate over IP when the ubiquitous User Datagram Protocol (UDP) will provide the same mechanisms and functions, and is already very widely implemented. Therefore in all cases where the IP protocol is available over a bearer service the WDP Datagram service offered for that bearer will be UDP. UDP is fully specified in [RFC768] while the IP networking layer is defined in [RFC791] and [RFC2460].

The bearers defined in this specification which adopt UDP as the WDP protocol definition are:

GSM Circuit-Switched Data, GSM GPRS, ANSI-136 R-Data, ANSI-136 Circuit-Switched Data, GPRS-136, CDPD, CDMA Circuit Switched Data, CDMA Packet Data, PDC Circuit-Switched Data, PDC Packet Data, iDEN Circuit-Switched Data, iDEN Packet Data, PHS Circuit-Switched Data, TETRA Packet Data, DECT connnection oriented services and DECT packet switched services.

## 6.3 Mapping of WDP for GSM SMS, ANSI-136 GHOST and USSD

WDP bearers in the Global System for Mobile Communications (GSM) include GSM Short Message Service (GSM SMS) and GSM Unstructured Supplementary Service Data (GSM USSD).

WDP bearers in ANSI-136 include GSM Hosted SMS Teleservice (GHOST).

WDP for GSM and ANSI-136 GHOST support mandatory binary and optional text based headers. GSM USSD Phase 2 supports binary headers; GSM SMS Phase 2 and ANSI-136 GHOST support both binary and text based headers and GSM SMS Phase 1 supports text based headers.

Each packet (segment) used in the WDP protocol is identified by a User Data Header Information Element Identifier defining a port number structure located in the header of the packet. This Information Element Identifier for GSM SMS, ANSI-136 GHOST, or USSD has a similar function to the Protocol Identifier in an IP based network. The construct enables the WDP protocol to coexist with other features of the legacy bearer network.

### 6.3.1 Binary Header Format

For GSM SMS, ANSI-136 GHOST and GSM USSD the WDP headers structure is defined using the User Data Header (UDH) framework as defined in [GSM0340]: See Appendix A for more information.

### 6.3.2 Segmentation and Reassembly

The WDP segmentation is implemented as specified in [GSM0340].

Two segmentation formats, the short format and the long format have been defined. The difference between the two formats is only the range of the Datagram Reference Number. A format with only 8 bits for reference number is good enough for mobile originated communication, but in high volume applications originated at a fixed server the reference number wraps

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

around very quickly. The larger reference number range significantly lessens the risk of overlapping reference numbers, and thus incorrect reassembly.

Mobile stations may use the 8 bit or 16 bit reference number header for sending messages, but fixed devices MUST use the 16 bit reference number, unless it is known to the device that the receiver supports only 8 bit reference numbers (this distinction is an implementation matter for each fixed device manufacturer). Each implementation of the WDP MUST support reception of both 8 and 16 bit reference numbers, but a mobile implementation can be restricted to sending capability of only 8 bit reference numbers.

#### 6.3.2.1 Fragmentation Information Element (short)

The Fragmentation Information-Element (short) -Identifier is defined in [GSM0340], where it is referred to as Concatenated short messages, 8-bit reference number. The Short Information-Element –Identifier is an octet with the hex value 00.

#### 6.3.2.2 Fragmentation Information Element (long)

The Fragmentation Information-Element (long) –Identifier is defined in [GSM0340], where it is referred to as Concatenated short messages, 16-bit datagram reference number. The Long Fragmentation Information-Element -Identifier is an octet with the hex value 08.

The Long Information-Element-Data octets shall be coded as shown in Figure 6-1.

| | | |
|---|---|---|
| Octet 1 - 2 | Datagram reference number | Octet 1 contains the high part of the reference number and octet 2 the low part.<br>These octets shall contain a modulo 0xFFFF counter indicating the reference number for a particular datagram. This reference number shall remain constant for every segment which makes up a particular datagram. |
| Octet 3 | Maximum number of segments in the datagram | This octet shall contain a value in the range 1 to 255 indicating the total number of segments within the datagram. The value shall remain constant for every segment which makes up the datagram. If the value is zero then the receiving entity shall ignore the whole Information Element. |
| Octet 4 | Sequence number of the current segment | This octet shall contain a value in the range 1 to 255 indicating the sequence number of a particular segment within the datagram. The value shall start at 1 and increment by one for every segment sent within the datagram. If the value is zero or the value is greater than the value in octet 3 then the receiving entity shall ignore the whole Information Element. |

**Figure 6-1: Segmentation and Reassembly Information Element using 16 bit reference number**

#### 6.3.2.3 Port address Information Element

The Information-Element-Identifier is defined in [GSM0340].

### 6.3.3 Mapping of WDP to GSM SMS Phase 1 Text-based Headers

The text-based headers are designed as an optional method for environments that support only reduced character sets, and for example not 8 bit binary headers. This is the case for GSM phase 1 SMS, but can also be used as a generic mechanism in similar environments.

No protocol indication at a higher level is needed to indicate the presence of protocol information in the data part of the message. The first characters "//SCK" identify the WDP datagram addressing scheme to the receiving device. The header can be presented in various lengths, from 2 bytes (only destination port) to 15 bytes (containing full WDP information), in addition to the 5 bytes of "//SCK". The format of the text-based headers is defined using Backus-Naur form notation in Figure 6-2.

```
<WDP -text-socket-header> ::=
        <WDP-keyword> <WDP-port-information> [<WDP-other-header> ] <WDP delimiter>

<WDP-delimiter> ::= <space>
```

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

```
<WDP-keyword> ::= "//SCK"

<WDP-port-information> ::=
        <WDP-short-destination-address> |
        <WDP-short-destination-address> <WDP-short-source-address> |
        <WDP-short-destination-address> <WDP-short-source-address> <WDP-SAR-information> |
        "L" <WDP-long-destination-address> |
        "L" <WDP-long-destination-address> <WDP-long-source-address> |
        "L" <WDP-long-destination-address> <WDP-long-source-address> <WDP-SAR-information>

<WDP-other-header> ::= <header-expansions-starting-with-// >

<WDP-short-destination-address> ::= <common-hex-digit> <common-hex-digit>
        ; Destination WDP port in ASCII coded hexadecimal [00..FF, or 00..FFFF].
        ; When the truncated port presentation is used (only destination port),
        ; then the source port of the message is defaulted to be the same as the destination port.'

<WDP-short-source-address> ::= <common-hex-digit> <common-hex-digit>
        ; Source WDP port in ASCII coded hexadecimal [00..FF], i.e., decimal [0..255].'

<WDP-long-destination-address> ::=
        <common-hex-digit> <common-hex-digit> <common-hex-digit> <common-hex-digit>
        ; Destination WDP port in ASCII coded hexadecimal [0000..FFFF] , i.e., decimal [0..65535].'

<WDP-long-source-address> ::=
        <common-hex-digit> <common-hex-digit> <common-hex-digit> <common-hex-digit>
        ; Source WDP port in ASCII coded hexadecimal [0000..FFFF] , i.e., decimal [0..65535].

<WDP-SAR-information> ::=
        <WDP-SAR-reference> <WDP-SAR-total-segments> <WDP-SAR-current-segment>

<WDP-SAR-reference> ::= <common-hex-digit> <common-hex-digit>
        ; Concatenated message reference number in ASCII coded hexadecimal [00..FF], i.e., decimal [0..255].'

<WDP-SAR-total-segments> ::= <common-hex-digit> <common-hex-digit>
        ; 'Concatenated message total segment count in ASCII coded hexadecimal [01..FF], i.e., decimal [1..255].'

<WDP-SAR-current-segment> ::= <common-hex-digit> <common-hex-digit>
        ; 'Concatenated message segment index in ASCII coded hexadecimal [01..FF], i.e., decimal [1..255].'
```

**Figure 6-2: Definition of WDP headers in text format**

The text based header is always terminated with a space (" ") character. This allows for future enhancements to the protocol.

Devices not supporting the concatenation should not put dummy values into the header, as they can be misinterpreted and consume valuable bandwidth. Instead they shall truncate the header and omit the Segmentation and Reassembly part of the header

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| "/" | | | | | | | |
| "/" | | | | | | | |
| "S" | | | | | | | |
| "C" | | | | | | | |
| "K" | | | | | | | |
| "L" | | | | | | | |
| Destination port MSB (High hex)<br>Destination port MSB (Low hex) | | | | | | | |
| Destination port LSB (High hex)<br>Destination port LSB (Low hex) | | | | | | | |
| Originator Port MSB (High hex)<br>Originator Port MSB (Low hex) | | | | | | | |
| Originator Port LSB (High hex)<br>Originator Port LSB (Low hex) | | | | | | | |
| Reference number (High hex) | | | | | | | |
| Reference number (Low hex) | | | | | | | |
| Total number of *segment*s (High hex) | | | | | | | |
| Total number of *segment*s (Low hex) | | | | | | | |
| Segment count (High hex) | | | | | | | |
| Segment count (Low hex) | | | | | | | |
| <space> | | | | | | | |
| 1 - n 7-bit characters of User Data | | | | | | | |
| | | | | | | | |

**Figure 6-3: Example of a WDP header for compatibility with legacy GSM networks**

### 6.3.4 Mapping of WDP to GSM USSD

GSM USSD adaptation layer is specified in WAP WDP Implementation Companion document, see [WAPGSMUD].

## 6.4 Mapping of WDP for ANSI-136 GUTS/R-Data

ANSI-136 GUTS is used to support UDP datagrams on ANSI-136 R-Data. GUTS adds a one octet protocol discriminator and message type to the UDP header. Port address information is assumed to be carried within the UDP header. Segmentation and reassembly can be optionally provided by the ANSI-136 Simplified Segmentation and Reassembly (SSAR) layer between GUTS and R-Data. IP address and routing information is specified within the R-Data layer when using GUTS.

## 6.5 Mapping of WDP to CDMA SMS

WDP sends datagrams in the User Data subparameter of IS-637 SMS point-to-point messages. A datagram consists of a four-byte header followed by the data.

Because some datagrams may be too long to fit in one SMS message, a datagram can be segmented, sent in several SMS messages, and reassembled at the destination. [TIAEIA-637] does not define segmentation and reassembly procedures, so they are defined in this document.

SMS messages containing WDP datagrams MUST use the WAP teleservice, which is defined in [TIAEIA-637].

