WAP WDP

Version 30-Apr-1998

Wireless Application Protocol
Wireless Datagram Protocol Specification

Disclaimer:

This document is subject to change without notice.

Contents

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) 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.

2 Document Status

This document is available online in the following formats:

- PDF format at URL, http://www.wapforum.org/.

2.1 Copyright Notice

2.2 Errata

Known problems associated with this document are published at http://www.wapforum.org/.

2.3 Comments

Comments regarding this document can be submitted to the WAP Forum in the manner published at http://www.wapforum.org/.

3 References

3.1 Normative references

[FLEX]	FLEX™ Protocol Specification and FLEX™ Encoding and Decoding Requirements, Version G1.9, Document Number 68P81139B01, March 16, 1998, Motorola.
[FLEXSuite]	FLEX™ Suite of Application Protocols, Version 1.0, Document Number 6881139B10, October 29, 1997, Motorola.
[GSM0260]	ETSI European Digital Cellular Telecommunication Systems (phase 2+) : General Packet Radio Service (GPRS) - stage 1 (GSM 02.60)
[GSM0290]	ETSI European Digital Cellular Telecommunication Systems (phase 2) : Unstructured Supplementary Service Data(USSD) - stage 1 (GSM 02.90)
[GSM0340]	ETSI European Digital Cellular Telecommunication Systems (phase 2+) : Technical realisation of the Short Message Service (SMS) Point-to-Point (P) (GSM 03.40)
[GSM0360]	ETSI European Digital Cellular Telecommunication Systems (phase 2+) : General Packet Radio Service (GPRS) - stage 2 (GSM 03.60)
[GSM0390]	ETSI European Digital Cellular Telecommunication Systems (phase 2) : Unstructured Supplementary Service Data(USSD) - stage 2 (GSM 03.90)
[GSM0490]	ETSI European Digital Cellular Telecommunication Systems (phase 2) : Unstructured Supplementary Service Data(USSD) - stage 3 (GSM 04.90)
[iDEN]	iDEN™ Technical Overview, Motorola Document Number 68P81095E55-A
[IS130]	EIA/TIA IS-130
[IS135]	EIA/TIA IS-135
[IS136]	EIA/TIA IS-136
[IS637]	TIA/EIA/IS-637: Short Message Services for Wideband Spread Spectrum Cellular Systems
[IS732]	EIA/TIA/IS-732 Cellular Digital Packet Data
[IS07498]	ISO 7498 OSI Reference Model
[ReFLEX]	ReFLEX25 Protocol Specification Document, Version 2.6, Document Number 68P81139B02-A, March 16, 1998, Motorola.
[RFC2119]	S. Bradner “Keywords for use in RFCs to Indicate Requirement Levels”, RFC2119
[TR45.3.6]	General UDP Transport Teleservice (GUTS) ñ Stage III, TR45.3.6/97.12.15
[WAE]	WAP Wireless Application Group, Wireless Application Environment Specification 30-April-1998 URL: http://www.wapforum.org/
[WAPARCH]	WAP Architecture Working Group “Wireless Application Protocol Architecture Specification”, version 1.0 URL: http://www.wapforum.org/
[WAPGSMUD]	WAP and GSM USSD 30-April-1998 URL: http://www.wapforum.org/
[WCMP]	WAP Wireless Transport Group, Wireless Control Message Protocol Specification 30-April-1998 URL: http://www.wapforum.org/
[WTPGOAL]	WAP WTP Working Group “Wireless Transport Protocol Goals Document” version 0.01; document number 112597 URL: http://www.wapforum.org/
[WTPREQ]	WAP WTP Working Group “Wireless Transport Protocol Requirements Document” version 0.02; document number 112597 URL: http://www.wapforum.org/
[WSP]	WAP Wireless Session Group, Wireless Session Protocol Specification 30-April-1998 URL: http://www.wapforum.org/
[WTLS]	WAP Wireless Session Group, Wireless Transport Layer Security Specification 30-April-1998 URL: http://www.wapforum.org/
[WTP]	WAP Wireless Transport Group, Wireless Transaction Protocol Specification 30-April-1998 URL: http://www.wapforum.org/

3.2 Informative References

[RFC768] J. Postel “User Datagram Protocol”, RFC768, August 1980

[RFC791] J. Postel “IP: Internet Protocol”, RFC791

[RFC793] J. Postel “Transmission Control Protocol”, RFC793, September 1981

[RFC2188] M. Banan (Neda), M. Taylor (AT&T), J. Cheng(AT&T) “Efficient Short Remote Operations Protocol Specification Version 1.2”, RFC2188, September 1997

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

4 Definitions and abbreviations

4.1 Definitions

For the purposes of this specification the following definitions apply.

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

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.

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.

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.

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.

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-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.

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

IS-136 R-DATA

IS-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.

Maximum Packet Lifetime, MPL

MPL is fixed by the used carrier (the network system).

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, IS-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.

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.

SMS

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

Transmission

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

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, IS-136 GUTS, 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.

4.2 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.

4.3 Abbreviations

For the purposes of this specification the following abbreviations apply.

API	Application Programming Interface
BMI	Base Station, MSC, Interworking Function (IWF)
BSD	Berkeley Software Distribution
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CSD	Circuit Switched Data
DBMS	Database Management System
DCS	Data Coding Scheme
ETSI	European Telecommunication Standardisation Institute
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
GTR	Group Trailer, indicates the end of packet group
GUTS	General UDP Transport Service
HLR	Home Location Register
iDEN	Integrated Digital Enhanced Network
IE	Information Element
IP	Internet Protocol
LAPi	Link Access Protocol iDEN
LSB	Least significant bits
MAC	Medium Access Control
MAP	Mobile Application Part
MDBS	Mobile Data Base Station
MDG	Mobile Data Gateway
MD-IS	Mobile Data - Intermediate System
MDLP	Mobile Data Link Protocol
MGL	Maximum Group Length
MMI	Man Machine Interface
MPL	Maximum Packet Lifetime (constant)
MPS	Maximum Packet Size
MSISDN	Mobile Subscriber ISDN (Telephone number or address of device)
MS	Mobile Station
MSB	Most significant bits
MSC	Mobile Switching Centre
MSS	Maximum Segment Size
PCI	Protocol Control Information
PCS	Personal Communication Services
PDLP	Packet Data Link Protocol
PLMN	Public Land Mobile Network
PPP	Point-to-Point Protocol
R-Data	Relay Data
RFCL	Radio Frequency Convergence Layer
RTT	Round-Trip Time
SAR	Segmentation and Reassembly

SMSC	Short Message Service Centre
SMS	Short Message Service
SNDCP	SubNetwork Dependent Convergence Protocol
SPT	Server Processing Time
SS7	Signalling System 7
SSAR	Simplified Segmentation and Reassembly
TCAP	Transaction Capability Application Part
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TIA/EIA	Telecommunications Industry Association/Electronic Industry Association
TSAP	Transport Service Access Point
TTR	Transmission Trailer, indicates the end of transmission
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
VLR	Visitor Location Registry
VPLMN	Visitor Public Land Mobile Network
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WSP	Wireless Session Protocol
WTP	Wireless Transaction Protocol

4.4 Requirements

This specification uses the following words for defining the significance of each particular requirement:

MUST

This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

MUST NOT

This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

SHOULD

This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT

This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

MAY

This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include

a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

4.5 Security Considerations

WDP has no authentication mechanisms.

5 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.

5.1 Reference Model

The model of protocol architecture for the Wireless Datagram Protocol is given in Figure 5.1.

