

FOUNDATION FOR INTELLIGENT PHYSICAL AGENTS

FIPA Nomadic Application Support Specification

Document title	FIPA Nomadic Application Support Specification		
Document number	XC00014D	Document source	FIPA Nomadic Application Support TC
Document status	Experimental	Date of this status	2001/08/10
Supersedes	FIPA00062, FIPA00063, FIPA00065, FIPA00066		
Contact	fab@fipa.org		
Change history			
2000/09/28	Approved for Experimental		
2001/08/10	Line numbering added		

© 2000 Foundation for Intelligent Physical Agents - <http://www.fipa.org/>

Geneva, Switzerland

Notice

Use of the technologies described in this specification may infringe patents, copyrights or other intellectual property rights of FIPA Members and non-members. Nothing in this specification should be construed as granting permission to use any of the technologies described. Anyone planning to make use of technology covered by the intellectual property rights of others should first obtain permission from the holder(s) of the rights. FIPA strongly encourages anyone implementing any part of this specification to determine first whether part(s) sought to be implemented are covered by the intellectual property of others, and, if so, to obtain appropriate licenses or other permission from the holder(s) of such intellectual property prior to implementation. This specification is subject to change without notice. Neither FIPA nor any of its Members accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from the use of this specification.

18 **Foreword**

19 The Foundation for Intelligent Physical Agents (FIPA) is an international organization that is dedicated to promoting the
20 industry of intelligent agents by openly developing specifications supporting interoperability among agents and agent-
21 based applications. This occurs through open collaboration among its member organizations, which are companies and
22 universities that are active in the field of agents. FIPA makes the results of its activities available to all interested parties
23 and intends to contribute its results to the appropriate formal standards bodies.

24 The members of FIPA are individually and collectively committed to open competition in the development of agent-
25 based applications, services and equipment. Membership in FIPA is open to any corporation and individual firm,
26 partnership, governmental body or international organization without restriction. In particular, members are not bound to
27 implement or use specific agent-based standards, recommendations and FIPA specifications by virtue of their
28 participation in FIPA.

29 The FIPA specifications are developed through direct involvement of the FIPA membership. The status of a
30 specification can be either Preliminary, Experimental, Standard, Deprecated or Obsolete. More detail about the process
31 of specification may be found in the FIPA Procedures for Technical Work. A complete overview of the FIPA
32 specifications and their current status may be found in the FIPA List of Specifications. A list of terms and abbreviations
33 used in the FIPA specifications may be found in the FIPA Glossary.

34 FIPA is a non-profit association registered in Geneva, Switzerland. As of January 2000, the 56 members of FIPA
35 represented 17 countries worldwide. Further information about FIPA as an organization, membership information, FIPA
36 specifications and upcoming meetings may be found at <http://www.fipa.org/>.

37 Contents

38	1	Scope	1
39	2	General Analysis	2
40	2.1	Overview	2
41	2.2	Monitoring and Controlling Quality of Service	3
42	2.3	Negotiation of Message Transport Requirements	4
43	2.3.1	Negotiation About Message Transport Protocols	4
44	2.3.2	Negotiation About Message Representation	4
45	3	Nomadic Application Support Ontology	5
46	3.1	Object Descriptions	5
47	3.1.1	Quality of Service Description	5
48	3.1.2	Rate Value	6
49	3.1.3	Time Value	7
50	3.1.4	Probability Value	7
51	3.1.5	Change Constraint	8
52	3.1.6	Time Constraint	8
53	3.1.7	Communication Channel Description	8
54	3.1.8	Transport Protocol Description	9
55	3.1.9	Transport Protocol Selection	9
56	3.1.10	Message Representation Description	9
57	3.1.11	Message Representation Selection	10
58	3.2	Function and Predicate Descriptions	11
59	3.2.1	Request Monitoring Information	11
60	3.2.2	Subscribe to Changes	12
61	3.2.3	Open Communication Channel	12
62	3.2.4	Close Communication Channel	12
63	3.2.5	Activate a Message Transport Protocol	13
64	3.2.6	Deactivate a Message Transport Protocol	13
65	3.2.7	Select a Message Transport Protocol	13
66	3.3	Exceptions	13
67	3.3.1	Not Understood Exception Propositions	13
68	3.3.2	Refusal Exception Propositions	14
69	3.3.3	Failure Exception Propositions	14
70	4	Registration of the Control Agent and Monitor Agent with the DF	15
71	5	Scenarios	16
72	5.1	Registration with a DF	16
73	5.2	Negotiating Message Transport Protocols	17
74	5.3	Negotiating Message Representations	21
75	5.4	Message Exchange Over a WAP Message Transport Protocol	22
76	5.4.1	Message Exchange Activation by an Agent in a Mobile Host	23
77	5.4.2	Message Exchange Termination to an Agent in a Mobile Host	25
78	6	Informative Annex A — Paramedic Scenario	28
79	6.1	Overview	28
80	6.2	Seamless Roaming	30
81	6.2.1	Disconnection and Reconnection of an Message Transport Connection	30
82	6.2.2	Example Negotiation of a Message Transport Protocol	35
83	6.2.3	Example Negotiation of a Message Representation	38
84	7	References	41
85			