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

### 6.5.1 Datagram Structure

A WDP datagram containing N bytes of data sent over IS-637 SMS has the following structure:

| Field | Length (bits) |
|---|---|
| SOURCE_PORT | 16 |
| DESTINATION_PORT | 16 |
| DATA | N * 8 |

### 6.5.2 SMS User Data

The CHARi fields of the User Data subparameter in a WDP SMS message contain one segment of a WDP datagram. The structure of the CHARi fields is as follows:

| Field | Length (bits) |
|---|---|
| MSG_TYPE | 8 |
| TOTAL_SEGMENTS | 8 |
| SEGMENT_NUMBER | 8 |
| DATAGRAM | (NUM_FIELDS – 3) * 8 |

**MSG_TYPE** **Message Type**

This field shall be set to '00000000', to indicate that this is a WDP message. This field distinguishes WDP messages from other WAP messages such as WCMP messages.

**TOTAL_SEGMENTS** **Total Number of Segments**

The entity performing segmentation for the IS-637 SMS bearer shall set this field to the total number of segments that make up the datagram being delivered. This field shall not be set to ‘00000000’.

**SEGMENT_NUMBER** **Segment Number**

The entity performing segmentation for the IS-637 SMS bearer shall set this field to the segment number for this segment of the datagram. In the first segment of a datagram this field shall be set to ‘00000000’. In each subsequent segment, SEGMENT_NUMBER shall increase by 1.

**DATAGRAM** **Datagram bytes**

The entity performing segmentation for the IS-637 SMS bearer shall fill this field with the datagram bytes in this segment of the datagram. The NUM_FIELDS field of the User Data subparameter shall be set to the number of datagram bytes in the segment plus 3. If SEGMENT_NUMBER is not ‘00000000’, the number of datagram bytes in this segment of the message shall not be greater than the number of bytes in the preceding segment.

### 6.5.3 Use of MESSAGE_ID Field

When sending a WDP datagram in an IS-637 SMS message, the IS-637 SMS endpoint MUST set the MESSAGE_ID field of the Message Identifier subparameter as follows:

- If this SMS message contains the first segment of the first WDP datagram sent after the IS-637 SMS endpoint has restarted, the endpoint MUST set MESSAGE_ID equal to a random number in the range 0 through 65535.
- Otherwise, if this SMS message contains the first segment of a WDP datagram, the endpoint MUST increment the MESSAGE_ID value from the last WDP datagram sent, modulo 65536, to generate the MESSAGE_ID field for the SMS message.
- A message centre terminating the IS-637 SMS protocol MAY use as MESSAGE_ID a message reference number provided via a short message entity interface protocol. A suitable reference number is, for example, the ‘sar_msg_ref_num’ in [WDPWCMPAdapt]. However, if no reference number is provided, the message centre MUST set the value of MESSAGE_ID according to the rules described in this section.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

- If the SMS message does not contain the first segment of a WDP datagram, the endpoint MUST set the MESSAGE_ID field equal to the MESSAGE_ID field from the SMS message containing the first segment of the WDP datagram.

### 6.5.4 Segmentation and Reassembly

Segmentation and reassembly of a datagram use five parameters in a WAP SMS message: the Originating Address parameter from the SMS Transport Layer, MESSAGE_ID from the SMS Message Identifier subparameter, MSG_TYPE, TOTAL_SEGMENTS, and SEGMENT_NUMBER.

MSG_TYPE identifies WAP messages containing WDP datagrams. The Originating Address and MESSAGE_ID together identify a datagram. TOTAL_SEGMENTS and SEGMENT_NUMBER are used to verify that a complete datagram has been received and is ready to be passed to a higher layer.

### 6.5.5 Segmentation Example

Figure 6-4 shows an example of a WDP Datagram that is sent in two IS-637 SMS Point-to-Point messages. The datagram has been broken into two segments, which are contained in the CHARi fields in the User Data subparameters of the messages (only the second SMS message is shown).

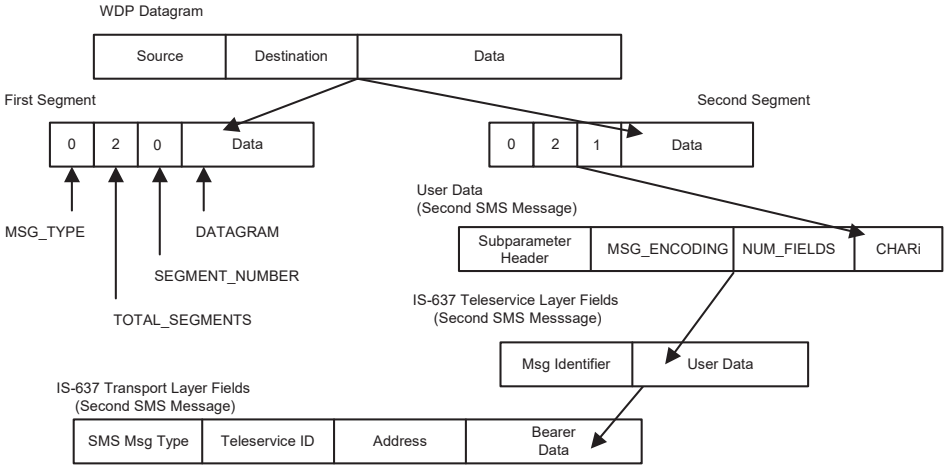



**Figure 6-4 Example of Segmentation**

## 6.6 Mapping of WDP to FLEX™ and ReFLEX™

In FLEX and ReFLEX systems, the WDP packet MUST be carried over the air in a FLEXsuite™ Uniform Addressing and Routing (UAR) protocol message. In this application, the UAR protocol is used to make the WDP packet transparent to the FLEX/ReFLEX protocol stacks (see Section4.4.7). The simplest and most likely implementation is a UAR protocol message composed of a UAR header, a content type, and a WDP packet.

| Field | WDP Usage |
|---|---|
| UAR Header | M |
| TO Address | O |
| FROM Address | O |
| Content Type | [application/x-wap.wdp] |
| Cyclic Redundancy Check | O |
| Data | WDP packet |

**Figure 6-5 Fields for FLEXsuite UAR protocol.**

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

The length of the **UAR Header** is one byte. It is used to identify the FLEXsuite message as a UAR message.

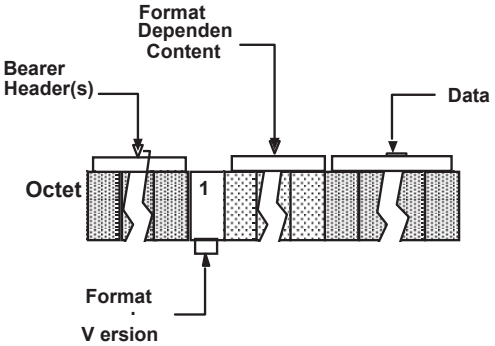
The **TO Address** and **FROM Address** fields MAY be used in systems with more than one WAP Proxy/Server. The content of the TO and FROM address fields is specific to the network protocol used between the WAP Proxy/Server and the FLEX/ReFLEX network. In UAR protocol messages that are being sent from the wireless device, the **TO Address** field MAY be specified to allow for more than one WAP proxy/gateway to be unambiguously identified. Conversely, in UAR protocol messages that are being sent to a wireless device, the **FROM Address** field MAY be specified to allow for more than one WAP proxy/gateway to be unambiguously identified.

The **Content Type** field identifies that the UAR Data field contains a WDP packet.

The **Cyclic Redundancy Check** is optional and helps to detect errors in the **UAR Header**, **TO Address**, **FROM Address**, and **Content Type** fields.

## 6.7 Mapping of WDP to DataTAC

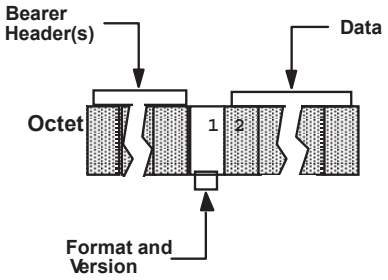
The generic WDP header format for DataTAC uses bit fields within octets. The bit fields are numbered from left to right with zero as the high order bit. The generic WDP header format for DataTAC is shown both graphically and in the table below:




| Octet(s) | Field name | Field description | Comments |
|---|---|---|---|
| | Bearer Header(s) | Any headers required by the Bearer Protocols | In a DataTAC system these include: Application, Native Command Language, DataTAC Messaging, RF and Standard Context Routing |
| 1 | Format and Version | Identifies the adaptation layer protocol format and version | A single octet binary field containing two bit fields The first field uses bits 0 through 3 to define the format. The second field uses bits 4 through 7 to define the version. |
| | Format Dependent Content | An optional content that carries WDP information that is not available in the standard bearer protocol headers. | A variable length field dependent on the Format and Version octet. |
| | Data | Contains the User Data | User specified text or binary information |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

The WDP header with the Format bits set to binary 0000 and the Version bits set to binary 0000 is shown both graphically and in the table below:



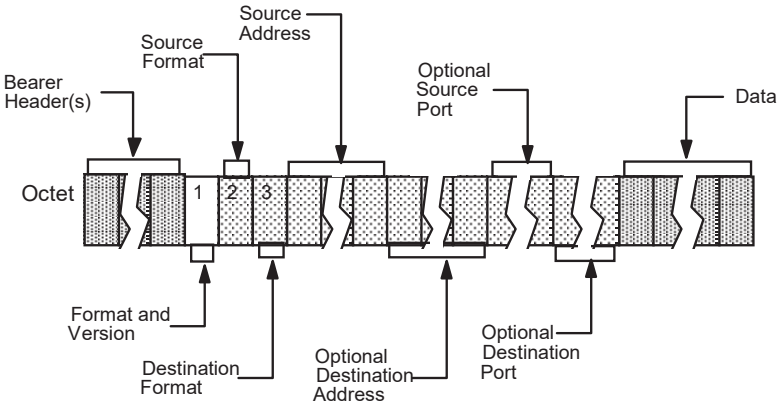

| Octet(s) | Field name | Field description | Comments |
|---|---|---|---|
| | Bearer Header(s) | Any headers required by the Bearer Protocols | In a DataTAC system these include: RF, Application, Standard Context Routing, DataTAC Messaging |
| 1 | Format and Version | Identifies the adaptation layer protocol format and version | Set bits to 0000 0000 (0x00) |
| 2 - ~ | Data | Contains the User Data | User specified text or binary information. The adaptation layer will log the received data. |

NOTES:

1. Format: 0000, Version: 0000 is reserved. The adaptation layer should log any received data and then discard the packet.
2. There is no Format Dependent Content.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