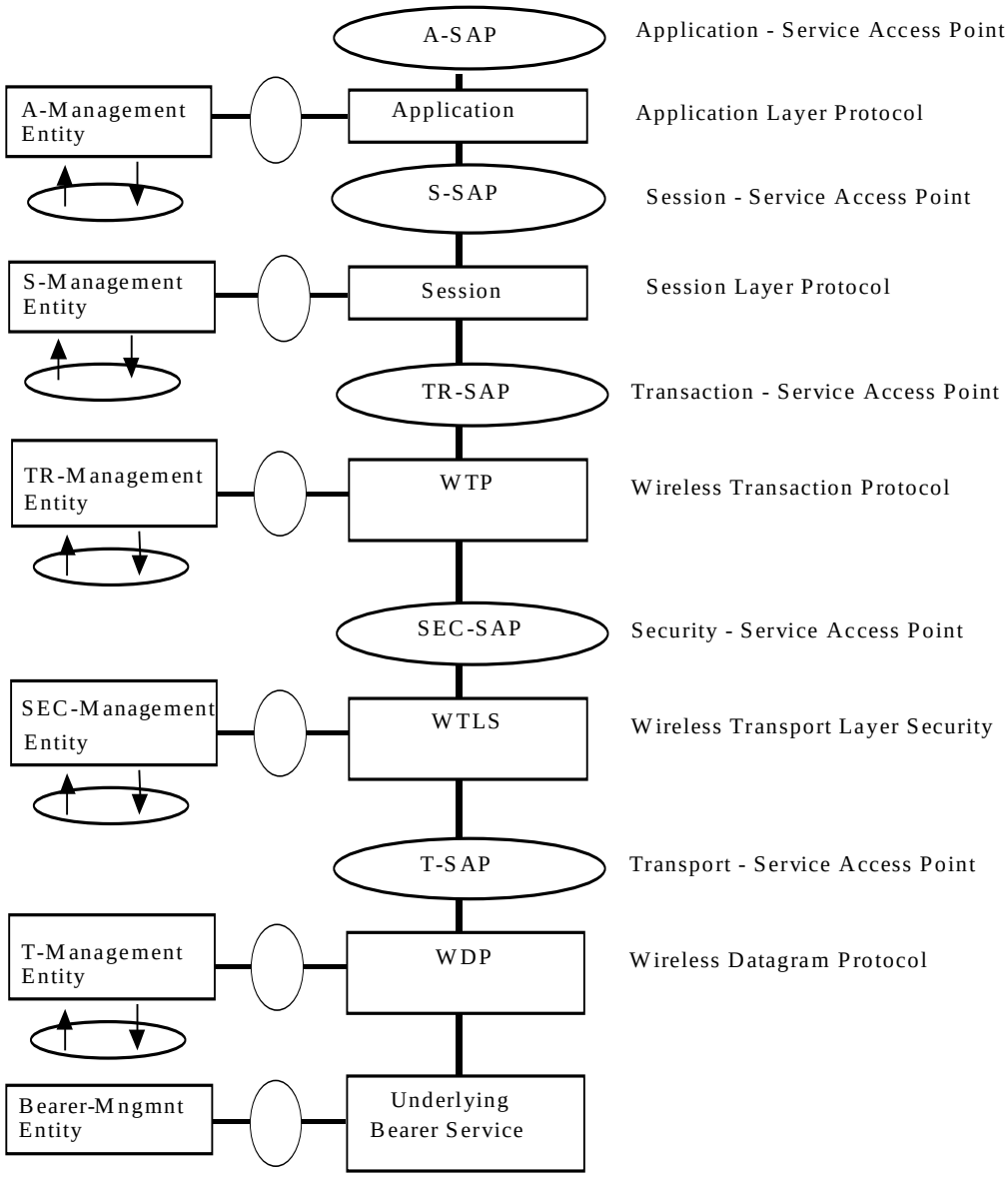

Figure 5.1: Wireless Datagram Protocol Architecture

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.

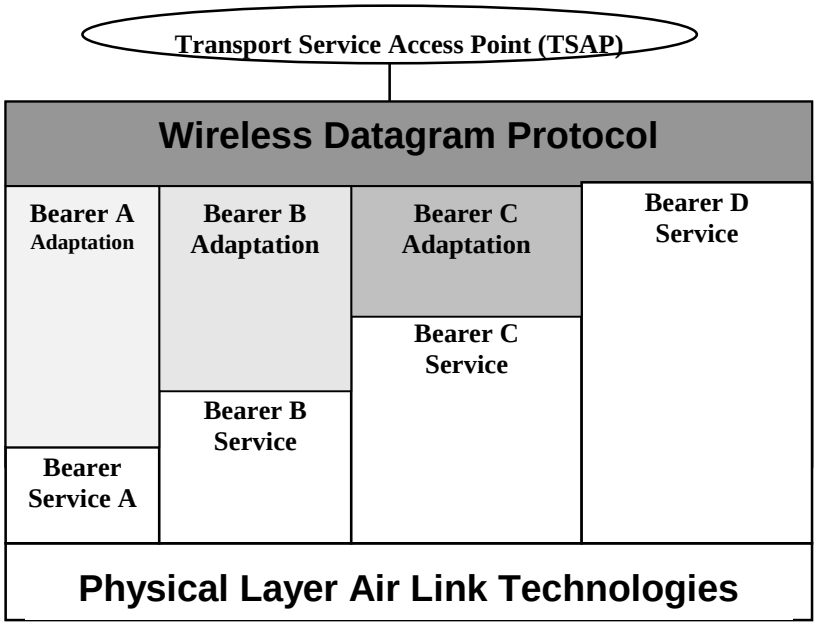

Figure 5.2: Wireless Datagram Protocol Architecture

The model of protocol architecture for the Wireless Transport Protocol is given in Figure 5.2.

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 5.2 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.

5.2 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 5.3 shows a general model of the WAP protocol architecture and how WDP fits into that architecture.

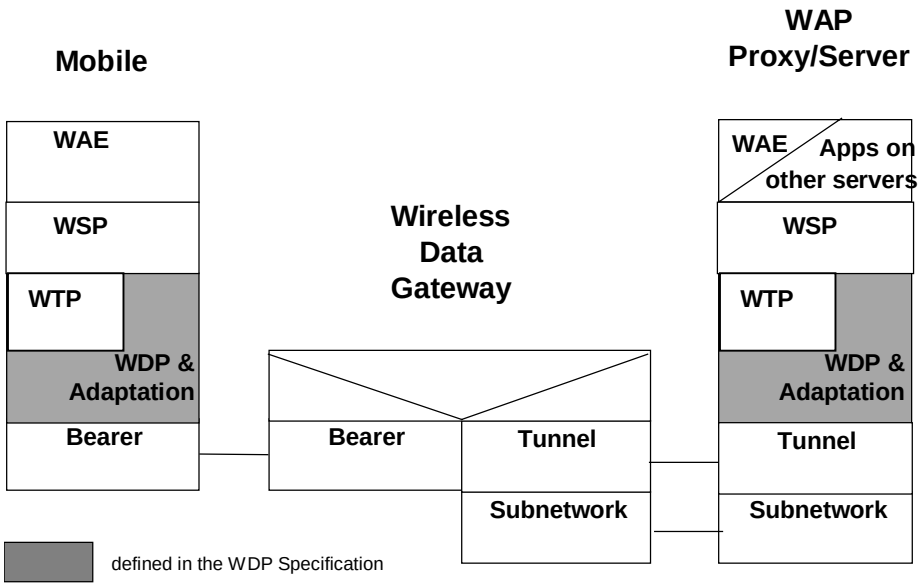

Figure 5.3 General WDP Architecture

In figure 5.3 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 IS-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.

5.2.1 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.

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.

5.2.2 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.

5.3 WDP Static Conformance Clause

This static conformance clause defines a minimum set of WDP features that can 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. In the following table Mandatory (M) and Optional (O) features of WDP when operating over a bearer not supporting IP are listed.

Function	Operation	WDP over a Non-IP bearer	Notes
Source Port Number	Send	M	
	Receive	M	
Destination Port Number	Send	M	
	Receive	M	
Segmentation and Reassembly (SAR)	Send	O	
	Receive	O	The provider must be able to recognise SAR upon receive, where applicable for the bearer.
Text Header	Send	O	
	Receive	O	
T-DUnitdata Service Primitive	Request	M	
	Indication	M	
T-Derror Service Primitive	Indication	O	

Table 5.1: WDP Static Conformance Clause for Non-IP Bearer Operation

5.4 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.

5.4.1 WDP over GSM

5.4.1.1 GSM SMS Profile

Figure 5.4 illustrates the protocol profile for the WDP layer when operating over the SMS bearer service.

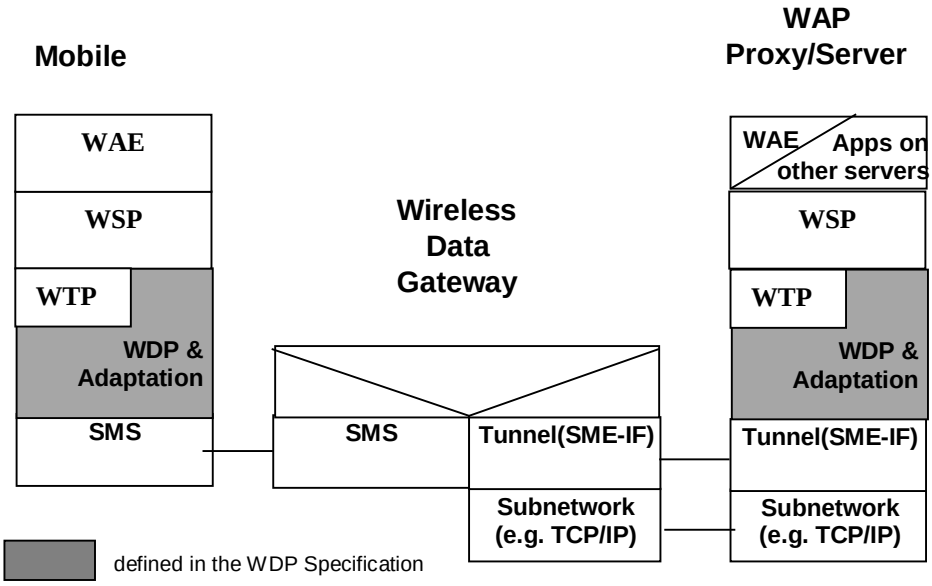

Figure 5.4: WDP over a GSM SMS

5.4.1.2 GSM USSD Profile

Figure 5.5 illustrates the protocol profile for the WTP layer when operating over the USSD bearer service.

