WAP WCMP Version 12-June-1998

Wireless Application Protocol
Wireless Control Message 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 protocols (Security, Transaction and Session) of WAP and communicates transparently over one of the available bearer services.

This document specifies the error reporting mechanism for WDP datagrams, the Wireless Control Message Protocol (WCMP). WCMP contains control messages that resemble the Internet Control Message Protocol (ICMP) [RFC 792] [RFC 1885] messages. WCMP can also be used for diagnostics and informational purposes.

2. Document Status

This document is available online in the following formats:

- PDF format at 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. Normative References

[FLEX]	FLEX Protocol Specification Document, version 1.9, Motorola.
[FLEXSuite]	FLEX Suite of Application Enabling Protocols, version 1.0, Motorola.
[GSM0290]	ETSI European Digital Cellular Telecommunication Systems (phase 2) : Unstructured Supplementary Service Data(USSD) - stage 1 (GSM 02.90)
[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)
[GSM0340]	ETSI European Digital Cellular Telecommunication Systems (phase 2+) : Technical realisation of the Short Message Service (SMS) Point-to-Point (P) (GSM 03.40)
[GSM0260]	ETSI European Digital Cellular Telecommunication Systems (phase 2+) : General Packet Radio Service (GPRS) - stage 1 (GSM 02.60)
[GSM0360]	ETSI European Digital Cellular Telecommunication Systems (phase 2+) : General Packet Radio Service (GPRS) - stage 2 (GSM 03.60)
[GUTS]	General UDP Transport Teleservice (GUTS) – Stage III, TR45.3.6/97.12.15
[IS136]	EIA/TIA IS-136
[IS130]	EIA/TIA IS-130
[IS135]	EIA/TIA IS-135
[IS176]	EIA/TIA IS-176 - CDPD 1.1 specifications
[IS637]	TIA/EIA/IS-637: Short Message Services for Wideband Spread Spectrum Cellular Systems
[IS07498]	ISO 7498 OSI Reference Model
[ReFLEX]	ReFLEX25 Protocol Specification Document, version 2.6, Motorola.
[RFC768]	J. Postel “User Datagram Protocol”, RFC768, August 1980
[RFC791]	J. Postel “IP: Internet Protocol”, RFC791
[RFC792]	J. Postel “Internet Control Message Protocol”, RFC792, September 1981
[RFC793]	J. Postel “Transmission Control Protocol”, RFC793, September 1981
[RFC1885]	A. Conta, S. Deering “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6”, RFC1885, December 1995
[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
[WAE]	WAP Wireless Application Group, Wireless Application Environment Specification 30-April-1998
[WAP]	WAP Architecture Working Group “Wireless Application Protocol Architecture Specification”, version 1.0
[WDP]	WAP Wireless Transport Group, Wireless Datagram Protocol Specification 30-April-1998
[WTP]	WAP Wireless Transport Group, Wireless Transaction Protocol Specification 30-April-1998

4. Abbreviations

For the purposes of this specification the following abbreviations apply.

ETSI	European Telecommunication Standardisation Institute
IE	Information Element
IP	Internet Protocol
LSB	Least significant bits
MSISDN	Mobile Subscriber ISDN (Telephone number or address of device)
MS	Mobile Station
MSB	Most significant bits
SMSC	Short Message Service Centre
SMS	Short Message Service
TCP/IP	Transmission Control Protocol/Internet Protocol
UDH	User-Data Header (see GSM 03.40)
UDP	Unreliable Datagram Protocol
USSD	Unstructured Supplementary Service Data
USSDC	Unstructured Supplementary Service Data Centre
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WSP	Wireless Session Protocol
WTP	Wireless Transaction Protocol

5. Terminology

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.)

6. WCMP Architectural Overview

Figure 6.1 shows a general model of the WAP protocol architecture and how WCMP fits into that architecture.