The WDP header with the Format bits set to binary 0001 and the Version bits set to binary 0000 is shown both graphically and in the table below:




| Octet(s) | Field name | Field description | Comments |
|---|---|---|---|
| | Bearer Header(s) | Any headers required by the Bearer Protocols | In a DataTAC system these include: RF, Application, Standard Context Routing, DataTAC Messaging |
| 1 | Format and Version | Identifies the adaptation layer protocol format and version | Set bits to 0001 0000 (0x10) |
| 2 | Source Format | Identifies the source address and port | A single-octet binary field containing two bit fields.<br><br>The Source Address Format field uses bits 0 through 3 as follows:<br>0000 = Extended<br>0001 = IPv4<br>0010 = IPv6<br>0011 = X.121<br>0100 = DataTAC LLI-4<br>0101 = DataTAC LLI-7<br>1111 = From Bearer Header(s)<br><br>The Source Port Format field uses the remaining four bits as follows:<br>0000 = Extended-1<br>0001 = Extended-2<br>0010-1100 = Table Lookup<br>1111=From Bearer Header(s) |
| 3 | Destination Format | Identifies the destination address and port | The bit field definitions for Destination Address Format and Destination Port Format match those in the Source Format field (Octet 2) |
| | Optional Source Address | Identifies, if required, an optional source address | An optional, variable-length field dependent on the Source Address Format (Octet 2) field values:<br>0000=An Address Type octet |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

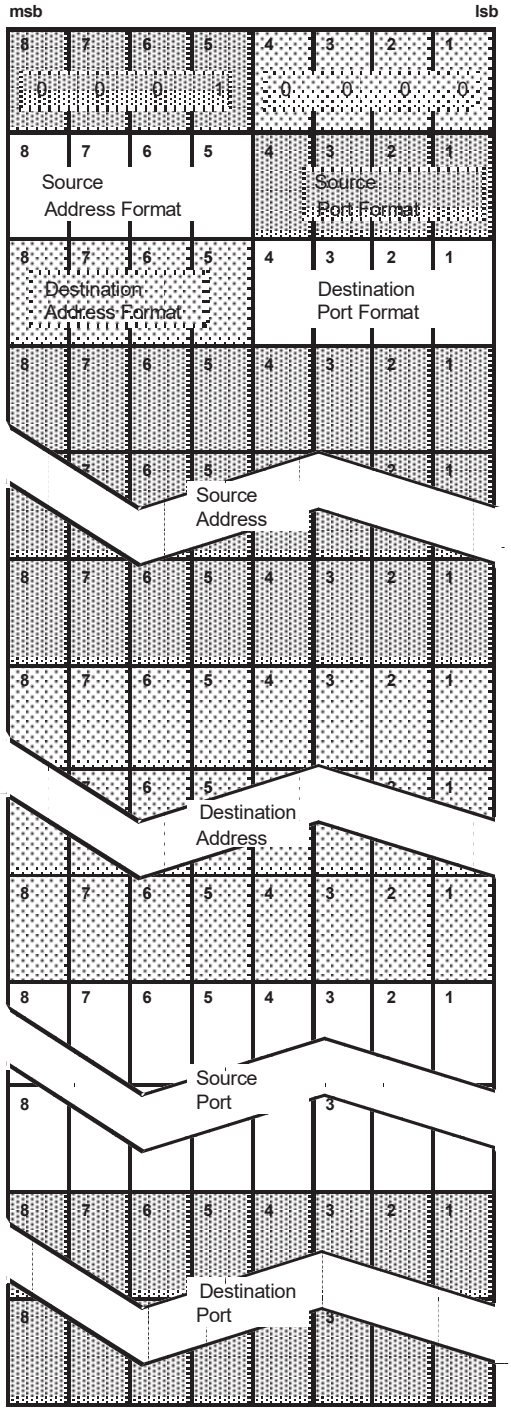
| Octet(s) | Field name | Field description | Comments |
|---|---|---|---|
| | | | followed by the address.<br>0001 = An IPv4 address<br>0010 = An IPv6 address<br>0011 = An X.121 address<br>0100 = A 4-octet DataTAC LLI<br>0101 = A 7-octet DataTAC LLI<br>0110-1111 = Field not included |
| | Optional Destination Address | Identifies, if required, an optional destination address | Refer to Optional Source Address; dependent on the Destination Address Format (Octet 3) field values |
| | Optional Source Port | Identifies, if required, an optional source port | An optional variable-length field dependent on the Source Port Format (Octet 2) field values:<br>0000 = A one octet binary port<br>0001 = A two octet binary port<br>0010-1111 = Field not included |
| | Optional Destination Port | Identifies, if required, an optional destination port | Refer to Optional Source Port; dependent on the Destination Port Format (Octet 3) values |
| | Data | Contains the User Data | User-specified text or binary information |

NOTES:

1. Format: 0001 Version: 0000 does not provide packet segmentation (i.e. this is a single-segment packet as far as WDP is concerned).
2. If a table lookup port is specified the adaptation layer will access a local table to determine the actual port. This mechanism can be used, for example, to store the WAP port numbers

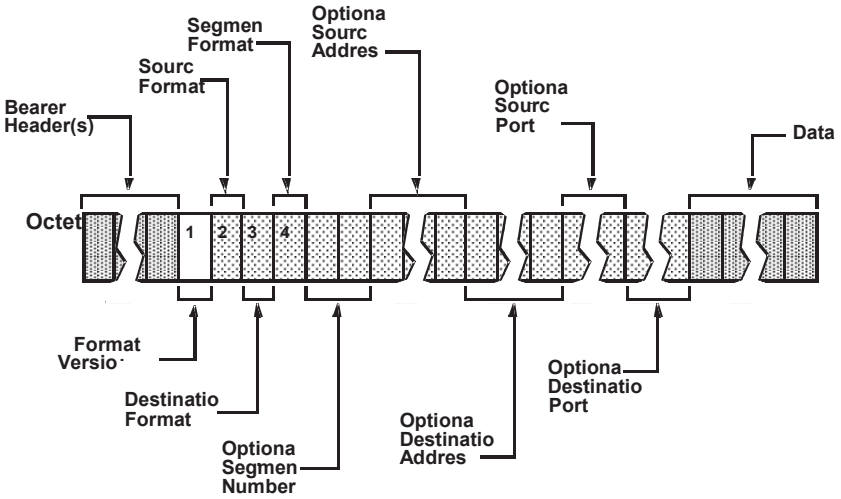
© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

The WDP header bit fields, with the Format bits set to binary 0001 and the Version bits set to binary 0000, are shown graphically below:




© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

The WDP header with the Format bits set to binary 0010 and the Version bits set to binary 0000 is shown both graphically and in the table below:




| Octet(s) | Field name | Field description | Comments |
|---|---|---|---|
| | Bearer Header(s) | Any headers required by the Bearer Protocols | In a DataTAC system these include: RF, Application, Standard Context Routing, DataTAC Messaging |
| 1 | Format and Version | Identifies the adaptation layer protocol format and version | Set bits to 0010 0000 (0x20) |
| 2 | Source Format | Identifies the source address and port | Refer to Format:0001, Version: 0000, Octet 2 |
| 3 | Destination Format | Identifies the destination address and port | Refer to Format:0001, Version: 0000, Octet 3 |
| 4 | Segment Format | Identifies the format used for packet segmentation | A single-octet binary field containing three bit fields.<br><br>The More Bit field uses bit 0 as follows:<br>0 = no more segments to come<br>1 = more segments to come<br><br>The Packet Segment Number field uses bits 1 through 3 as follows:<br>000 = Extended<br>001-111 = Segment numbers 1 through 7<br><br>The Packet Number field uses the remaining four bits as follows:<br>0000 = Reserved<br>0001-1111 = Packet numbers 1 through 15 |
| | Optional Segment Number | Identifies, if required, an optional packet segment number | An optional two-octet field dependent on the Packet Segment Number field values of the Segment Format (Octet 4):<br>000 = A two-octet binary packet segment number<br>001-111 = Field not included |
| | Optional Source Address | Identifies, if required, an optional source address | Refer to Format:0001 Version: 0000 |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

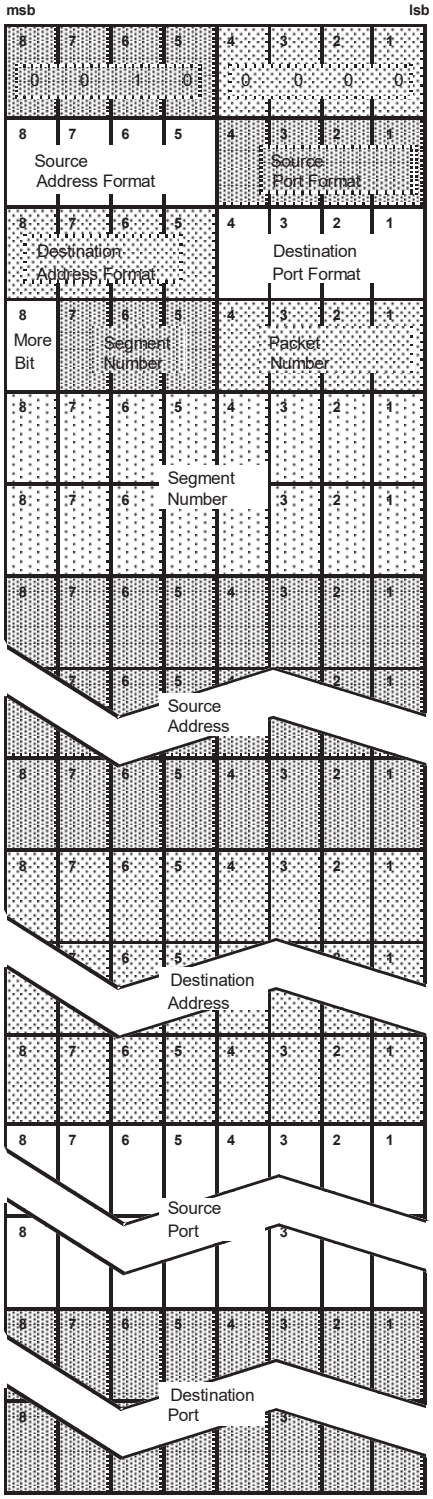
| Octet(s) | Field name | Field description | Comments |
|---|---|---|---|
| | Optional Destination Address | Identifies, if required, an optional destination address | Refer to Format:0001 Version: 0000 |
| | Optional Source Port | Identifies, if required, an optional source port | Refer to Format:0001 Version: 0000 |
| | Optional Destination Port | Identifies, if required, an optional destination port | Refer to Format:0001 Version: 0000 |
| | Data | Contains the User Data | User specified text or binary information |