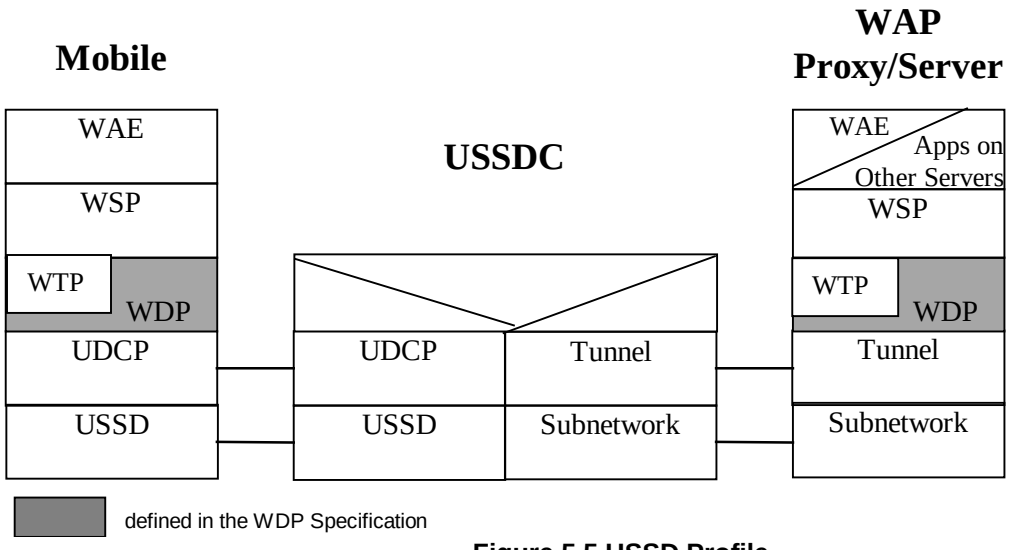

Figure 5.5 USSD Profile.

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.

5.4.1.3 GSM Circuit-Switched Data

Figure 5.6 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.

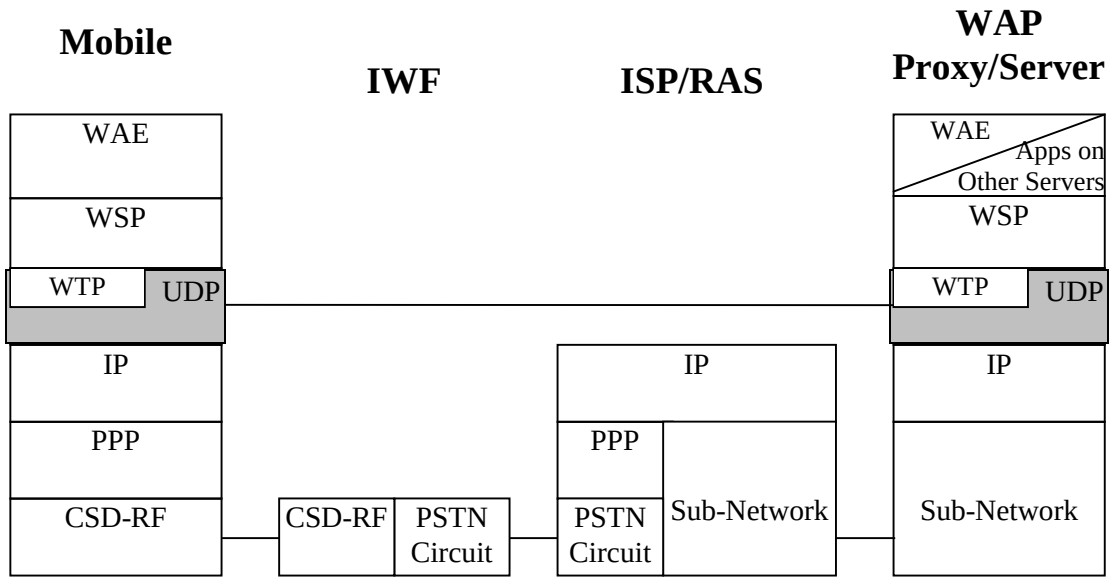

Figure 5.6: WDP over GSM Circuit-Switched Data Channel

5.4.1.4 GSM GPRS Profile

Figure 5.7 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.

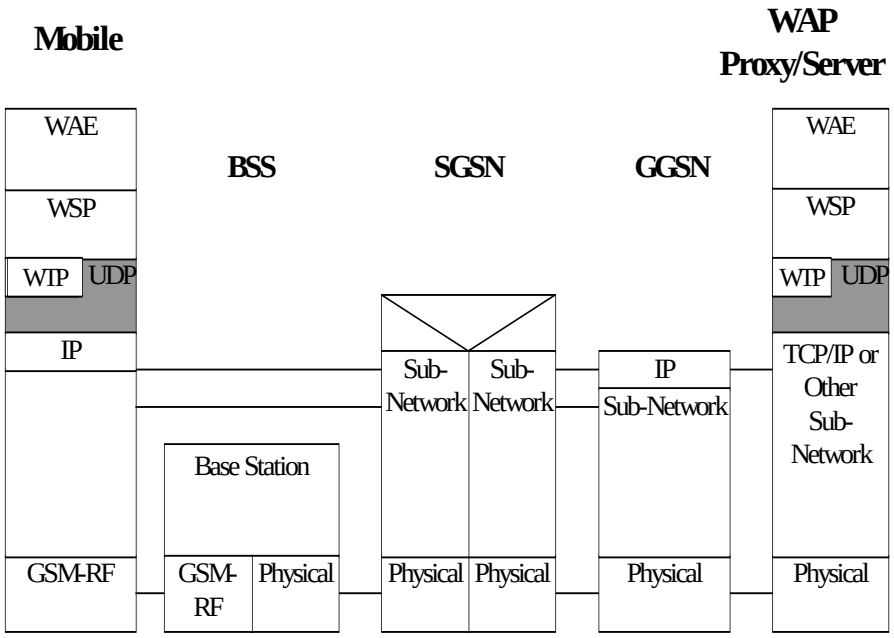

Figure 5.7: WDP over GSM GPRS

5.4.2 WDP over IS-136

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

5.4.2.1 IS-136 R-Data Profile

Figure 5.8 illustrates the protocol profile for the WDP layer when operating over the IS-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 IS-136 Teleservice Server interface protocol is SubNetwork dependent and not specified in the WAP specifications.

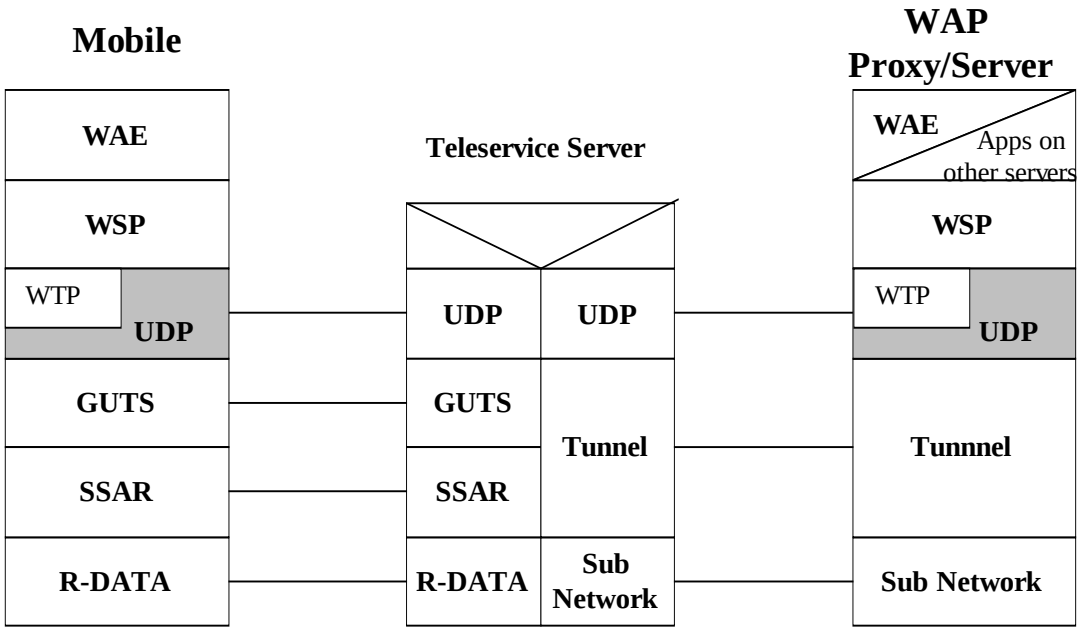

Figure 5.8 WDP over IS-136 R-Data

5.4.2.2 IS-136 Circuit-Switched Data Profile

Figure 5.9 illustrates the protocol profile for the WDP layer when operating over an IS-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.