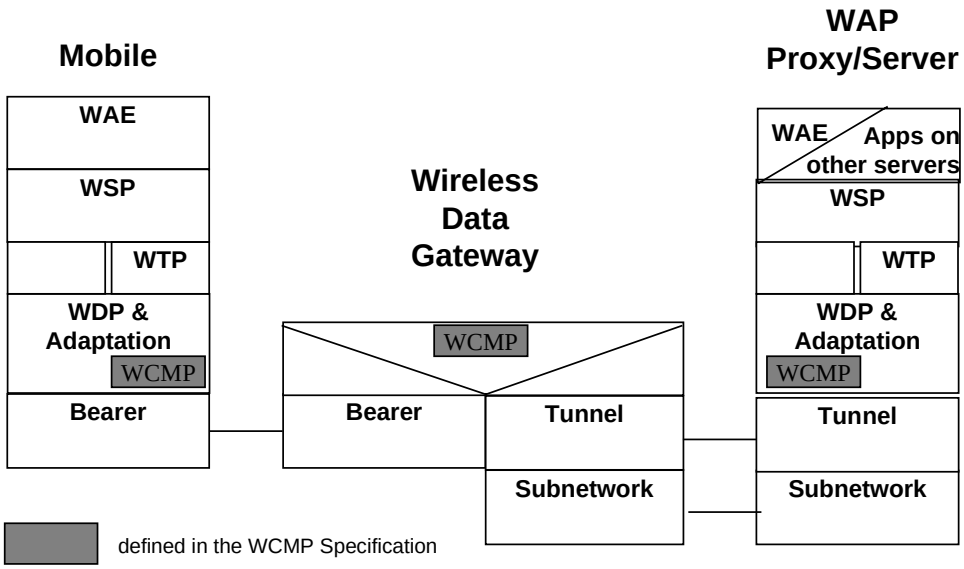

Figure 6.1 WCMP in the WAPArchitecture

The Transport layer protocol in the WAP architecture is the Wireless Datagram Protocol (WDP). The WDP protocol operates above the data capable bearer services supported by multiple network types. WDP offers a consistent but unreliable service to the upper level protocols of WAP and communicates transparently over one of the available bearer services.

WCMP is used by WDP nodes and Wireless Data Gateways to report errors encountered in processing datagrams. WCMP can also be used for informational and diagnostic purposes.

7. WCMP Protocol Description

7.1 General

The Wireless Control Message Protocol (WCMP) is used in environments that do not provide an IP bearer. WCMP is used by WDP nodes and Wireless Data Gateways to report errors encountered in processing datagrams. WCMP messages are usually generated by the WDP layer, the management entity or a higher layer protocol. WCMP can also be used for informational and diagnostic purposes.

WCMP error message MUST NOT be generated in response to another WCMP error message. To report an error related to a fragmented datagram, more than one WCMP message MUST NOT be sent. Additionally, one WCMP MUST fit to a single bearer level fragment.

The Wireless Control Message Protocol (WCMP) provides an efficient error handling mechanism for WDP, resulting in improved performance for WAP protocols and applications.

7.2 Static WCMP Conformance Clause

This static conformance clause defines a minimum set of WCMP features that can be implemented to ensure that the implementation will be able to interoperate.

WCMP Message	WCMP Type	WCMP Code	Mandatory / Optional		Note
Destination Unreachable	**51**				
• No route to destination		0	WDP Node	N/A	
			Wireless Data Gw	O	
• Communication administratively prohibited		1	WDP Node	N/A	
			Wireless Data Gw	O	
• Address unreachable		3	WDP Node	N/A	
			Wireless Data Gw	O	
• Port unreachable		4	WDP Node	M	
			Wireless Data Gw	N/A	
Parameter Problem	**54**				
• Erroneous header field		0	WDP Node	O	
			Wireless Data Gw	O	
Message Too Big	**60**	0	WDP Node	M	
			Wireless Data Gw	N/A	
Reassembly Failure	**61**				
• Reassembly time exceeded		1	WDP Node	O	
			Wireless Data Gw	N/A	
• Buffer Overflow		2	WDP Node	O	
			Wireless Data Gw	N/A	
Echo Request	**178**	0	WDP Node	O	
			Wireless Data Gw	N/A	
Echo Reply	**179**	0	WDP Node	M	1)
			Wireless Data Gw	N/A	

Note 1) WCMP implementations MAY impose restrictions on the quantity of Echo Reply messages generated, to protect for example from network overload or denial of service attacks.