NOTES:

If a table lookup port is specified the adaptation layer will access a local table to determine the actual port. This mechanism can be used, for example, to store the WAP port numbers.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

The WDP header fields with the Format bits set to binary 0010 and the Version bits set to binary 0000 are shown graphically below:

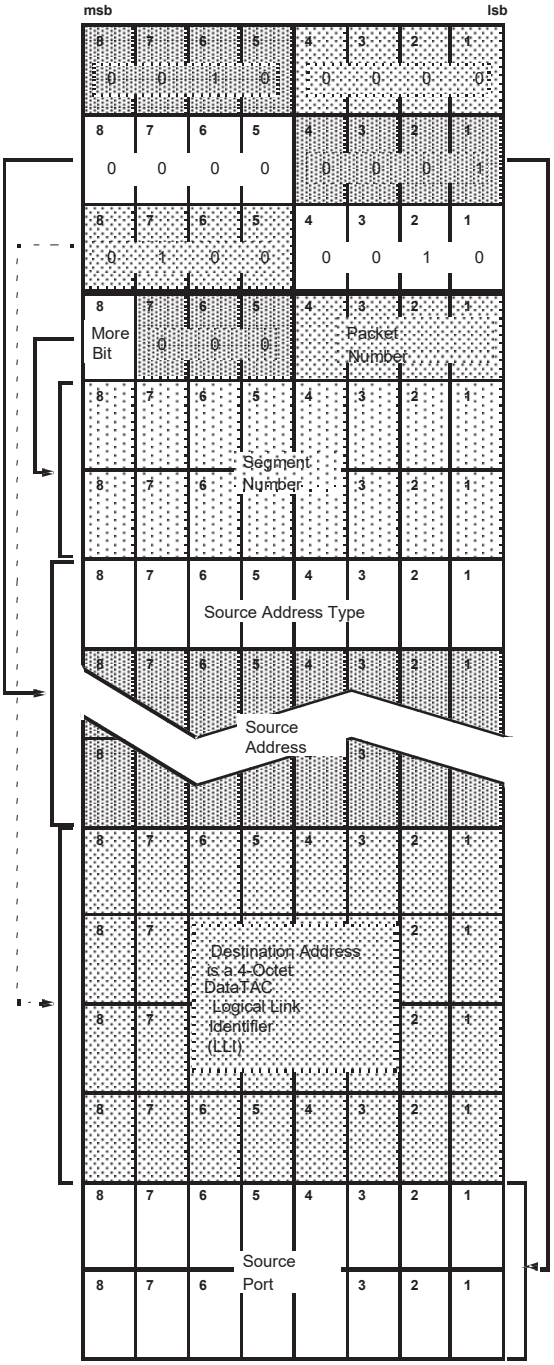



© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

An example of the WDP header with Format bits set to binary 0010 and the Version bits set to 0000 is shown below. This example is provided simply to demonstrate how some of the extensible fields may be used and is not intended to represent any specific implementation of WAP over DataTAC.

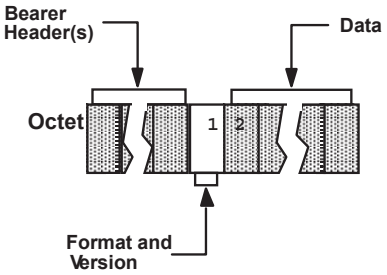
In this example, an extended source address type is used with a two-byte source port. The destination address is a 4-byte DataTAC LLI and the destination port is obtained from a table-lookup algorithm to be defined within the WDP adaptation layer. An extended segment numbering scheme is used with a two-byte segment number.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.




The WDP header with the Format bits set to binary 0100 and the Version bits set to binary 0000 is shown both graphically and in the table below:

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.



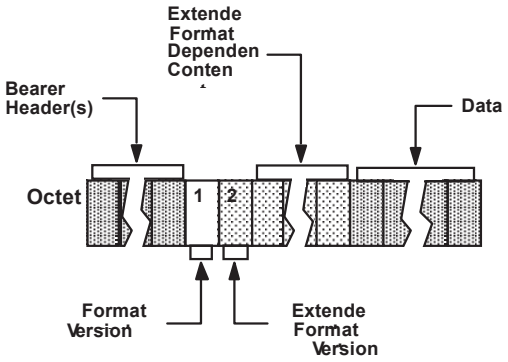

| Octet(s) | Field name | Field description | Comments |
|---|---|---|---|
| | Bearer Header(s) | Any headers required by the Bearer Protocols | In a DataTAC system these include: RF, Application, Standard Context Routing, DataTAC Messaging |
| 1 | Format and Version | Identifies the adaptation layer protocol format and version | Set bits to 0100 0000 (0x40) |
| 2 - ~ | Data | Contains the User Data | User specified text or binary information |

NOTES:

1. There is no Format Dependent Content
2. This format may be used to intercept DataTAC '@nn' infrastructure signals. Applications that use the '@nn' format are also supported provided a minimal adaptation layer exists and the port and address mappings are static.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

The WDP header with the Format bits set to binary 1111 and the Version bits set to binary 0000 is shown both graphically and in the table below:




| Octet(s) | Field name | Field description | Comments |
|---|---|---|---|
| | Bearer Header(s) | Any headers required by the Bearer Protocols | In a DataTAC system these include: Application, Native Command Language, DataTAC Messaging, RF and Standard Context Routing |
| 1 | Format and Version | Identifies the adaptation layer protocol format and version | Set bits to 1111 0000 (0xF0). This format indicates that an Extended Format and Version field is present. |
| 2 | Extended Format and Version | Identifies the adaptation layer protocol extended format and version | A single-octet binary field containing two bit fields.<br><br>The Extended Format field uses bits 0 through 3<br><br>The Extended Version field uses the remaining four bits |
| | Extended Format Dependent Content | An optional content that carries WDP information that is not available in the standard bearer protocol headers. | A variable-length field dependent on the Extended Format and Version octet. |
| | Data | Contains the User Data | User specified text or binary information |

## 6.8 Mapping of WDP to GSM Cell Broadcast

### 6.8.1 Binary Header Format

WDP over GSM Cell Broadcast uses the binary User Data Header (UDH) framework as defined in [GSM0340] to provide port level addressing. A WDP entity receiving a CBS message in which the data encoding is set to 8-bit data must assume the existence of a User Data Header in the message.

### 6.8.2 Source and Destination Port Addressing

WDP over GSM Cell Broadcast uses the 8 or 16 bit address application port addressing scheme as defined in [GSM0340] to provide port level addressing.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

### 6.8.3 Segmentation and Reassembly

The GSM CBS message comprises of 82 octets of user data. Concatentation of up to 15 CBS messages, where supported in the GSM network, is handled via the GSM macro-message as described in [GSM0341].

The Concatenated short messages (0x00) and (currently proposed) Enhanced Concatenated short messages (0x08) Information Element Identifiers should not be used for WAP formatted messages over GSM Cell Broadcast. A WDP entity should ignore any CBS message received which contains either of these Information Element Identifiers relating to concatenation.

## 6.9 Mapping of WDP to TETRA SDS

The TETRA SDS Adaptation Layer Protocol (TSALP) is designed for transmitting WDP datagrams over the TETRA SDS bearer [TET SDSTL]. The basic function of the TSALP is to map the WDP protocol onto the underlying SDS bearer making the Short Data Service transparent for the WAP protocol stack. The TSALP is limited in scope; it does not provide end-to-end data reliability, flow control, or sequencing, however, it optionally provides a segmentation mechanism.

Figure 6-6 shows the TSALP header format.

| Bit/Octet | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 1 | Length of Header | | | | | a | b | sar |
| 2 | Destination Port (High) | | | | | | | |
| 3 | Destination Port (Low) | | | | | | | |
| 4 | Source Port (High) | | | | | | | |
| 5 | Source Port (Low) | | | | | | | |
| 6 | Datagram Reference Number | | | | | | | |
| 7 | Number of Segments | | | | Segment Count | | | |
| 8 | User Data (up to 249 octets) | | | | | | | |

**Figure 6-6 Format of the TSALP header**

The **Length of Header** field specifies the length of the TSALP header starting from the following octet; the Length of Header field itself is excluded from the count. The length of header is measured in octets.

The bits **a** and **b** are reserved for future use.

The **sar** bit field indicates whether the SAR is used or not. When a datagram is sent in segments, the TSALP sets sar bit to one and appends the header fields controlling the SAR (Datagram Reference Number, Number of Segments and Segment Count). If the original datagram fits into a single packet, the sar field must be set zero, and consequently, the header fields used for SAR should not be included in the header.

The **Destination** and **Source Port** fields contain port numbers received from the service user in the request primitive.

The following three fields are optional elements of the TSALP header. When the size of a datagram exceeds the maximum size of the user data that can be sent in a single TSALP message, the sender sets the sar bit to one and appends the SAR-controlling fields to the header to communicate SAR information to the destination.

The **Datagram Reference Number** field resolves the problem with duplicate, dropped, and out of order packet delivery when SAR is used. The Datagram Reference Number is a modulo 0xFFFF counter that the TSALP increments for each outgoing datagram. When the TSALP segments a datagram it copies the Datagram Reference Number field into each segment. When segment arrives, the destination uses this field along with the source address to identify the datagram.

The **Number of Segments** field indicates the total number of segments within the datagram. This octet shall contain a value in the range 2 to 15. When the TSALP segments a datagram it copies the number of segments field into each segment. The destination uses this field along with the segment count field for reassembling the original datagram.

The **Segment Count** field specifies the position of the segment in the sequence starting at one. This octet shall contain a value in the range 1 to 15. To reassemble the datagram, the TSALP must receive all segments starting with segment that has

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-SpecWAP-20030912]

segment count one through the segment with the segment count that equals the value indicated in the Number of Segments field.

The **User Data** field contains user data received from the WDP. The length of this field varies depending on the used TETRA link and the presence of the header fields controlling SAR. The maximum size, 249 octets, can be achieved over the TETRA advanced link with no SAR used. However, if the datagram is segmented and sent over the TETRA basic link, the maximum size is limited to 120 octets.

## 6.10 Mapping of WDP for Mobitex

The following sections show the mapping of WDP for Mobitex, designed for transmitting WDP datagrams over the Mobitex bearer [Mobitex]. This protocol provides a segmentation and reassembly mechanism. It does not however provide retransmission capabilities for lost frames.

If user data that arrives from an upper layer fits into one MPAK, Short Datagram Format MUST be used.