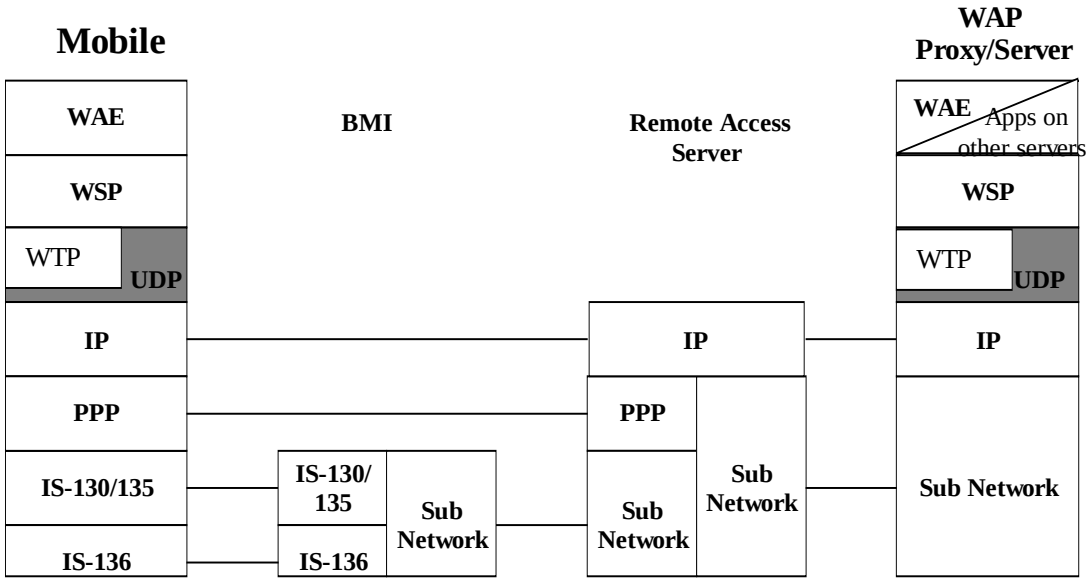

Figure 5.9 WDP over IS-136 Circuit-Switched Data

5.4.2.3 IS-136 Packet Data Profile

Figure 5.10 illustrates the protocol profile for the WDP layer when operating over the IS-136 Packet Data bearer service. IS-136 Packet Data supports IP to the mobile therefore UDP/IP will provide the datagram services.

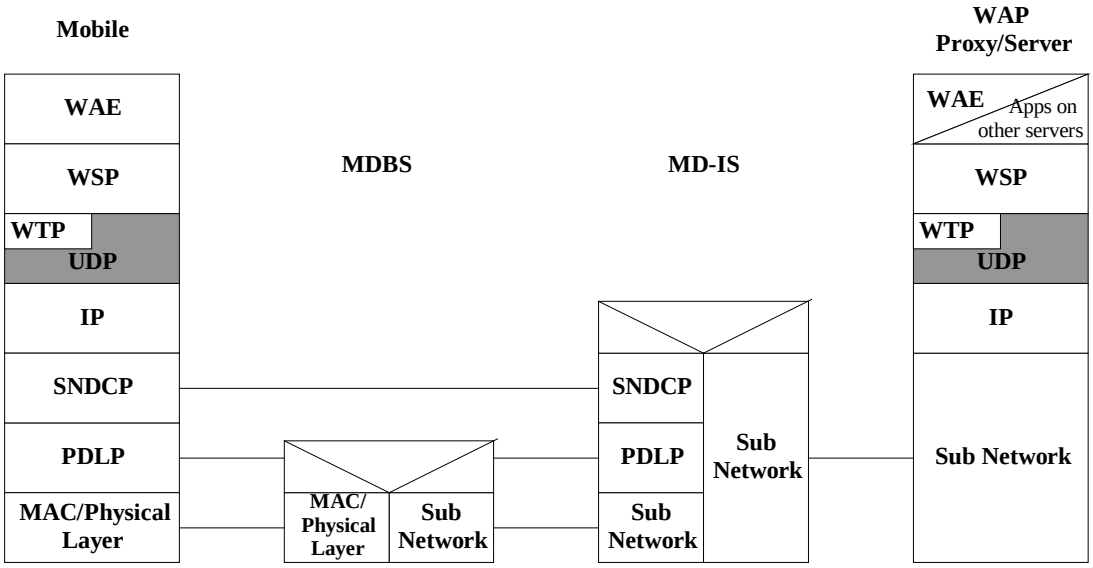

Figure 5.10 WDP over IS-136 Packet Data

5.4.3 WDP over CDPD

Figure 5.11 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.

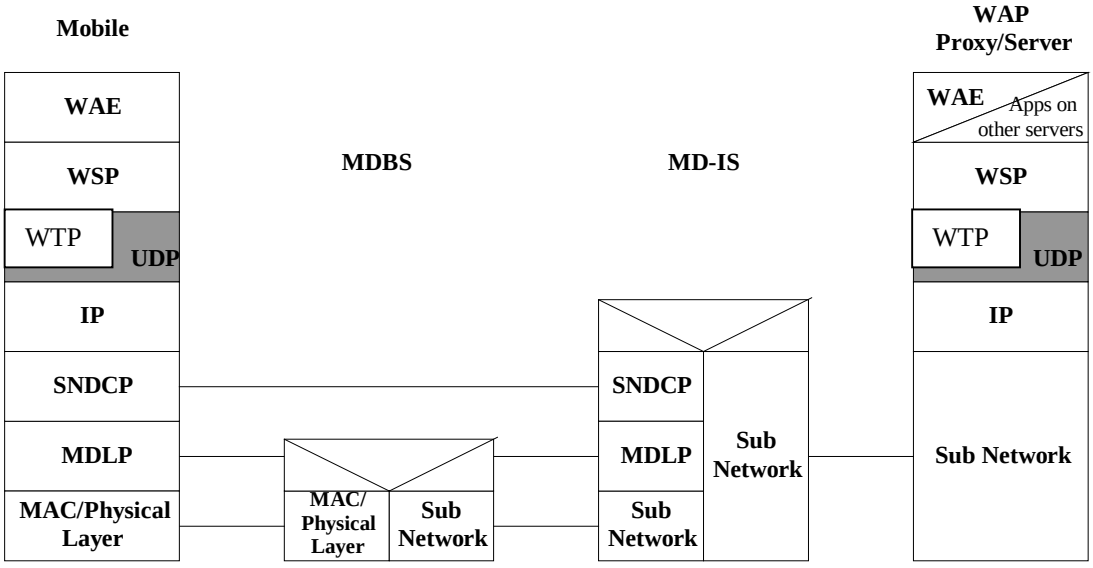

Figure 5.11 WDP over CDPD

5.4.4 WDP over CDMA

The WDP layer operates above the data capable bearer services supported by CDMA. Figure 5.12 identifies the CDMA bearer services presented in this specification.

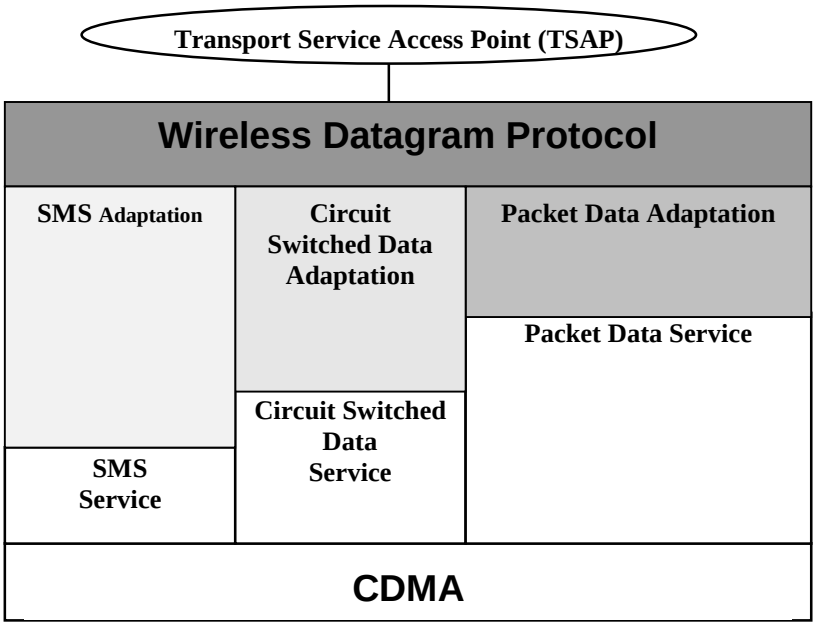

Figure 5.12 WDP over CDMA Bearer Services

5.4.4.1 CDMA Circuit-Switched Data Profile

Figure 5.13 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 IS-707 specification over IS-95 air interface.