85 **1 Scope**

86 This document is part of the FIPA specifications and deals with agent middleware to support applications in nomadic
87 environment. The environment of mobile computing is very different compared to today's environment of traditional
88 distributed systems in many respects. Bandwidth, latency, delay, error rate, interference, interoperability, computing
89 power, quality of display, among other things may change dramatically as a nomadic end-user moves from one location
90 to another. All these cause new demands for adaptability of data services.

91
92 Adaptability to the changes in the environment of nomadic end-users is an important issue. A nomadic end-user
93 confronted with these circumstances would benefit from having the following functionality provided by the infrastructure:
94 information about expected performance, agents controlling over the transfer operations, a condition-based control
95 policy, capability provided by agents to work in a disconnected mode, advanced error recovery methods, and
96 adaptability.

97
98 This specification gives an overview of the Nomadic Application Support area and contains specifications for:

- 99
100 Monitor Agent (MA) functionality,
- 101
102 Control Agent (CA) functionality, and,
- 103
104 An ontology for representing the quality of service of the Message Transport Service in the context of nomadic
105 application support.

106
107 In addition, two other FIPA specifications are related to Nomadic Application Support: FIPA Agent Message Transport
108 Protocol for WAP Specification [FIPA00076] and FIPA ACL Message Representation in Bit-Efficient Encoding
109 Specification [FIPA00069].

110
111

111 2 General Analysis

112 2.1 Overview

113 The results of current developments in both wireless data communications and mobile computers are being combined
 114 to facilitate a new trend: *nomadic computing*. Compared to today's traditional distributed systems, the nomadic
 115 computing environment is very different in many respects. Bandwidth, latency, delay, error rate, quality of display and
 116 other non-functional parameters may change dramatically when a nomadic end-user moves from one location to
 117 another and thus from one computing environment to another, for example, from a wireline LAN to a UMTS network.
 118 The variety of mobile workstations, handheld devices and smart phones, which allow nomadic end-users to access
 119 Internet services, is increasing rapidly. The capabilities of mobile devices range from very low performance equipment
 120 (such as PDAs) up to high performance laptop PCs. All these devices create new demands for adaptability of Internet
 121 services. For example, PDAs cannot display properly high quality images and as nomadic end-users may be charged
 122 based on the amount of data transmitted over the GPRS-UMTS network, they may have to pay for bits that are totally
 123 useless to them.

124
 125 Confronted with these circumstances, the nomadic end-user would benefit from having the following functionality
 126 provided by the infrastructure: information about expected performance, agent monitoring and controlling the transfer
 127 operations, and adaptability.

128
 129 The ability to automatically adjust to changes in a transparent and integrated fashion is essential for *nomadicity*;
 130 nomadic end-users are usually professionals in areas other than computing. Furthermore, today's mobile computer
 131 systems are already very complex to use as productivity tools. Thus, nomadic end-users need all the support that a
 132 FIPA agent-based distributed system can deliver and adaptability to the changes in the environment of nomadic end-
 133 users is an important issue.

134
 135 FIPA uses the Wireless Application Protocol (WAP) [WAP99] as its wireless Message Transport Protocol (MTP - see
 136 [FIPA00076]). The WAP Forum has developed industry-wide specifications for low bandwidth wireless services (such
 137 as GSM, GPRS, etc.) and wireless devices (such as mobile telephones and personal digital assistants). The WAP
 138 specification address the characteristics of wireless networks by adapting low bandwidth wireless services and low-end
 139 mobile devices to the special requirements of information services. The WAP specification defines a set of standard
 140 components that can be used in agent message communication, such as standard data formats and standard data
 141 communication protocols.

142
 143 The adaptation of applications to various nomadic computing environments is an important area. There are several
 144 tasks that agents need to carry out during application adaptation:

- 145 1. Selection of MTP and Message Transport Connection (MTC) to be used for agent communication.
- 146 2. Selection of an ACL and content language representation to be used for agent communication.
- 147 3. Provision of support for application agents to carry out adaptation of application data, such as still images, video
 148 and audio, XML, etc. Today's Internet application data (such as multimedia content) are designed with high
 149 performance desktop PCs and high quality displays in mind. Therefore, the application data is frequently unsuitable
 150 for nomadic computing using wireless wide-area networks and low performance mobile devices, and hence
 151 requires modification.
- 152 4. Communication between agents performing adaptation.