If user data that arrives from an upper layer does not fit into one MPAK it MUST be segmented, and then reassembled at the destination. A Long Datagram consists of two or more Segments. Each MPAK, by this definition thus contains one Segment.

### 6.10.1 Short Datagram Format

If user data that arrives from an upper layer fits into one MPAK, Short Datagram Format MUST be used. SAR bit MUST be set to 0.

**Note!** Bit 0 is MSB and bit 7 is LSB.

| Short Datagram Format | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octet | MSB 0 | 1 | 2 | 3 | 4 | 5 | 6 | LSB 7 |
| 1 | SAR (0) | C | B | A | Version (0x0) | | | |
| 2 | Destination Port (High) | | | | | | | |
| 3 | Destination Port (Low) | | | | | | | |
| 4 | Source Port (High) | | | | | | | |
| 5 | Source Port (Low) | | | | | | | |
| 6<br>.<br>. | User Data (Up to 507 octets, i.e. 512-5)<br>.<br>. | | | | | | | |

**Figure 6-7 Short Datagram Format**

The **Version** field specifies the version of the Mobitex Adaptation Layer Protocol. The first version of the protocol uses version number 0x0. If the version number separates from 0x0, a WCMP message (Parameter problem) SHOULD be generated to the sender.

**Bit set (A, B, C)** – see section 6.10.4.

The **Destination** and **Source Port** fields contain the port numbers received from the service user in the request primitive.

The **SAR** bit in this case indicates that segmentation is not needed (SAR=0) and consequently, the user data follows immediately after the Destination and Source Port fields.

### 6.10.2 Long Datagram Format

**Note!** Bit 0 is MSB and bit 7 LSB.

| Long Datagram Format |
|---|

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

| Octet | MSB 0 | 1 | 2 | 3 | 4 | 5 | 6 | LSB 7 |
|---|---|---|---|---|---|---|---|---|
| 1 | SAR (1) | C | B | A | Version (0x0) | | | |
| 2 | Destination Port (High) | | | | | | | |
| 3 | Destination Port (Low) | | | | | | | |
| 4 | Source Port (High) | | | | | | | |
| 5 | Source Port (Low) | | | | | | | |
| 6 | Datagram Reference Number (High) | | | | | | | |
| 7 | Datagram Reference Number (Low) | | | | | | | |
| 8 | Number of Segments | | | | | | | |
| 9 | Segment Count | | | | | | | |
| 10<br>.<br>. | User Data (Up to 503 octets, i.e. 512-9)<br>.<br>. | | | | | | | |

**Figure 6-8 Long Datagram Format**

The **SAR** bit in this case, Long Datagram Format, indicates that Segmentation and Reassembly MUST be used.

**Note!** If the datagram to be segmented is more than 4 kByte long, the separate segments to the addressed mobile need to be paced to account for the difference in data rate between the radio link and the gateway connection to the network.

**Bit set (A, B, C) –** see section 6.10.4.

The **Datagram Reference Number** field contains the value of a modulo 0xFFFF counter that is incremented each time a new datagram is sent using SAR to a specific destination. The counter is incremented individually for each destination.

The **Number of Segments** field contains the total number of segments included in the datagram, 2 - 255 (or 0x02 - 0xFF). This information is copied into each segment sent. This field is used when reassembling the segmented datagram.

The **Segment Count** field specifies which segment of the datagram is contained in the MPAK, 1 - 255 (or 0x01 - 0xFF). The segment count starts at 1 for a new datagram and is incremented for each new segment.

### 6.10.3 Long Datagram Format with Space Saving Function (SSF)

When using SSF the first segment follows the ordinary Long Datagram Format. The 2nd to Nth segment headers are specified in Figure 6-9.

| **Long Datagram Format with SSF– 2nd to nth segment** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octet | MSB 0 | 1 | 2 | 3 | 4 | 5 | 6 | LSB 7 |
| 1 | SAR (1) | C (1) | B (1) | A (0) | Version (0x0) | | | |
| 2 | Datagram Reference Number (High) | | | | | | | |
| 3 | Datagram Reference Number (Low) | | | | | | | |
| 4 | Segment Count | | | | | | | |
| 5<br>.<br>. | User Data (Up to 508 octets, i.e. 512-4)<br>.<br>. | | | | | | | |

**Figure 6-9 Long Datagram Format with SSF – 2nd to Nth segment**

### 6.10.4 Bit Set for Datagram

**Sending a Short or a Long Datagram without SSF implemented**

The A, B and C bits are not used, but should be set to zero when being sent and ignored at reception.

**Sending a Short or a Long Datagram with SSF implemented**

Unknown if the Destination supports SSF:

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

As long as it is unknown whether the destination supports SSF, **C** MUST be set to 0, and **B** MUST be set to 1, in every segment (both Long and Short Datagram). The SSF capability is exposed by setting the B bit. For a Long Datagram the 2nd to the nth segment MUST be sent in the format described in Figure 6-8.

**A** is a reserved bit, it is not used in this case but should be set to zero when being sent and ignored at reception.

Both the Destination and the Source supports and use SSF:

**C** MUST be set to 0, and **B** MUST be set to 1, if it is the first segment in a Datagram.

If it is a Long Datagram and it is the 2nd to nth segment **C** MUST be set to 1, and **B** MUST be set to 1.

**A** is a reserved bit, it is not used in this case but should be set to zero when being sent and ignored at reception.

### 6.10.5 Encapsulation of WDP Mapping for Mobitex into MPAKs

When WDP datagrams, or segments of WDP datagrams, are to be sent over a Mobitex bearer, they MUST be put into Mobitex Packets (MPAKs). The MPAK MUST be initialised as described below. For further information on the MPAK format, see [Mobitex]. **Note!** Bit 0 is MSB and bit 7 is LSB.

| MPAK Encapsulation format | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octet | MSB 0 | 1 | 2 | 3 | 4 | 5 | 6 | LSB 7 |
| 1 | SENDER (Mobitex MAN) | | | | | | | |
| 2 | | | | | | | | |
| 3 | | | | | | | | |
| 4 | ADDRESSEE (Mobitex MAN) | | | | | | | |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 9 | Mobitex Time (not used) | | | | | | | |
| 10 | | | | | | | | |
| 11 | | | | | | | | |
| 12 | WAP/WDP-Specific Protocol Identification (0x0B) | | | | | | | |
| 13 . . | Payload (Datagram) | | | | | | | |

**Figure 6-10 MPAK Encapsulation Format**

The **SENDER** field shall contain the Mobitex MAN of the sender.

The **ADDRESSEE** field shall contain the Mobitex MAN of the addressee.

**Octets 7 and 8** in the MPAK above use one possible set of MPAK flags. Other combinations can be used without causing compatibility restriction. Further information about the flags can be found in [Mobitex].

The WDP layer should ignore the **Mobitex Time** field.

The **Protocol Identification** field shall be set to the identification value defined for WAP/WDP over Mobitex (0x0B), according to the Mobitex Interface Specification [Mobitex].

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# Appendix A. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [IOPProc].

## A.1. Protocol Functions

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-C-001 | WDP client functions | Appendix A | M | WDP-ANSI-C-000 OR<br>WDP-CDMA-C-000 OR<br>WDP-CT-C-002 OR<br>WDP-CT-C-006 OR<br>WDP-CT-C-008 OR<br>WDP-DECT-C-000 OR<br>WDP-FLEX-C-001 OR<br>WDP-FLEX-C-002 OR<br>WDP-GSM-C-000 OR<br>WDP-PDC-C-000 OR<br>WDP-MOBITEX-C-000 OR<br>WDP-TETRA-C-000 |
| WDP-C-002 | Wireless Control Message Protocol | [WCMP] | O | WCMP:MCF |
| WDP-S-001 | WDP server functions | Appendix A | M | WDP-ANSI-S-000 OR<br>WDP-CDMA-S-000 OR<br>WDP-CT-S-002 OR<br>WDP-CT-S-006 OR<br>WDP-CT-S-008 OR<br>WDP-DECT-S-000 OR<br>WDP-FLEX-S-001 OR<br>WDP-FLEX-S-002 OR<br>WDP-GSM-S-000 OR<br>WDP-PDC-S-000 OR<br>WDP-MOBITEX-S-000 OR<br>WDP-TETRA-S-000 |
| WDP-S-002 | Wireless Control Message Protocol | [WCMP] | O | WCMP:MSF |
| WDP-CORE-C-001 | Basic WDP functions | Appendix A | M | WDP-PF-C-001 AND<br>WDP-PF-C-002 AND<br>WDP-NA-C-006 AND<br>WDP-NA-C-007 |
| WDP-CORE-S-001 | Basic WDP functions | Appendix A | M | WDP-PF-S-001 AND<br>WDP-PF-S-002 AND<br>WDP-NA-S-006 AND<br>WDP-NA-S-007 |
| WDP-PF-C-001 | Abstract service primitive functions for T-Dunitdata.Req. | 5.3.2 | M | |
| WDP-PF-C-002 | Support the abstract service primitive functions for T-DUnitdata.Ind | 5.3.2 | M | |
| WDP-PF-C-003 | Support the abstract service primitive functions for T-DError.Ind | 5.3.3 | O | |
| WDP-PF-S-001 | Abstract service primitive functions for T-Dunitdata.Req. | 5.3.2 | M | |
| WDP-PF-S-002 | Support the abstract service primitive functions for T-DUnitdata.Ind | 5.3.2 | M | |
| WDP-PF-S-003 | Support the abstract service primitive functions for T-DError.Ind | 5.3.3 | O | |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# A.2. Cellular Technology / Network Type