7.3 WCMP in IP networks

In IP based networks, the functionality of the WCMP is implemented by using the Internet Control Message Protocol (ICMP). ICMP is defined in [RFC 792] for IPv4 and [RFC 1885] for IPv6.

At the time of publication, the known IP-based bearer networks that will use ICMP are GSM CSD, GSM GPRS, TDMA CSD, CDPD, CDMA CSD, iDEN CSD, iDEN Packet Data and CDMA Packet Data.

7.4 WCMP in non-IP networks

7.4.1 WCMP in GSM SMS

For GSM SMS, the User Data Header (UDH) framework as defined in GSM 03.40 is used. The WCMP messages are carried in the UDH in an Information Element. A new WCMP Information Element Identifier (IEI) must be reserved for this purpose from ETSI.

The WDP datagram protocol operates on top of the SMS Transfer Layer and has a need to report errors unique to the datagram layer, end to end. This is done by using WCMP. Error messages supported by WCMP deal e.g. with erroneous port numbers, failures when re-assemble a segmented message and parameter errors in the WDP header. These datagram related errors occur above the SMS transfer layer.

Failures to transfer or process a short message at the SMS transfer layer are reported using the SMS-SUBMIT-REPORT, SMS-DELIVER-REPORT, and SMS-STATUS-REPORT protocol data units. These messages may trigger the SMSC to generate WCMP messages if needed.

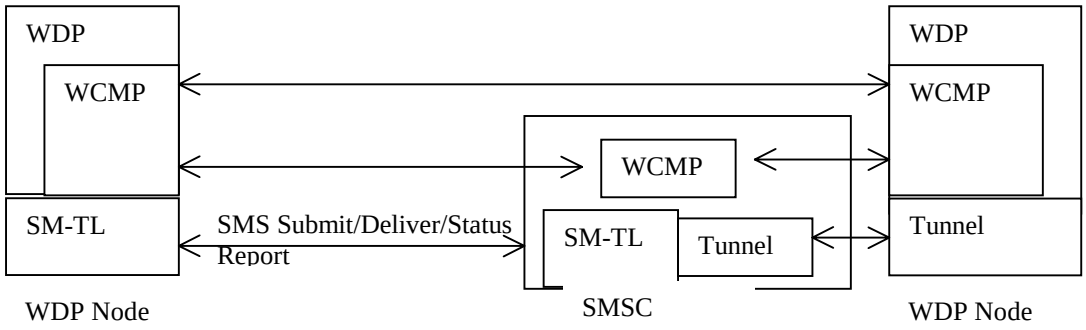

Figure 7.1 Error reporting protocols for WDP and the Short Message Transfer Layer.

The complete list of SMS transfer layer failure causes can be found in [GSM0340].

7.4.2 WCMP in GSM USSD

For GSM USSD, the User Data Header (UDH) framework as defined in GSM 03.40 is used. The WCMP messages are carried in the UDH in an Information Element. A new WCMP Information Element Identifier (IEI) must be reserved for this purpose from ETSI.

7.4.3 WCMP in FLEX and ReFLEX

To be defined later.

7.4.4 WCMP in CDMA SMS

To be defined later.

7.4.5 WCMP in iDEN SMS

To be defined later.

7.4.6 WCMP in TDMA R-data

To be defined later.

7.5 WCMP Messages

7.5.1 General Message Structure

Network bit order for bit fields is "big-endian". In other words, the left-most bit in the bit field is the most significant bit of the octet and is transmitted first followed subsequently by less significant bits. In two-byte fields, the first byte is the high order byte.