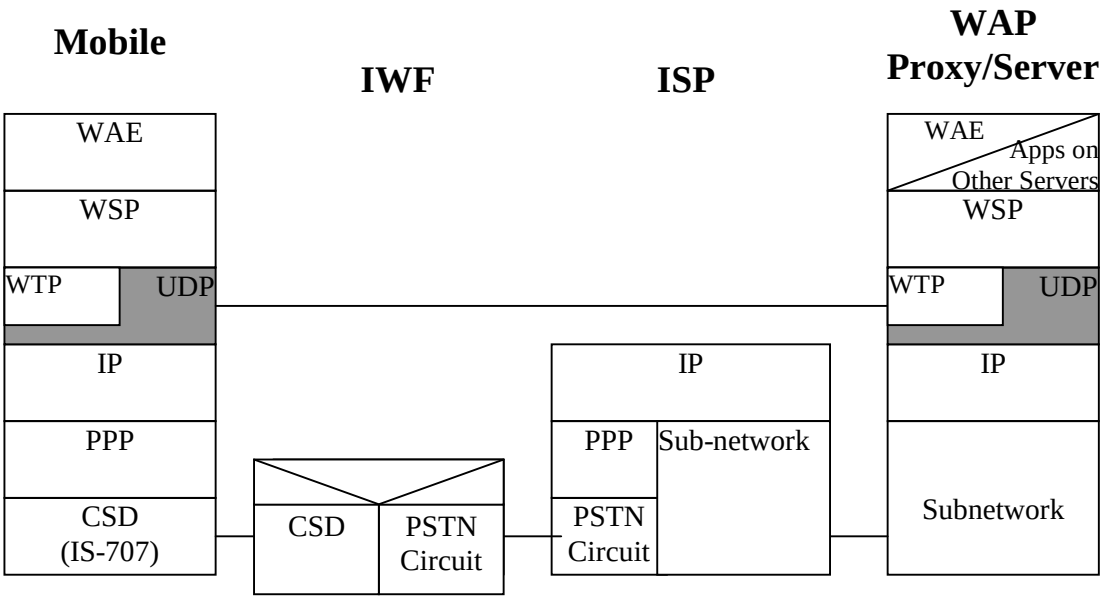

Figure 5.13: WDP over CDMA Circuit-Switched Data Channel

5.4.4.2 CDMA Packet Data Profile

To be defined by WDP CDMA Ad Hoc Group

5.4.4.3 CDMA SMS

WDP over CDMA SMS will be defined in a companion document [WAP over CDMA SMS] that is currently being developed, to be released at a later date.

5.4.5 WDP over PDC (Japan)

The WDP layer operates above the data capable bearer services supported by PDC. Figure 5.14 identifies the PDC bearer services presented in this specification.

The SMS bearer service for PDC is not a part of the specification. Operators have their proprietary solutions. It is therefore left to the operators and applicable vendors to define WDP interface for each proprietary SMS bearer service.

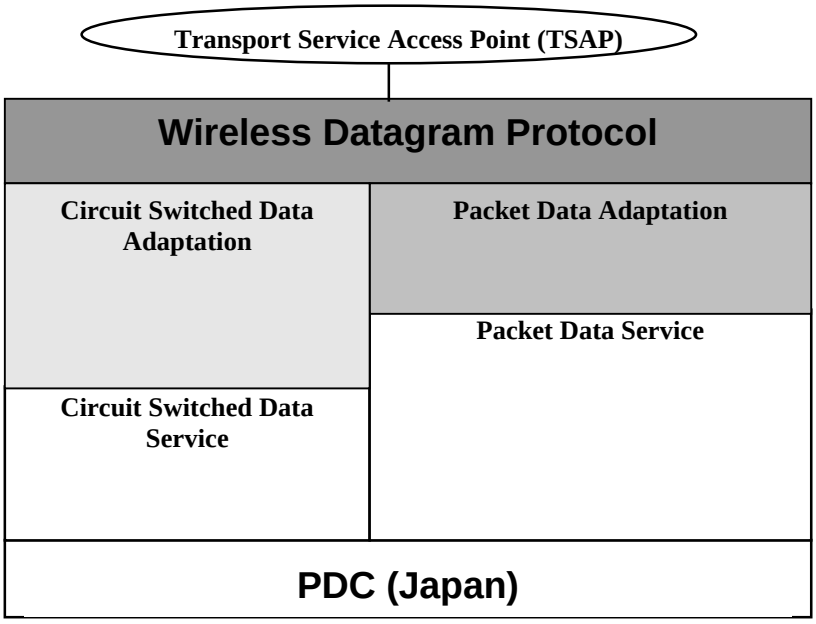

Figure 5.14: WTP over PDC Bearer Services

5.4.5.1 PDC Circuit-Switched Data

Figure 5.15 illustrates the protocol profile for the WTP layer when operating over a Circuit-Switched Data connection. The IWU provides CSD services. 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. WTP over UDP and UDP/IP provide transaction-oriented and datagram services respectively to WSP. The WAP Proxy/Server can terminate the WAE or serve as a proxy to other applications on the Internet.

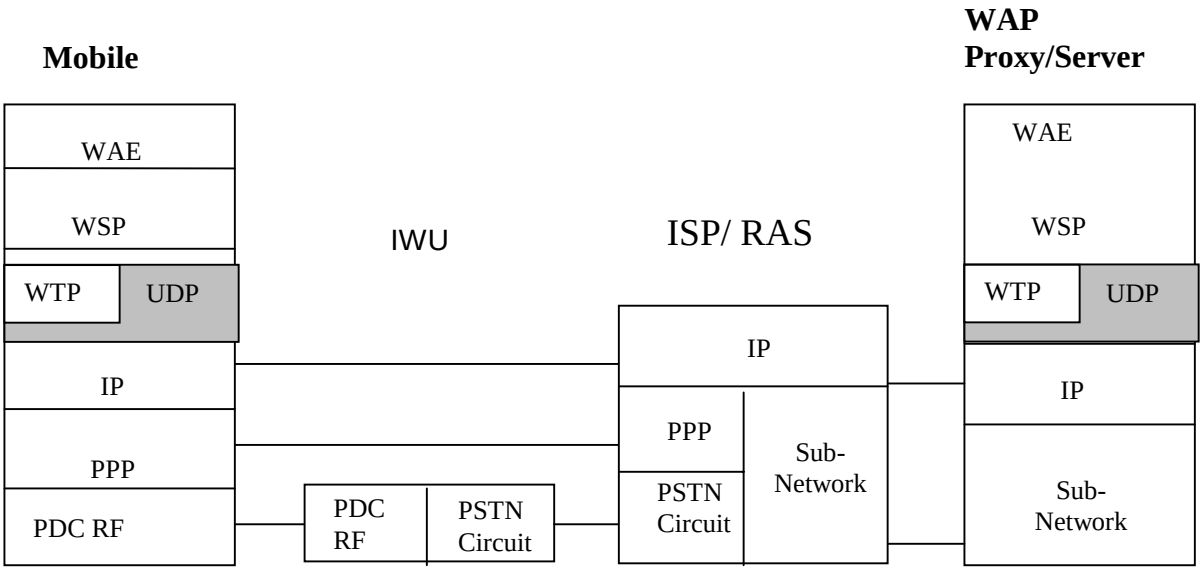

Figure 5.15: WDP over PDC Circuit-Switched Data Channel

5.4.5.2 PDC Packet Data Profile

Figure 5.16 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.

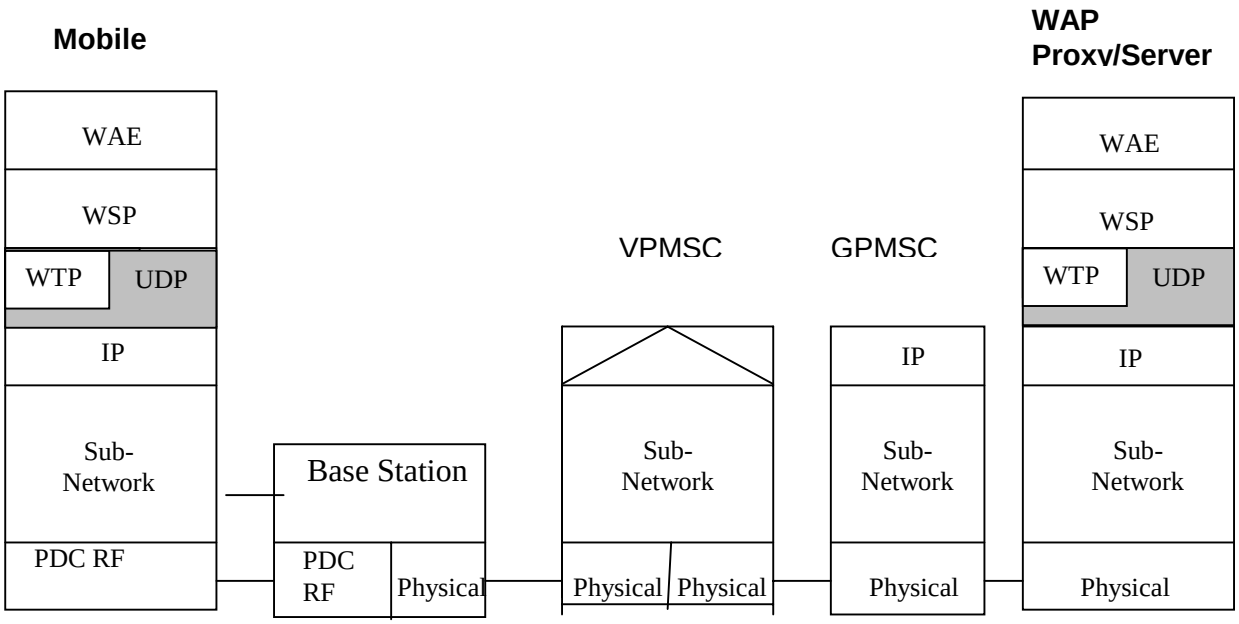

Figure 5.16: WDP over PDC Packet Data Channel

5.4.6 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.