153
 154 The FIPA Nomadic Application Support specifications define agent middleware to:

155
 156 Monitor and control an MTP and the underlying MTC, and,

157
 158 An ontology for representing the quality of service of the Message Transport Service in the context of nomadic
 159 application support.

164 In addition, this specification gives examples of the use of the above scenarios.
 165

166 **2.2 Monitoring and Controlling Quality of Service**

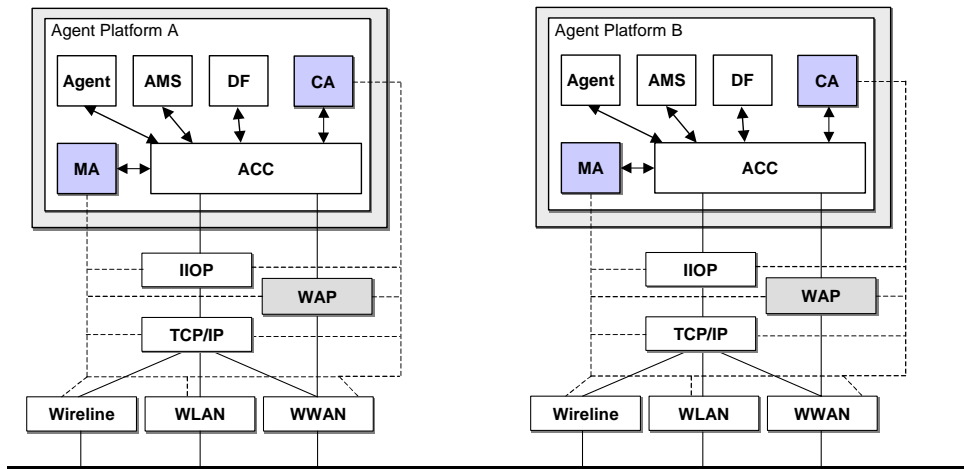
167 The functions required to carry out monitoring and controlling for quality of service can be split into several specific
 168 tasks:

- 169
- 170 1. Observing the quality of service of MTPs and MTCs,
 - 171
 - 172 2. Measuring (if there are no other means to obtain the required information) the quality of service of an MTP and
 173 MTC,
 - 174
 - 175 3. Collecting information from the observing and measuring sources,
 - 176
 - 177 4. Analysing the information, and,
 - 178
 - 179 5. Controlling an MTC and selecting an MTP.

180 Based on this division, the agent middleware consists of the following logical agents (see Figure 1):

181 A **Monitor Agent (MA)** which carries out tasks 1 through 4, and,

182
 183 A **Control Agent (CA)** which carries out task 5.
 184
 185
 186



187
 188
 189 **Figure 1: Reference Model of Agent based Adaptation**
 190

191 The most appropriate configuration of MAs and CAs is that there is at least one pair in each AP involving adaptation.
 192 The MA may measure the actual quality of service of an MTC, if the network running an MTC does not provide users
 193 with required performance data¹.

194 An MA may:

195
 196 Consist of network-service-specific components that collect raw performance data at fixed intervals,

197
 198 Provide a repository for the measurement data collected,

199
 200 Perform first level analysis of the collected data, and,
 201
 202

¹ The way this actual measurement is performed is not a subject of standardisation within FIPA.

203 Send the results of the analysis to CA, if requested to do so.

204

205 A CA may:

206

207 Manage (establish, close, suspend, activate, etc.) an MTC².

208

209 In some cases there is a need for MAs and CAs in heterogeneous APs to communicate with each other; therefore,
210 interaction protocols and ontologies to achieve this are specified in this document.

211

212 2.3 Negotiation of Message Transport Requirements

213 There are several mechanisms that can determine the MTP, message representation and content language to use
214 between communicating entities:

215

216 Communicating entities know a peer entity's preferences beforehand and use them.

217

218 The activating entity tries to use a method and if the peer entity is not capable of using the suggested method, then
219 the activating entity may try another one (and so on).

220

221 The communicating entities negotiate about a method to be used.

222

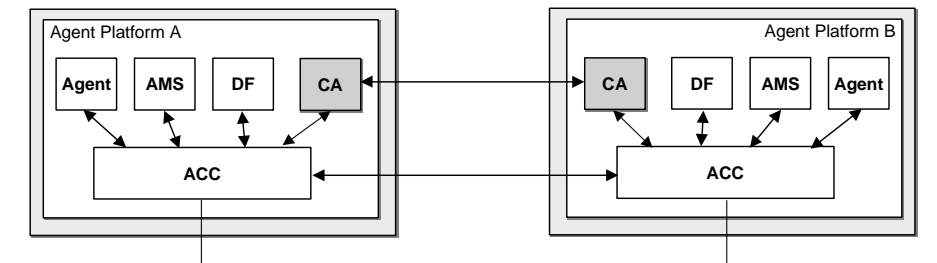
223 2.3.1 Negotiation About Message Transport Protocols

224 Previous FIPA specifications have implicitly assumed that the MTC is operational all the time (meaning that the MTC
225 has been established before the agent message exchange and that it is reliable). However, this is not always the case
226 within a nomadic environment.