Bit/Octet	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
1	Type of Control Message							
2	Code of Control Message							
3 - N	Data Fields for WCMP (0 .. N octets)							

Fig. 7.1 General format of a WCMP message

Different WCMP messages are identified by the Type and Code fields. The Type field indicates the type of the message. Its value determines the format of the remaining data. The Code field depends on the message type and defines the format of the Data Fields.

WCMP messages are grouped into two classes, error messages and informational messages. Error messages have message types from 0 to 127, informational messages have message types from 128 to 191. Types 192 – 255 are reserved for future purposes.

WCMP Type values are different from ICMP Type values. WCMP Type values have been selected by adding 50 to the respective ICMP Type. WCMP Codes are the same than in ICMP.

Message Description	***WCMP MsgType***	***WCMP Code***
Destination Unreachable	**51**	
• No route to destination		0
• Communication administratively prohibited		1
• Address unreachable		3
• Port unreachable		4
Parameter Problem	**54**	
• Erroneous header field		0
Message Too Big	**60**	0
Reassembly Failure	**61**	
• Reassembly time exceeded		1
• Buffer Overflow		2
Echo Request	**178**	0
Echo Reply	**179**	0

Fig. 7.2 Types and Codes for WCMP messages.

7.5.2 Address Information Formats

The following Address Information field format MUST be used in the WCMP messages:

Bit/Octet	7	6	5	4	3	2	1	0
1	Address Type = GSM							
2	Address Length							
3 – N	Address Data							

If the Address Type is GSM, the Address Data MUST be coded using the semi-octet representation defined in GSM 03.40.

Bit/Octet	7	6	5	4	3	2	1	0
1	Address Type = IPv4							
2	Address Length							
3	32 bit IP address							
4								
5								
6								

Bit/Octet	7	6	5	4	3	2	1	0
1	Address Type = IPv6							
2	Address Length							
3	1-32 bits of IP address							
4								
5								
6								
7	33-64 bits of IP address							
8								
9								
10								
11	65-96 bits of IP address							
12								
13								
14								
15	97-128 bits of IP address							
16								
17								
18								

If the Address Type is IPv4 or IPv6, the address MUST be coded with the most significant bit first.

Bit/Octet	7	6	5	4	3	2	1	0
1	Address Type = FLEX							
2	Address Length							
3 – N	Address Data							

Bit/Octet	7	6	5	4	3	2	1	0
1	Address Type = ReFLEX							
2	Address Length							
3	R	I	30 bit ReFLEX address					
4								
5								
6								

If the Address Type is FLEX, the Address Data MUST be coded according to [FLEX], Section 6.12, FLEX Capcodes.

If the Address Type is ReFLEX, the Address Data MUST be coded according to [ReFLEX]. The I-bit identifies whether the address is a personal or information services address. The R-bit (reserved), should be set to 0.

The assigned Address Type values for different bearers are specified in [WDP].

7.5.3 WCMP Messages

7.5.3.1 Destination Unreachable

Bit/Octet	7	6	5	4	3	2	1	0
1	Type of Control Message							
2	Code of Control Message							
3	Destination port of original datagram							
4								
5	Originator port of original datagram							
6								
7 – N	Address Information							

Description

A Destination Unreachable message SHOULD be generated by the receiving WDP node in response to a packet that cannot be delivered to its destination for reasons other than congestion. When the reason is 'Port Unreachable', the WDP node MUST send a Destination Unreachable message.

A Destination Unreachable message SHOULD be generated by Wireless Data Gateways (e.g. SMSC, USSDC) when it cannot route the datagram to a WAP Gateway.

A WCMP message MUST NOT be generated if a packet is dropped due to congestion.

Type 51

Code

0 If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table (e.g. in the SMSC or USSDC), the Code field is set to 0 (No Route To Destination).