5.4.6.1 iDEN Short Message Service

The SMS service adaptation of WDP has not yet been defined.

5.4.6.2 iDEN Circuit-Switched Data

Figure 5.17 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.

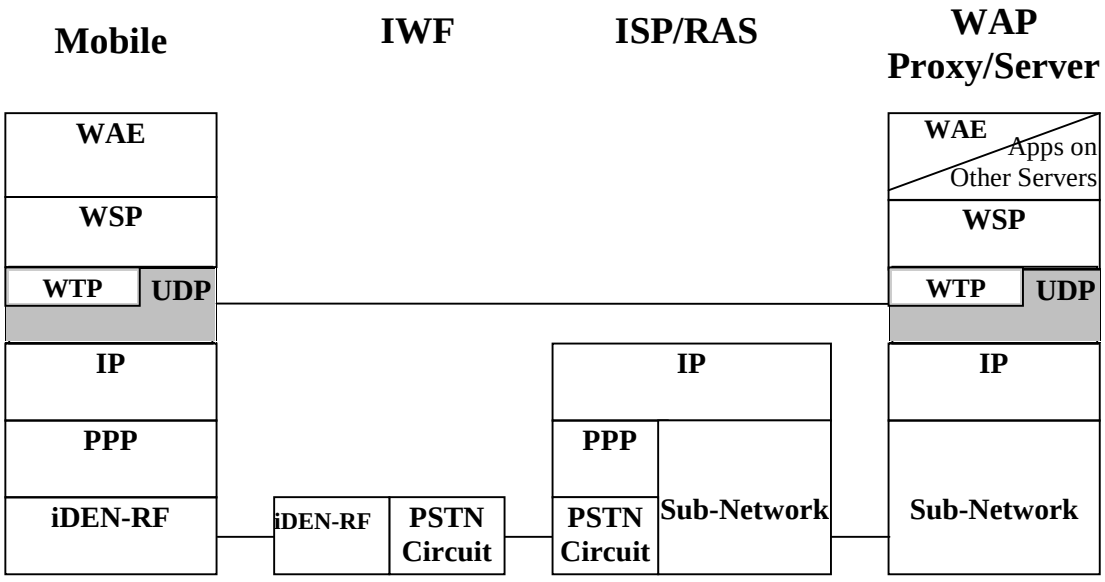

Figure 5.17: WDP over iDEN Circuit-Switched Data Channel

5.4.6.3 iDEN Packet Data

Figure 5.18 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.

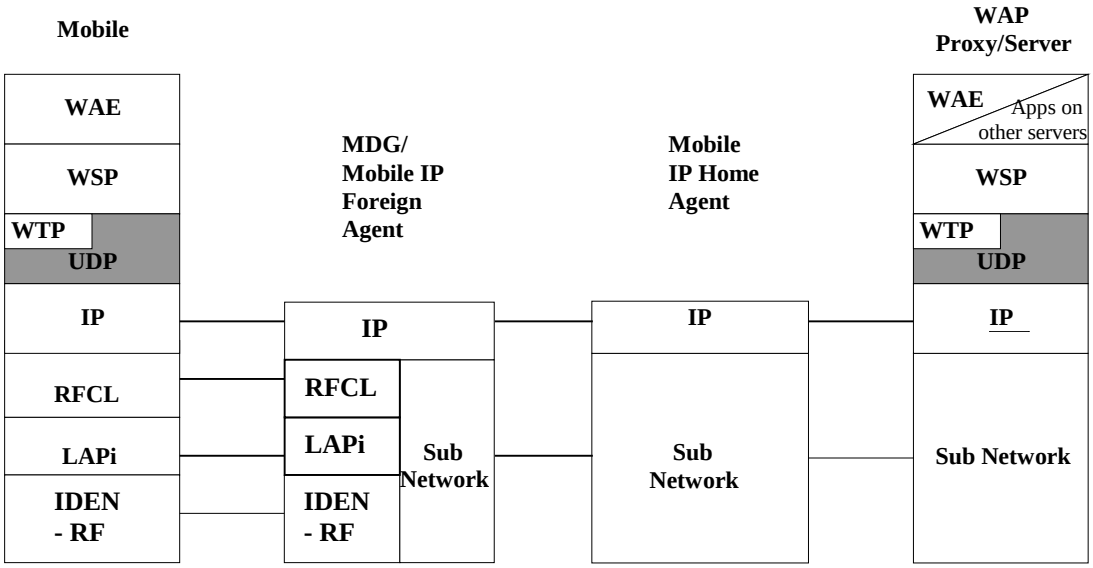

Figure 5.18 WTP over iDEN Packet Data

5.4.7 WDP over FLEX and ReFLEX

Figure 5.19 illustrates the protocol profile for the WDP layer when operating over the FLEX and ReFLEX paging protocols. The profile for FLEX and ReFLEX requires a generic messaging network protocol for connecting the WAP Proxy/Server to the FLEX or ReFLEX network. WDP packets are transferred between the mobile and the paging network through the use of the FLEX Suite of Application Enabling protocols. Optionally, the FLEX Suite protocols may be carried to the WAP Proxy/Server, depending on the desired functionality. The WAP Proxy/Server can terminate the WAE or serve as a proxy to other applications on the Internet or other networks.

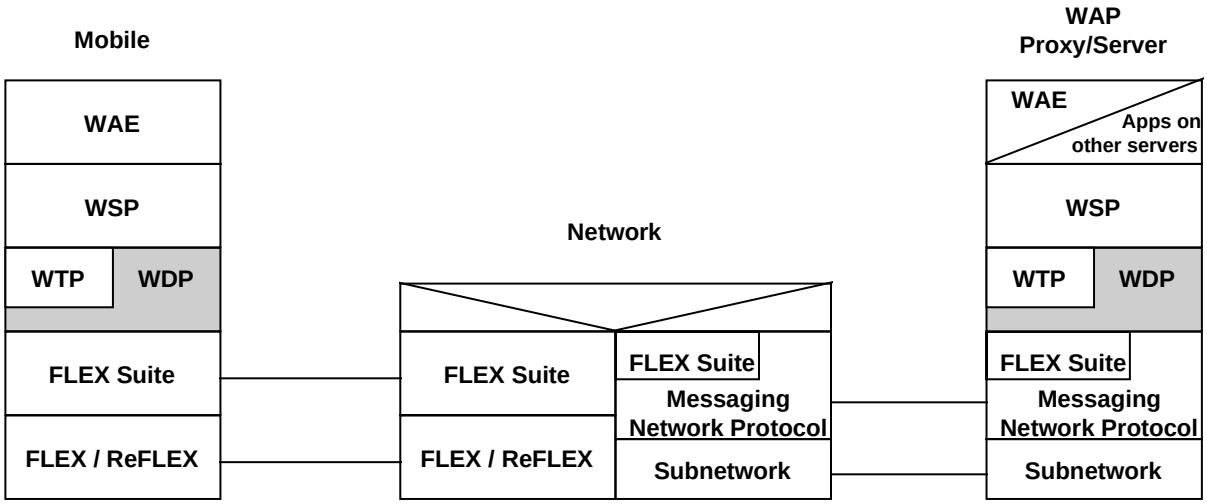

Figure 5.19: FLEX and ReFLEX Profile

6 Elements for layer-to-layer communication

6.1 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.

6.2 Service Primitives Types

The primitives types defined in this specification are:

6.2.1 Request (.Req)

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

6.2.2 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.

6.2.3 Response (.Res)

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

6.2.4 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).

6.3 WDP Service Primitives

6.3.1 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 may also receive a T-DError primitive if the requested transmission cannot be executed by the WDP protocol layer.

6.3.1.1 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.

6.3.1.2 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 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 / **Parameter**	**T-Error**			
	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.

7 WDP Protocol Description

7.1 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.

7.2 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 RFC 768 while the IP networking layer is defined in RFC 791.