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-CT-C-001 | CDMA technology | [TIAEIA-95] | O | |
| WDP-CT-C-002 | CDPD technology | [TIAEIA-732] | O | |
| WDP-CT-C-003 | FLEX™ technology | [FLEX] | O | |
| WDP-CT-C-004 | GSM technology | [ETSI GSM] | O | |
| WDP-CT-C-005 | ANSI-136 (TDMA) technology | [ANSI-136] | O | |
| WDP-CT-C-006 | iDEN technology | [IDEN] | O | |
| WDP-CT-C-007 | PDC technology | [RCR STD-27] | O | |
| WDP-CT-C-008 | PHS technology | [RCR STD-28] | O | |
| WDP-CT-C-009 | TETRA technology | [TET 392-2] | O | |
| WDP-CT-C-010 | DECT technology | [DECT] | O | |
| WDP-CT-C-011 | ReFLEX™ technology | [ReFLEX] | O | |
| WDP-CT-C-012 | Mobitex technology | [Mobitex] | O | |
| WDP-CT-S-001 | CDMA technology | [TIAEIA-95] | O | |
| WDP-CT-S-002 | CDPD technology | [TIAEIA-732] | O | |
| WDP-CT-S-003 | FLEX™ technology | [FLEX] | O | |
| WDP-CT-S-004 | GSM technology | [ETSI GSM] | O | |
| WDP-CT-S-005 | ANSI-136 (TDMA) technology | [ANSI-136] | O | |
| WDP-CT-S-006 | iDEN technology | [IDEN] | O | |
| WDP-CT-S-007 | PDC technology | [RCR STD-27] | O | |
| WDP-CT-S-008 | PHS technology | [RCR STD-28] | O | |
| WDP-CT-S-009 | TETRA technology | [TET 392-2] | O | |
| WDP-CT-S-010 | DECT technology | [DECT] | O | |
| WDP-CT-S-011 | ReFLEX™ technology | [ReFLEX] | O | |
| WDP-CT-S-012 | Mobitex technology | [Mobitex] | O | |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# A.3. Network and Application Addressing

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-NA-C-000 | At least one network addressing scheme must be supported | | M | WDP-NA-C-001 OR<br>WDP-NA-C-002 OR<br>WDP-NA-C-003 OR<br>WDP-NA-C-004 OR<br>WDP-NA-C-005 OR<br>WDP-NA-C-008 OR<br>WDP-NA-C-009 |
| WDP-NA-C-001 | E.164 addresses support | [ITU E.164] | O | |
| WDP-NA-C-002 | X.25 addresses support | [ITU X.25] | O | |
| WDP-NA-C-003 | Ipv4 addresses support | [RFC791] | O | |
| WDP-NA-C-004 | IPv6 addresses support | [RFC 2373] | O | |
| WDP-NA-C-005 | Proprietary addressing scheme support | Not Applicable | O | |
| WDP-NA-C-006 | Destination Port application addressing support | 4.2, 6.1 | M | |
| WDP-NA-C-007 | Source Port application addressing support | 4.2, 6.1 | M | |
| WDP-NA-C-008 | TETRA addresses support | [TET 392-1] | O | |
| WDP-NA-C-009 | Mobitex address support | [Mobitex] | O | |
| WDP-NA-S-000 | At least one network addressing scheme must be supported | | M | WDP-NA-S-001 OR<br>WDP-NA-S-002 OR<br>WDP-NA-S-003 OR<br>WDP-NA-S-004 OR<br>WDP-NA-S-005 OR<br>WDP-NA-S-008 OR<br>WDP-NA-S-009 |
| WDP-NA-S-001 | E.164 addresses support | [ITU E.164] | O | |
| WDP-NA-S-002 | X.25 addresses support | [ITU X.25] | O | |
| WDP-NA-S-003 | Ipv4 addresses support | [RFC791] | O | |
| WDP-NA-S-004 | IPv6 addresses support | [RFC 2373] | O | |
| WDP-NA-S-005 | Proprietary addressing scheme support | Not Applicable | O | |
| WDP-NA-S-006 | Destination Port application addressing support | 4.2, 6.1 | M | |
| WDP-NA-S-007 | Source Port application addressing support | 4.2, 6.1 | M | |
| WDP-NA-S-008 | TETRA addresses support | [TET 392-1] | O | |
| WDP-NA-S-009 | Mobitex address support | [Mobitex] | O | |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

## A.4. Registered Ports

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-RP-C-001 | Port 2948 for Push Connectionless Session Service | Appendix B | O | |
| WDP-RP-C-002 | Port 2949 for Push Secure Connectionless Session Service | Appendix B | O | |
| WDP-RP-C-003 | Port 9204 for vCard Datagram Service | Appendix B | O | |
| WDP-RP-C-004 | Port 9205 for vCal Datagram Service | Appendix B | O | |
| WDP-RP-C-005 | Port 9206 for vCard Secure Datagram Service | Appendix B | O | |
| WDP-RP-C-006 | Port 9207 for vCal Secure Datagram Service | Appendix B | O | |
| WDP-RP-S-001 | Port 2805 for WTA Secure Connectionless Session Service | Appendix B | O | |
| WDP-RP-S-002 | Port 2923 for WTA Secure Session Service | Appendix B | O | |
| WDP-RP-S-003 | Port 9200 for WAP Connectionless Session Service | Appendix B | O | |
| WDP-RP-S-004 | Port 9201 for WAP Session Service | Appendix B | O | |
| WDP-RP-S-005 | Port 9202 for WAP Secure Connectionless Session Service | Appendix B | O | |
| WDP-RP-S-006 | Port 9203 for WAP Secure Session Service | Appendix B | O | |
| WDP-RP-S-007 | Port 9204 for vCard Datagram Service | Appendix B | O | |
| WDP-RP-S-008 | Port 9205 for vCal Datagram Service | Appendix B | O | |
| WDP-RP-S-009 | Port 9206 for vCard Secure Datagram Service | Appendix B | O | |
| WDP-RP-S-010 | Port 9207 for vCal Secure Datagram Service | Appendix B | O | |

## A.5. CDMA Cellular Technology

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-CDMA-C-000 | Some CDMA bearer | Appendix A | O | WDP-CDMA-C-001 OR WDP-CDMA-C-002 OR WDP-CDMA-C-003 |
| WDP-CDMA-C-001 | SMS bearer service | [TIAEIA-637] | O | WDP-CT-C-001 |
| WDP-CDMA-C-002 | Packet bearer service | [TIAEIA-707], 6.2 | O | WDP-CT-C-001 |
| WDP-CDMA-C-003 | Circuit-Switched bearer service | [TIAEIA-707], 6.2 | O | WDP-CT-C-001 |
| WDP-CDMA-S-000 | Some CDMA bearer | Appendix A | O | WDP-CDMA-S-001 OR WDP-CDMA-S-002 OR WDP-CDMA-S-003 |
| WDP-CDMA-S-001 | SMS bearer service | [TIAEIA-637] | O | WDP-CT-S-001 |
| WDP-CDMA-S-002 | Packet bearer service | [TIAEIA-707] | O | WDP-CT-S-001 |
| WDP-CDMA-S-003 | Circuit-Switched bearer service | [TIAEIA-707] | O | WDP-CT-S-001 |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# A.6. GSM Cellular Technology

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-GSM-C-000 | Some GSM bearer | Appendix A | O | WDP-CT-C-004 AND ( WDP-GSM-C-001 OR WDP-GSM-C-005 OR WDP-GSM-C-007 OR WDP-GSM-C-008 OR WDP-GSM-C-009 ) |
| WDP-GSM-C-001 | SMS bearer service | [GSM0340] | O | WDP-GSM-C-010 AND WDP-GSM-C-011 |
| WDP-GSM-C-002 | SMS Phase 1 text headers | 6.3.3 | O | |
| WDP-GSM-C-003 | Long fragmentation information element sending | [GSM0340] [WAPGSMUD] | O | |
| WDP-GSM-C-004 | Short fragmentation information element sending | [GSM0340] [WAPGSMUD] | O | |
| WDP-GSM-C-005 | USSD bearer service | [GSM0390] | O | WDP-GSM-C-006 AND WDP-GSM-C-010 AND WDP-GSM-C-011 AND WAPoverGSMUSSD:MCF |
| WDP-GSM-C-006 | USSD bearer service information elements | [WAPGSMUD] | O | |
| WDP-GSM-C-007 | GPRS bearer service | [GSM0360] | O | |
| WDP-GSM-C-008 | Circuit Switched bearer service | [ETSI GSM] | O | |
| WDP-GSM-C-009 | Cell Broadcast bearer service | [GSM0341] | O | |
| WDP-GSM-C-010 | Long fragmentation information element receiving | [GSM0340] [WAPGSMUD] | O | |
| WDP-GSM-C-011 | Short fragmentation information element receiving | [GSM0340] [WAPGSMUD] | O | |
| WDP-GSM-S-000 | Some GSM bearer | Appendix A | O | WDP-CT-S-004 AND ( WDP-GSM-S-001 OR WDP-GSM-S-005 OR WDP-GSM-S-007 OR WDP-GSM-S-008 OR WDP-GSM-S-009 ) |
| WDP-GSM-S-001 | SMS bearer service | [WDP] | O | WDP-GSM-S-003 AND WDP-GSM-S-010 AND WDP-GSM-S-011 |
| WDP-GSM-S-002 | SMS Phase 1 text headers | 6.3.3 | O | |
| WDP-GSM-S-003 | Long fragmentation information element sending | [GSM0340] [WAPGSMUD] | O | |
| WDP-GSM-S-004 | Short fragmentation information element sending | [GSM0340] [WAPGSMUD] | O | |
| WDP-GSM-S-005 | USSD bearer service | [GSM0390] | O | WDP-GSM-S-006 AND WDP-GSM-S-003 AND WDP-GSM-S-010 AND WDP-GSM-S-011 AND WAPoverGSMUSSD:MSF |
| WDP-GSM-S-006 | USSD bearer service information elements | [WAPGSMUD] | O | |
| WDP-GSM-S-007 | GPRS bearer service | [GSM0360] | O | |
| WDP-GSM-S-008 | Circuit Switched bearer service | [ETSI GSM] | O | |
| WDP-GSM-S-009 | Cell Broadcast bearer service | [GSM0341] | O | |
| WDP-GSM-S-010 | Long fragmentation information element receiving | [GSM0340] [WAPGSMUD] | O | |
| WDP-GSM-S-011 | Short fragmentation information element receiving | [GSM0340] [WAPGSMUD] | O | |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# A.7. ANSI-136 Cellular Technology