1 If the reason for the failure to deliver is administrative prohibition, e.g., a node acts as a "firewall filter", the Code field is set to 1 (Communication Administratively Prohibited).

3 If there is another reason for the failure to deliver, e.g., inability to resolve the WDP destination address into a corresponding link or device address, or a link-specific problem of some sort, then the Code field is set to 3 (Address unreachable).

4 If the transport protocol (e.g. WDP) does not have a listener for a particular port, the destination node MUST send a Destination Unreachable message with Code 4 (Port Unreachable).

Address Information

The Address is the Destination Address of the original datagram.

7.5.3.2 Parameter Problem

Bit/Octet	7	6	5	4	3	2	1	0
1	Type of Control Message							
2	Code of Control Message							
3 – N	Address Information							
N + 1	Index (Value 0 – 64)							
N + 2 – N + 65	Data From The Original Datagram (64 octets)							

Description

If a WDP node processing a packet finds a problem with a field in the WDP header such that it cannot complete processing the packet, it MUST discard the packet and SHOULD send a WCMP Parameter Problem message to the packet's source.

Type 54

Code 0 - erroneous header field encountered

Address Information

The Address is the Destination Address of the original datagram.

Index

Index to point to the octet in the original datagram which caused the problem. When the index cannot point to that octet it MUST be set to zero.

Data From The Original Datagram

64 octets from the beginning of the original datagram.

7.5.3.3 Message Too Big

Bit/Octet	7	6	5	4	3	2	1	0
1	Type of Control Message							
2	Code of Control Message							
3	Destination port of original datagram							
4								
5	Originator port of original datagram							
6								
7 – N	Address information							
N + 1	Maximum message size in octets							
N + 2								

Description

The Message Too Big message MUST be used to inform the sending party about buffer size limitations of the receiver. It MUST be used when the first datagram of a segmented message is received and there is not enough buffer space for the whole message.

Type 60

Code 0

Address Information

The Address is the Destination Address of the original datagram.

7.5.3.4 Reassembly Failure

Bit/Octet	7	6	5	4	3	2	1	0
1	Type of Control Message							
2	Code of Control Message							
3	Destination port of original datagram							
4								
5	Originator port of original datagram							
6								
7 – N	Address Information							

Description

If a node reassembling a fragmented datagram cannot complete the reassembly it MAY send a Reassembly Failure message. The node SHOULD discard the datagram.

If the first fragment of a segmented message is not available, the Reassembly Failure message SHOULD NOT be sent however all fragments for the given message SHOULD be silently discarded.

Type 61

Code

1 Fragment reassembly time exceeded
2 Buffer overflow

Address Information

The Address is the Destination Address of the original datagram.

7.5.3.5 WCMP Echo Request/Reply

Bit/Octet	7	6	5	4	3	2	1	0
1	Type of Control Message							
2	Code of Control Message							
3	Identifier number							
4								
5	Sequence number							
6								
7 – N	Data							

Description

A WDP node MUST implement a WCMP Echo function that receives Echo Requests and sends corresponding Echo Replies. A node SHOULD also implement an application-layer interface for sending Echo Requests and receiving Echo Replies, for diagnostic purposes.

The data received in the WCMP Echo Request message MUST be returned entirely and unmodified in the WCMP Echo Reply message, unless the Echo Reply would exceed the MTU of the path back to the Echo requester, in which case the data is truncated to fit that path MTU.

Type 178 Echo Request
179 Echo Reply

Code 0

Identifier Number

The Identifier Number is used as an aid to match Echo Replies to this Echo Request. May be zero.

Sequence Number

The Sequence Number is used as an aid to match Echo Replies to this Echo Request. May be zero.

Data

The Data can be zero or more octets of arbitrary data.

Appendix A. History and Contact Information

Document history		
Date	**Status**	**Comment**
30-Apr-1998	Draft Specification	First version.
12-June-1998	Specification	First version.

Contact Information

http://www.wapforum.org.

technical.comments@wapforum.org