7.3 Mapping of WDP for GSM SMS 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 for GSM supports mandatory binary and optional text based headers. GSM USSD Phase 2 supports binary headers, GSM SMS Phase 2 supports both binary and text based headers and GSM SMS Phase 1 supports text based headers.

Each packet (segment) used in the WDP protocol are 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 or USSD has a similar function to the Protocol Identifier in a IP based network. The construct enables the WDP protocol to coexist with other features of the legacy bearer network.

7.3.1 Header Formats

7.3.1.1 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: See Appendix A for more information.

7.3.2 Segmentation and Reassembly

The WDP segmentation is implemented as specified in GSM 03.40

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 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 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). 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.

7.3.2.1 Fragmentation Information Element (short)

The Fragmentation Information-Element -Identifier is defined in GSM 03.40.

7.3.2.2 Fragmentation Information Element (long)

The Long Fragmentation Information-Element -Identifier is an octet with the hex value XX.

The Long Information-Element-Data octets shall be coded as shown in figure 7.1.

Octet 1-2	Datagram reference number	This octet 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 2 then the receiving entity shall ignore the whole Information Element.

Figure 7.1: Segmentation and Reassembly Information Element using 16 bit reference number

An Information Element (IE) identifier is to be applied and obtained from ETSI.

7.3.2.3 Port address Information Element

The Information-Element-Identifier is defined in GSM 03.40.

7.3.3 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".

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

<WDP-delimiter> ::= <space>

<*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 7.2: Definition of WDP headers in text format

7	6	5	4	3	2	1	0
"/"							
"/"							
"S"							
"C"							
"K"							
"L"							
Destination port (High hex)							
Destination Port (Low hex)							
Originator Port (High hex)							
Originator Port (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)							
1 - n 7-bit characters of User Data							

Figure 7.3: Example of a WDP header for compatibility with legacy GSM networks

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

7.3.4 Mapping of WDP to GSM USSD

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

7.4 Mapping of WDP for IS-136 GUTS/R-Data

IS-136 GUTS is used to support UDP datagrams on IS-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 IS-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.

7.5 Mapping of WDP to CDMA

To be defined.

7.6 Mapping of WDP to PDC

To be defined.

7.7 Mapping of WDP to iDEN

To be defined.

7.8 Mapping of WDP to FLEX and ReFLEX

To be defined.

Appendix A: PICS Proforma

The supplier of a protocol implementation that claims conformance to this Specification shall complete a copy of the PICS proforma provided in this appendix, including the information necessary to identify both the supplier and the implementation.

A.1 Introduction

The supplier of a protocol implementation which is claimed to conform to this Specification shall complete the following Protocol Implementation Conformance Statement (PICS) proforma.

A completed PICS proforma is the PICS for the implementation in question. The PICS is a statement of which capabilities and options of the protocol have been implemented. The PICS can have a number of uses, including use

- by the protocol implementor, as a check-list to reduce the risk of failure to conform to the standard through oversight;
- by the supplier and acquirer — or potential acquirer — of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma;
- by the user — or potential user — of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSs);
- by a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

A.2 Abbreviations and special symbols

A.2.1 Status symbols

M	mandatory
O	optional
O.<n>	optional, but support of at least one of the group of options labelled by the same numeral <n> is required
X	prohibited
<pred>:	conditional-item symbol, including predicate identification (see A.3.4)
^	logical negation, applied to a conditional item’s predicate

A.2.2 Other symbols

<r>	receive aspects of an item
<s>	send aspects of an item

A.3 Instructions for completing the PICS proforma

A.3.1 General structure of the PICS proforma

The first part of the PICS proforma — Implementation Identification and Protocol Summary — is to be completed as indicated with the information necessary to identify fully both the supplier and the implementation.

The main part of the PICS proforma is a fixed-format questionnaire divided into a number of major subclauses; these can be divided into further subclauses each containing a group of individual items. Answers to the questionnaire items are to be provided in the rightmost column, either by simply marking an answer to indicate a restricted choice (usually Yes or No), or by entering a value or a set or range of values.

NOTE — There are some items for which two or more choices from a set of possible answers can apply. All relevant choices are to be marked in these cases.

Each item is identified by an item reference in the first column; the second column contains the question to be answered; and the third column contains the reference or references to the material that specifies the item in the main body of this Specification. The remaining columns record the status of the item — whether support is mandatory, optional, prohibited, or conditional — and provide space for the answers (see also A.3.4).

A supplier may also provide further information, categorized as either Additional Information or Exception Information. When present, each kind of further information is to be provided in a further subclause of items labelled A<i> or X<i>, respectively, for cross-referencing purposes, where <i> is any unambiguous identification for the item (e.g., a number); there are no other restrictions on its format or presentation.

A completed PICS proforma, including any Additional Information and Exception Information, is the Protocol Implementation Conformance Statement for the implementation in question.

NOTE — Where an implementation is capable of being configured in more than one way, a single PICS may be able to describe all such configurations. However, the supplier has the choice of providing more than one PICS, each covering some subset of the implementation's configuration capabilities, in cases where this makes for easier and clearer presentation of the information.

A.3.2 Additional information

Items of Additional Information allow a supplier to provide further information intended to assist in the interpretation of the PICS. It is not intended or expected that a large quantity will be supplied, and a PICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations, or a brief rationale — based perhaps upon specific application needs — for the exclusion of features which, although optional, are nonetheless commonly present in implementations of this protocol.

References to items of Additional Information may be entered next to any answer in the questionnaire, and may be included in items of Exception Information.

A.3.3 Exception information

It may occasionally happen that a supplier will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No pre-printed answer will be found in the support column for this; instead, the supplier shall write the missing answer into the Support column, together with an X<i> reference to an item of Exception Information, and shall provide the appropriate rationale in the Exception Information item itself.

An implementation for which an Exception Information item is required in this way does not conform to this Specification.

NOTE — A possible reason for the situation described above is that a defect in the standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

A.3.4 Conditional status

A.3.4.1 Conditional items

The PICS proforma contains a number of conditional items. These are items for which the status — mandatory, optional, or prohibited — that applies is dependent upon whether or not certain other items are supported, or upon the values supported for other items.

In many cases, whether or not the item applies at all is conditional in this way, as well as the status when the item does apply.

Where a group of items is subject to the same condition for applicability, a separate preliminary question about the condition appears at the head of the group, with an instruction to skip to a later point in the questionnaire if the "Not Applicable" answer is selected. Otherwise, individual conditional items are indicated by one or more conditional symbols (on separate lines) in the status column.

A conditional symbol is of the form "<pred>:<x>" where "<pred>" is a predicate as described in A.3.4.2, and "<x>" is one of the status symbols M, O, O.<n>, or X.

If the value of the predicate in any line of a conditional item is true (see A.3.4.2), then the conditional item is applicable, and its status is that indicated by the status symbol following the predicate; the answer column is to be marked in the usual way. If the value of a predicate is false, the Not Applicable (N/A) answer is to be marked in the relevant line. Each line in a multi-line conditional item should be marked: at most one line will require an answer other than N/A.

A.3.4.2 Predicates

A predicate is one of the following:

a) an item-reference for an item in the PICS proforma: the value of the predicate is true if the item is marked as supported, and is false otherwise;

b) a predicate name, for a predicate defined elsewhere in the PICS proforma (usually in the Major Capabilities section or at the end of the section containing the conditional item): see below; or

c) the logical negation symbol "^" prefixed to an item-reference or predicate name: the value of the predicate is true if the value of the predicate formed by omitting the "^" is false, and vice versa.

The definition for a predicate name is one of the following

a) an item-reference, evaluated as at (a) above;

b) a relation containing a comparison operator (=, < , etc.) with at least one of its operands being an item-reference for an item taking numerical values as its answer; the predicate is true if the relation holds when each item-reference is replaced by the value entered in the Support column as an answer to the item referred to; or

c) a boolean expression constructed by combining simple predicates, as in (a) and (b), using the boolean operators AND, OR, and NOT, and parentheses, in the usual way; the value of such a predicate is true if the boolean expression evaluates to true when the simple predicates are interpreted as described above.

Each item whose reference is used in a predicate or predicate definition is indicated by an asterisk in the Item column.

A.4 Identification

A.4.1 Implementation identification

Supplier	
Contact point for queries about the PICS	
Implementation name(s) and version(s)	
Other information necessary for full identification (e.g., name(s) and version(s) of machines and/or operating systems, system name(s))	

NOTES

1 Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.

2 The terms Name and Version should be interpreted appropriately to correspond with a supplier's terminology (e.g., Type, Series, Model).

A.4.2 Protocol summary

Identification of protocol specification	WAP Wireless Datagram Protocol
Identification of corrigenda and amendments to the PICS proforma	
Protocol version(s) supported	
Have any Exception Information items been required (see A.3.3)? (The answer YES means that the implementation does not conform to this Specification)	YES ☐ NO ☐

Date of statement	

A.5 Wireless Datagram Protocol

A.5.1 Applicability

Clause A.5 is applicable to all implementations that claim conformance to this Specification.