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-ANSI-C-000 | Some ANSI bearer | Appendix A | O | WDP-ANSI-C-001 OR<br>WDP-ANSI-C-002 OR<br>WDP-ANSI-C-003 OR<br>WDP-ANSI-C-004 |
| WDP-ANSI-C-001 | ANSI-136 R-Data service | [TIAEIA-136-750] | O | WDP-CT-C-005 |
| WDP-ANSI-C-002 | ANSI-136 Packet Data service | [TIAEIA-136-370] | O | WDP-CT-C-005 |
| WDP-ANSI-C-003 | ANSI-136 Circuit-Switched Data service | [TIAEIA-136-350] | O | WDP-CT-C-005 |
| WDP-ANSI-C-004 | ANSI-136 R-Data GHOST Service | [TIAEIA-136-711] | O | WDP-CT-C-005 AND<br>WDP-ANSIBEAR-C-003 AND<br>WDP-ANSIBEAR-C-004 |
| WDP-ANSIBEAR-C-001 | Long fragmentation information element sending | [TIAEIA-136-711] | O | |
| WDP-ANSIBEAR-C-002 | Short fragmentation information element sending | [TIAEIA-136-711] | O | |
| WDP-ANSIBEAR-C-003 | Long fragmentation information element receiving | [TIAEIA-136-711] | O | |
| WDP-ANSIBEAR-C-004 | Short fragmentation information element receiving | [TIAEIA-136-711] | O | |
| WDP-ANSI-S-000 | Some ANSI bearer | Appendix A | O | WDP-ANSI-S-001 OR<br>WDP-ANSI-S-002 OR<br>WDP-ANSI-S-003 OR<br>WDP-ANSI-S-004 |
| WDP-ANSI-S-001 | ANSI-136 R-Data service | [TIAEIA-136-750] | O | WDP-CT-S-005 |
| WDP-ANSI-S-002 | ANSI-136 Packet Data service | [TIAEIA-136-370] | O | WDP-CT-S-005 |
| WDP-ANSI-S-003 | ANSI-136 Circuit-Switched Data service | [TIAEIA-136-350] | O | WDP-CT-S-005 |
| WDP-ANSI-S-004 | ANSI-136 R-Data service GHOST Service | [TIAEIA-136-711] | O | WDP-CT-S-005 AND<br>WDP-ANSIBEAR-S-002 AND<br>WDP-ANSIBEAR-S-003 AND<br>WDP-ANSIBEAR-S-004 |
| WDP-ANSIBEAR-S-001 | Long fragmentation information element sending | [TIAEIA-136-711] | O | |
| WDP-ANSIBEAR-S-002 | Short fragmentation information element sending | [TIAEIA-136-711] | O | |
| WDP-ANSIBEAR-S-003 | Long fragmentation information element receiving | [TIAEIA-136-711] | O | |
| WDP-ANSIBEAR-S-004 | Short fragmentation information element receiving | [TIAEIA-136-711] | O | |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# A.8. PDC Cellular Technology

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-PDC-C-000 | Some PDC bearer | Appendix A | O | WDP-PDC-C-001 OR WDP-PDC-C-002 |
| WDP-PDC-C-001 | PDC Packet Data service | 4.4.5.2, 6.2 | O | WDP-CT-C-007 |
| WDP-PDC-C-002 | PDC Circuit-Switched Data service | 4.4.5.1, 6.2 | O | WDP-CT-C-007 |
| WDP-PDC-S-000 | Some PDC bearer | Appendix A | O | WDP-PDC-S-001 OR WDP-PDC-S-002 |
| WDP-PDC-S-001 | PDC Packet Data service | 4.4.5.2, 6.2 | O | WDP-CT-S-007 |
| WDP-PDC-S-002 | PDC Circuit-Switched Data service | 4.4.5.1, 6.2 | O | WDP-CT-S-007 |

# A.9. TETRA Cellular Technology

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-TETRA-C-000 | Some TETRA bearer | Appendix A | O | WDP-TETRA-C-001 OR WDP-TETRA-C-002 |
| WDP-TETRA-C-001 | TETRA SDS bearer service | 4.4.10.1, 6.9 | O | WDP-CT-C-009 |
| WDP-TETRA-C-002 | TETRA Packet Data service | 4.4.10.2, 6.2 | O | WDP-CT-C-009 |
| WDP-TETRA-S-000 | Some TETRA bearer | Appendix A | O | WDP-TETRA-S-001 OR WDP-TETRA-S-002 |
| WDP-TETRA-S-001 | TETRA SDS bearer service | 4.4.10.1, 6.9 | O | WDP-CT-S-009 |
| WDP-TETRA-S-002 | TETRA Packet Data service | 4.4.10.2, 6.2 | O | WDP-CT-S-009 |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-SpecWAP-20030912]

# A.10. DECT Cellular Technology

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-DECT-C-000 | Some DECT bearer | Appendix A | O | WDP-DECT-C-001 OR<br>WDP-DECT-C-002 OR<br>WDP-DECT-C-003 |
| WDP-DECT-C-001 | DECT short message service | 4.4.11.1, 6.3.1, 6.3.2 | O | WDP-CT-C-010 |
| WDP-DECT-C-002 | DECT connection oriented services | 4.4.11.2, 6.2 | O | WDP-CT-C-010 |
| WDP-DECT-C-003 | DECT packet switched services | 4.4.11.3, 6.2 | O | WDP-CT-C-010 |
| WDP-DECT-S-000 | Some DECT bearer | Appendix A | O | WDP-DECT-S-001 OR<br>WDP-DECT-S-002 OR<br>WDP-DECT-S-003 |
| WDP-DECT-S-001 | DECT short message service | 4.4.11.1, 6.3.1, 6.3.2 | O | WDP-CT-S-010 |
| WDP-DECT-S-002 | DECT connection oriented services | 4.4.11.2, 6.2 | O | WDP-CT-S-010 |
| WDP-DECT-S-003 | DECT packet switched services | 4.4.11.3, 6.2 | O | WDP-CT-S-010 |

# A.11. Mobitex Cellular Technology

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-MOBITEX-C-000 | Mobitex MPAK bearer service | 4.4.12, 6.10 | O | WDP-CT-C-012 |
| WDP-MOBITEX-S-000 | Mobitex MPAK bearer service | 4.4.12, 6.10 | O | WDP-CT-S-012 |

# A.12. FLEX/ReFLEX Technology

| Item | Function | Reference | Status | Requirement |
|---|---|---|---|---|
| WDP-FLEX-C-001 | FLEX™ technology | 4.4.7, 6.6 | O | WDP-CT-C-003 |
| WDP-FLEX-C-002 | ReFLEX™ technology | 4.4.7, 6.6 | O | WDP-CT-C-011 |
| WDP-FLEX-S-001 | FLEX™ technology | 4.4.7, 6.6 | O | WDP-CT-S-003 |
| WDP-FLEX-S-002 | ReFLEX™ technology | 4.4.7, 6.6 | O | WDP-CT-S-011 |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# Appendix B. Port Number Definitions (Normative)

WAP has registered the following ports with IANA (Internet Assigned Numbers Authority).

| Port Number | Application/Protocol |
|---|---|
| 2805 | *WAP WTA secure connection-less session service* |
| | Protocol: WSP/WTLS/Datagram |
| 2923 | *WAP WTA secure session service* |
| | Protocol: WSP/WTP/WTLS/Datagram |
| 2948 | *WAP Push connectionless session service (client side)* |
| | Protocol: WSP/Datagram |
| 2949 | *WAP Push secure connectionless session service (client side)* |
| | Protocol: WSP/WTLS/Datagram |
| 9200 | *WAP connectionless session service* |
| | Protocol: WSP/Datagram |
| 9202 | *WAP secure connectionless session service* |
| | Protocol: WSP/WTLS/Datagram |
| 9201 | *WAP session service* |
| | Protocol: WSP/WTP/Datagram |
| 9203 | *WAP secure session service* |
| | Protocol: WSP/WTP/WTLS/Datagram |
| 9204 | *WAP vCard* |
| | Protocol: vCard/Datagram |
| 9206 | *WAP vCard Secure* |
| | Protocol: vCard/WTLS/Datagram |
| 9205 | *WAP vCal* |
| | Protocol: vCalendar/Datagram |
| 9207 | *WAP vCal Secure* |
| | Protocol: vCalendar/WTLS/Datagram |

The WAP protocols defined in the initial specifications are:

- Wireless Session Protocol (WSP/B) with and without security. The Wireless Session Protocol has two modes: a connection oriented mode and a connectionless mode, and thus 4 ports are reserved. The connection oriented mode uses [WTP] for transaction support.
- vCard for use for push of “phone book items” (with and without security) to an application in either a mobile client or a fixed server. The vCard structure is placed as the userdata of the UDP/WDP datagram.
- vCalendar for push of calendar events (with and without security) to a calendar application in either a mobile client or a fixed server. The vCalendar structure is placed as the userdata of the UDP/WDP datagram.

The security protocol for the above secure ports is WTLS.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# Appendix C. Bearer Type Assignments (Normative)

## Network Bearer Table

The Network bearer table defines a numbering space for network, bearer and address type combinations. Its uses are expected to include higher level protocols such as WSP.

Note: network or bearer type can be "any", in this case the bearer adaptor is free to choose any available network/bearer that supports the address format.

| Network | Bearer type | Address type | Assigned number |
|---|---|---|---|
| Any | Any | IPv4 | 0x00 |
| Any | Any | IPv6 | 0x01 |
| GSM | USSD | Any (Note 2) | 0x02 |
| GSM | SMS | GSM_MSISDN (Note 1) | 0x03 |
| ANSI-136 | GUTS/R-Data | ANSI_136_MSISDN | 0x04 |
| IS-95 CDMA | SMS | IS_637_MSISDN | 0x05 |
| IS-95 CDMA | CSD | IPv4 | 0x06 |
| IS-95 CDMA | Packet data | IPv4 | 0x07 |
| ANSI-136 | CSD | IPv4 | 0x08 |
| ANSI-136 | Packet Data | IPv4 | 0x09 |
| GSM | CSD | IPv4 | 0x0A |
| GSM | GPRS | IPv4 | 0x0B |
| GSM | USSD | IPv4 | 0x0C |
| AMPS | CDPD | IPv4 | 0x0D |
| PDC | CSD | IPv4 | 0x0E |
| PDC | Packet Data | IPv4 | 0x0F |
| IDEN | SMS | iDEN_MSISDN | 0x10 |
| IDEN | CSD | IPv4 | 0x11 |
| IDEN | Packet Data | IPv4 | 0x12 |
| Paging network | FLEX™ | FLEX_MSISDN | 0x13 |
| PHS | SMS | PHS_MSISDN | 0x14 |
| PHS | CSD | IPv4 | 0x15 |
| GSM | USSD | GSM_Service_Code | 0x16 |
| TETRA | SDS | TETRA_ITSI | 0x17 |
| TETRA | SDS | TETRA_MSISDN | 0x18 |
| TETRA | Packet Data | IPv4 | 0x19 |
| Paging Network | ReFLEX™ | ReFLEX_MSISDN | 0x1A |
| GSM | USSD | GSM_MSISDN | 0x1B |
| Mobitex | MPAK | MAN | 0x1C |
| ANSI-136 | GHOST/R_DATA | GSM_MSISDN (Note 1) | 0x1D |
| Reserved | Reserved | Reserved | 0x1E to 0xFF |

Note 1: If the Address Type is GSM_MSISDN, the Address MUST be coded as defined in [GSM03.40]. The semi-octet representation defined in [GSM03.40] must be used.

Note 2: This assignment is used only for backward compability reasons. It can be used with all address types supported in [WAPGSMUD].

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-SpecWAP-20030912]

## Network Bearer Address Types

| Address type | Specification | Short description |
|---|---|---|
| IPv4 | [RFC791] | IPv4 header format |
| IPv6 | [RFC2373] | IPv6 header format |
| IS_637_MSISDN | [TIAEIA-637] | IS-637 address format |
| ANSI_136_MSISDN | [ANSI-136] | ANSI-136 address format |
| GSM_MSISDN | [GSM0340] | GSM SMS address format |
| CDMA_MSISDN | [TIAEIA-637] | CDMA SMS address format |
| iDEN_MSISDN | [IDEN] | iDEN SMS address format |
| FLEX_MSISDN | [FLEX] | FLEX address format |
| GSM_Service_Code | [GSM0290] | GSM USSD service code address format |
| PHS_MSISDN | | PHS SMS address format |
| ReFLEX_MSISDN | [ReFLEX] | ReFLEX address format |
| TETRA_ITSI | [TET 392-1] | TETRA SDS address format |
| TETRA_MSISDN | [TET 392-1] | TETRA SDS address format |
| MAN | [Mobitex] | Mobitex MAN address format |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# Appendix D. Mapping WDP into UDH Format (Informative)

This appendix describes additional information on mapping WDP over GSM SMS, ANSI-136 GHOST and GSM USSD.

## D.1 Binary Header Format

For GSM SMS and GSM USSD the WDP headers structure is defined using the User Data Header (UDH) framework as defined in GSM 03.40:

| FIELD | LENGTH |
|---|---|
| Length of User Data Header | 1 octet |
| Information Element Identifier ‘A’ | 1 octet |
| Length of Information-Element 'A' | 1 octet |
| Information-Element 'A' Data | 1 to ‘n’ octets |
| Information-Element-Identifier 'B' | 1 octet |
| Length of Information-Element 'B' | 1 octet |
| Information-Element 'B' Data | 1 to ‘n’ octets |
| . . . . . | |
| Information-Element-Identifier 'n' | 1 octet |
| Length of Information-Element 'n' | 1 octet |
| Information-Element 'n' Data | 1 to ‘n’ octets |

**Figure D- 1 The Generic User Data Header Structure in GSM SMS and USSD**

The ‘Length-of-Information-Element’ fields shall be the integer representation of the number of octets within its associated ‘Information-Element-Data’ field, which follows and shall not include itself in its count value.

The ‘Length-of-User-Data-Header’ field shall be the integer representation of the number of octets within the ‘User-Data-Header’ information fields which follow and shall not include itself in its count.

Byte order of integers is most significant byte first. In case the information word of the payload data is different from an octet then the binary header is padded with bits to the start position of an information word (GSM uses a 7-bit alphabet) in most cases. Thus the header is compatible with legacy devices not supporting the WDP Datagram protocol.

## D.2 Segmentation and Reassembly

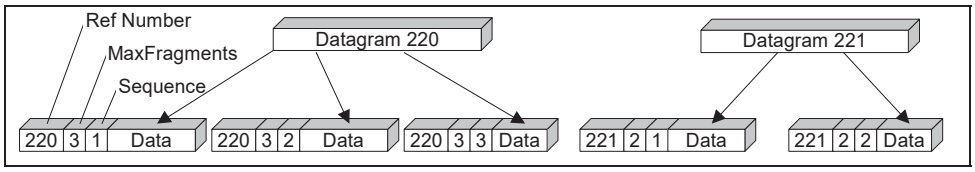



**Figure D-2 Segmentation**

Figure D-2 shows how a typical datagram will be segmented to be transported. It only shows the segmentation logic, i.e. the adaptation layer. A reference number is used to distinguish between different datagrams. The segmentation and reassembly mechanism uses a sequence number and a maxsize number to define the order and the completeness of the message.

The header of a packet contains the following segmentation information:

1. reference number for WDP packet (0-255, or 0-65535)
2. total number of segments in datagram (max 255)
3. segment number. (1-255)

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

The maximum length of a segmented datagram using this scheme is dependent on the packet size. In GSM SMS the maximum network packet size is 140 bytes and in GSM USSD the maximum network packet size is 160 bytes

The sequence (reference and segment) number may be used to resolve problems with duplicate, dropped, and out of order packet delivery. The sequence number can be regarded as a counter that is incremented for each packet.

Reassembly is performed using a list of received packets. As packets arrive, they are inserted in order into the list, and then the list is checked for a complete datagram (all packets received, matching sequence numbers and originator address). If an entire datagram exists it can be delivered to the upper layer.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

## D.3 Combined Use of Headers

The figures below illustrate the use of the User Data Header framework and the various Information Elements defined for WDP. A datagram always contains the port numbers for application level routing, and optionally (if segmentation and reassembly is needed) contains also the adaptation layer.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Length of total User Data Header (all Information Elements) | | | | | | | |
| UDH IE identifier: Port numbers (5) | | | | | | | |
| UDH port number IE length (4) | | | | | | | |
| Destination Port (High) | | | | | | | |
| Destination Port (Low) | | | | | | | |
| Originator Port (High) | | | | | | | |
| Originator Port (Low) | | | | | | | |
| UDH IE identifier: SAR (0) | | | | | | | |
| UDH SAR IE length (3) | | | | | | | |
| Datagram Reference number | | | | | | | |
| Total number of segments in Datagram | | | | | | | |
| Segment count | | | | | | | |
| Padding Bits if User Data uses 7 bit alphabet | | | | | | | |
| 1 - n bytes of User Data | | | | | | | |
| | | | | | | | |

**Figure D-3 A complete datagram header with 8-bit reference and 16-bit addressing scheme**

Figure D-3 shows the complete datagram header using GSM phase 2 backward compatible headers.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Length of total User Data Header (all Information Elements) | | | | | | | |
| UDH IE identifier: Port numbers (5) | | | | | | | |
| UDH port number IE length (4) | | | | | | | |
| Destination Port (High) | | | | | | | |
| Destination Port (Low) | | | | | | | |
| Originator Port (High) | | | | | | | |
| Originator Port (Low) | | | | | | | |
| Padding Bits if User Data uses 7 bit alphabet | | | | | | | |
| 1 - n bytes of User Data | | | | | | | |
| | | | | | | | |

**Figure D-4 A datagram header without SAR**

Figure D-4 shows a datagram which content fits into one bearer network package. In this case no Segmentation and Reassembly header is present. This is possible since the UDH framework is modular.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# Appendix E. Implementation Notes (Informative)

**Port Number usage**

This section of the appendix clarifies some of the questions that are often asked about use of port numbers in WAP.

The UDP ports registered with IANA are server ports, i.e. an entity able to receive requests. The WAP Proxy/Gateway is supposed to listen to the port defined for the protocol it supports. For example, a Proxy supporting WSP/WTP/WTLS/WDP (a secure session service based on transactions) should listen to port 9203.

The client can bind his stack (which really is an application in the UDP environment) to any port number. The Proxy (i.e. server) must execute the transaction on the same Address-port pair as where it has been initiated. The client knows the port number in the proxy (Gateway, Server) a priori, as it per definition is well known.

In fact, both the WSP session as well as the security connection is tied to a particular Address and port quadruplet.

If a device runs two browser instances they should be bound to separate ports. But both can (should) talk to the same port in proxy.

A device with server functionality (i.e. a proxy) should ALWAYS listen to the well-known port that defines the protocol it supports! When a user sends a request for a session to one of the listen ports, the proxy should accept it and isolate it as a logical entity. From here on the port will be used both to listen for new session requests, as well as to handle communication with this logical entity.

The port numbers used by WAP have been registered with IANA. At the moment WAP only defines protocols based on datagrams, i.e. WDP and UDP. However, IANA has reserved also the TCP ports for use by WAP. As WAP has not defined the protocol stacks to be used over a future Wireless TCP the TCP ports should be regarded as “reserver for future use”. They should not be used for any purpose to avoid future collisions of functionality.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

# Appendix F. Change History (Informative)

## F.1 Approved Version History

| Reference | Date | Description |
|---|---|---|
| WAP-200-WDP-20000219-a. | 19-Feb-2000 | The used baseline specification. |
| Class 3 | 16-Apr-2000 | All Converted to use the new specification template. |
| WAP-200_001-WDP-20001212-a | 17-Apr-2000 | 2, 6.2, 4.2.2 Fix normative/informative references. Add reference to IPv6 RFC.<br>Make explicit that payload protection is required. |
| WAP-200_002-WDP-20001213-a | 17-Apr-2000 | App A New SCR table format. |
| WAP-200_003-WDP-20010319-a | 19-Apr-2001 | 2, 4, 3.2,<br>4.4.4, 6.5,<br>App C,<br>App A, 5.5<br>Fix CDMA references. Add SCR entries for registered ports. Fix handling of IS-637 SMS MESSAGE_ID |
| Class 0 | 19-Apr-2001 | 6.11 Add Mobitex Space Saving Function (SSF) |
| Class 3 | 22-Apr-2001 | 2 Reclassify references as normative and informative. Add missing references. 4, 6,App A, |
| Class 3 | 22-Apr-2001 | App C<br>Use proper reference format.Update format of references. |
| Class 2 | 22-Apr-2001 | App A Use more accurate references. |
| Class 3 | 22-Apr-2001 | 3.4 Removed unused abbreviations. Added missing abbreviations. |
| Class 3 | 22-Apr-2001 | 4.3 Removed redundant conformace table - superceded by Appendix A. |
| Class 3 | 26-Apr-2001 | 4.4.6, 6 Removed sections for iDEN SMS, since it will not be defined. |
| WAP-259_001-WDP-20010518-p | 18-May-2001 | 2.1, App A Restructuring of SCR tables |
| WAP-259_002-WDP-20010614-p | 14-Jun-2001 | 2.1, 6.10.5,<br>App C<br>Clarify document reference. Fix Mobitex bit ordering problem.<br>Label anonymous table for easier reference |
| OMA-WAP WDP-20010614-a | 16 Dec 2003 | Updated for new OMA Template |
| WAP-259-WDP-20010614-a | 10-Jan-2005 | Revert document numbering to WAP Forum format. Fixed references for WCMPWDPAdapt, WAPGSMUD. WCMP, WTP & WSP |

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.