A.5.2 Cellular Technology / Network Type

Item	Description	Reference	Status	Support
RFCDMA	Does the implementation operate with CDMA technology?	TIA/EIA/IS-95	O.1	YES NO
RFCDPD	Does the implementation operate with CDPD technology?	TIA/EIA/IS-732	O.1	YES NO
RFFLEX	Does the implementation operate with FLEX technology?	Motorola Doc# 68P81139B02-A	O.1	YES NO
RFGSM	Does the implementation operate with GSM technology?	ETSI GSM	O.1	YES NO

Item	Description	Reference	Status	Support
RFIS136	Does the implementation operate with IS-136 (TDMA) technology?	TIA/EIA/IS-136	O.1	YES NO
RfiDEN	Does the implementation operate with iDEN technology?	Motorola Doc# 68P81095E55-A	O.1	YES NO
RFPDC	Does the implementation operate with PDC technology?		O.1	YES NO
RFPHS	Does the implementation operate with PHS technology?		O.1	YES NO

A.5.3 Bearer Services Supported

Item	Description	Reference	Status	Support
BCDMA-SMS	Does the implementation operate with CDMA SMS bearer service?	TIA/EIA/IS-637	RFCDMA:O.1	YES NO
BCDMA-PKT	Does the implementation operate with CDMA Packet bearer service?	TIA/EIA/IS-707	RFCDMA:O.1	YES NO
BCDMA-CSD	Does the implementation operate with CDMA Circuit-Switched bearer service?	TIA/EIA/IS-707	RFCDMA:O.1	YES NO
BCDPD-PKT	Does the implementation operate with CDPD Packet service?	TIA/EIA/IS-732	RFCDPD:O.2	YES NO
BCDPD-CSD	Does the implementation operate with Circuit-Switched CDPD service?	TIA/EIA/ IS-732-1024	RFCDPD:O.2	YES NO
BFLEX	Does the implementation operate with FLEX service?	Motorola Doc# 68P81139B01	RFFLEX:M	YES NO
BGSM-SMS	Does the implementation operate with GSM SMS bearer service?	ETSI GSM 03.40	RFGSM:O.3	YES NO
BGSM-USSD	Does the implementation operate with GSM USSD bearer service?	ETSI GSM 03.90	RFGSM:O.3	YES NO
BGSM-GPRS	Does the implementation operate with GSM GPRS bearer service?	ETSI GSM 03.60	RFGSM:O.3	YES NO
BGSM-CSD	Does the implementation operate with GSM Circuit Switched bearer service?	ETSI GSM	RFGSM:O.3	YES NO
BIS136-RDAT	Does the implementation operate with IS-136 R-Data service?	TIA/EIA/IS-136	RFIS136:O.4	YES NO

Item	Description	Reference	Status	Support
BIS136-PKT	Does the implementation operate with IS-136 Packet Data service?	TIA/EIA/IS-136	RFIS136:O.4	YES NO
BIS136-CSD	Does the implementation operate with IS-136 Circuit-Switched Data service?	TIA/EIA/IS-136	RFIS136:O.4	YES NO
BiDEN	Does the implementation operate with iDEN service?	Motorola Doc# 68P81095E55-A	RFiDEN:M	YES NO
BPDC-PKT	Does the implementation operate with PDC Packet Data service?		RFPDC:O.5	YES NO
BPDC-CSD	Does the implementation operate with PDC Circuit-Switched Data service?		RFPDC:O.5	YES NO
BPHS	Does the implementation operate with PHS service?		RFPHS:O.6	YES NO

A.5.4 Network and Application Addressing

Item	Description	Reference	Status	Support
NA-E164	Does the implementation use E.164 addresses?	ITU E.164	O.1	YES NO
NA-X25	Does the implementation use X.25 addresses?	ITU X.25	O.1	YES NO
NA-IPV4	Does the implementation use IPv4 addresses?	RFC 791	O.1 BCDMA-PKT:M BCDPD-PKT:M BCDPD-CSD:M BGSM-GPRS:M BGSM-CSD:M BiDEN:M	YES NO
NA-OTH	Does the implementation use a proprietary addressing scheme?	Not Applicable	O.1	YES[1] NO
AA-DPORT	Does the implementation support Destination Port application addressing?	3.1, 6.1	M	YES NO
AA-SPORT	Does the implementation support Source Port application addressing?	3.1, 6.1	M	YES NO

Note 1) If a proprietary addressing scheme is used, supply a reference document here, or describe the addressing scheme in a separate attachment to this PICS.

A.5.5 Protocol Functions

Item	Function	Reference	Status	Support
ASPUDR	Does the implementation support the abstract service primitive functions for T-DUnitdata.Req?	5.3.1.1	M	YES NO
ASPUDI	Does the implementation support the abstract service primitive functions for T-DUnitdata.Ind?	5.3.1.1	M	YES NO
ASPERR	Does the implementation support the abstract service primitive functions for T-DError.Ind?	5.3.1.2	O	YES NO

A.5.6 Network Type and Bearer Specific Features

This section of the PICS will cover issues specific to a network type and bearer service within that network type.

A.5.6.1 GSM SMS Specific Features

Item	Function	Reference	Status	Support
GSM-SMS01	Does the implementation support GSM SMS Phase 1 text headers?	6.3.3	BGSM-SMS:O	YES NO
GSM-SMS02	Does the implementation support GSM SMS long fragmentation information element?	6.3.2, 6.3.2.2	BGSM-SMS:M	YES NO
GSM-SMS03	Does the implementation support GSM SMS short fragmentation information element?	6.3.2, 6.3.2.1	BGSM-SMS:O	YES NO

A.5.6.2 GSM USSD Specific Features

Item	Function	Reference	Status	Support
GSM-USSD01			BGSM-USSD	

A.5.6.3 GSM GPRS Specific Features

Item	Function	Reference	Status	Support
GSM-GPRS01			BGSM-GPRS	

A.5.6.4 GSM Circuit Switched Data Specific Features

Item	Function	Reference	Status	Support
GSM-CSD01			BGSM-CSD	

Appendix B: Mapping WDP over GSM SMS and USSD

This appendix describes additional information on mapping WDP over GSM SMS and USSD.

B.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 B.1:The generic User Data Header structure in GSM SMS and GSM 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.

B.2 Segmentation and Reassembly

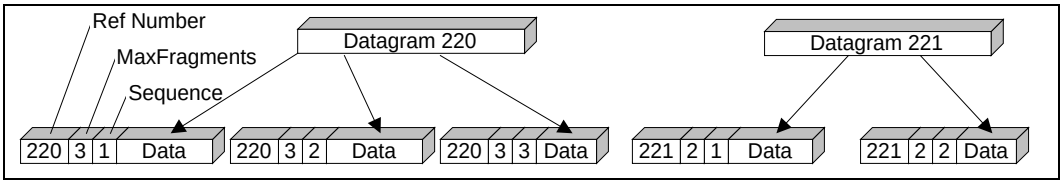

Figure B.2: Segmentation

Figure B.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)

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.

B.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.

7	6	5	4	3	2	1	0
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 B.3: A complete datagram header with 8 bit reference for WDP in GSM SMS

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

7	6	5	4	3	2	1	0
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 B.4: A datagram header without SAR for WDP in GSM SMS

Figure B.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.

Appendix C: Port Number Definitions

WAP is in the process of registering ports for applications in the WAP space. However, at the moment no applications to IANA have yet been made and ports from the Dynamic/Private range are defined. These temporary ports will be changed when ports from the registered range are approved.

Port Number	***Application/Protocol***
49152	Connectionless WAP Browser Proxy Server
	Protocol: WSP/Datagram
49153	Secure Connectionless WAP Browser Proxy Server
	Protocol: WSP/WTLS/Datagram
49154	WAP Browser Proxy Server
	Protocol: WSP/WTP/Datagram
49155	Secure WAP Browser Proxy Server
	Protocol: WSP/WTP/WTLS/Datagram
49156	vCard Receiver
	Protocol: vCard/Datagram
49157	Secure vCard Receiver
	Protocol: vCard/WTLS/Datagram
49158	vCalendar Receiver
	Protocol: vCalendar/Datagram
49159	Secure vCalendar Receiver
	Protocol: vCalendar/WTLS/Datagram

Table C.1: Temporary WAP Port Numbers

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 vCalendar 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.

Appendix D: Bearer Type Assignments

This appendix lists the bearer type code assignments.

Bearer	Assigned Number
IPv4	0x00
IPv6	0x01
GSM USSD	0x02
GSM SMS	0x03
IS-136 R-Data	0x04

Table D.1: Bearer Type Codes

Appendix E. History and Contact Information

Document history		
Date	**Status**	**Comment**
30-Jan-1998	Draft	Draft Version of the Specification for public review
30-Apr-1998	Final	Version 1.0 of the Specification

Contact Information

http://www.wapforum.org/
technical.comments@wapforum.org