227

228 A CA can activate the selection of an MTP or an agent can propose an MTP to a CA and it is the responsibility of the
229 CA to either accept or reject the proposal based on whether it is possible to use the proposed MTP. CAs negotiate with
230 peer CAs to use proposed MTPs which is illustrated in *Figure 2*.

231



232

233

234

235

236 CAs use the `FIPA-Propose` interaction protocol [FIPA00036] and the `use` action to negotiate about an MTP. An
237 example negotiation is given in section 5.2, *Negotiating Message Transport Protocols*.

238

239 2.3.2 Negotiation About Message Representation

240 In the environment of nomadic applications, it may be necessary to switch from one ACL representation to another; for
241 example, when a mobile host roams from a wireline network to a wireless network. Application agents may use the
242 `FIPA-Propose` interaction protocol and the `use` action to negotiate about the representation of ACL. Examples of this
243 negotiation are given in section 5.3, *Negotiating Message Representation*.

244

² The way that management actions are executed is not a subject of standardisation within FIPA.

244 3 Nomadic Application Support Ontology

245 The FIPA-Nomadic-Application ontology is a combination of FIPA-MTS-QoS, FIPA-Communication-
246 Management, and FIPA-Message-Representation ontologies.

247 3.1 Object Descriptions

248 This section describes a set of frames, that represent the classes of objects in the domain of discourse within the
249 framework of the FIPA-Nomadic-Application ontology.

250
251 The following terms are used to describe the objects of the domain:

252
253 **Frame.** This is the mandatory name of this entity, that must be used to represent each instance of this class.

254
255 **Ontology.** This is the name of the ontology, whose domain of discourse includes the parameters described in the
256 table.

257
258 **Parameter.** This is the mandatory name of a parameter of this frame.

259
260 **Description.** This is a natural language description of the semantics of each parameter.

261
262 **Presence.** This indicates whether each parameter is mandatory or optional.

263
264 **Type.** This is the type of the values of the parameter: Integer, Word, String, URL, Term, Set or Sequence.

265
266 **Reserved Values.** This is a list of FIPA-defined constants that can assume values for this parameter.
267

268 3.1.1 Quality of Service Description

269 This type of object represents the quality of service of the transport protocol or communication channel.
270

Frame Ontology	qos FIPA-MTS-QoS	Parameter	Description	Presence ³	Type	Reserved Values
line-rate	The bandwidth in one direction over the link.	Optional	rate-value			
throughput	The number of user data bits successfully transferred in one direction across the link ⁴ . Successful transfer means that no user data bits are lost, added or inverted in transfer.	Optional	rate-value			
throughput-std-dev	The current standard deviation of the throughput within a time unit.	Optional	rate-value			
rtt	The round trip time which is the time required for a data segment to be transmitted to a peer entity and a corresponding acknowledgement sent back to the originating entity.	Optional	time-value			
rtt-std-dev	The standard deviation of the round-trip time within a time unit.	Optional	time-value			

³ While all of the parameters for this object are optional, a valid qos object will contain at least one parameter.

⁴ See [ITU135].

delay	The (nominal) time required for a data segment to be transmitted to a peer entity.	Optional	time-value	
delay-std-dev	The standard deviation of the delay time within a time unit.	Optional	time-value	
mean-up-time	The expected uptime of an established link.	Optional	time-value	
omission-rate	The probability that a data segment is not transmitted correctly over a link.	Optional	probability-value	
ber	The ratio of the number of bit errors to the total number of bits transmitted in a given time interval ⁵ .	Optional	probability-value	
frame-error-rate	The probability that a data segment is not transmitted correctly over a link.	Optional	probability-value	
conn-setup-delay	The (sampled) delay to establish a connection between communicating entities.	Optional	time-value	
conn-setup-failure-prob	The ratio of total call attempts that result in call setup failure to the total call attempts in a population of interest.	Optional	probability-value	
status	The connectivity status of the link. <i>Connected</i> means that there (at least) logical connection between communicating entities. <i>Disconnected</i> means that there is no connection between communicating entities, and the communicating entities are not establishing a connection at the moment. <i>Connecting</i> means that there is no connection between communicating entities, but they are currently establishing a connection between them.	Optional	Word	Connected Disconnected Connecting

271 **3.1.2 Rate Value**

272 This type of object represents a data transfer value.

273

Frame Ontology	rate-value FIPA-MTS-QoS			
Parameter	Description	Presence	Type	Reserved Values
direction	The direction in which this value is measured. <i>Inbound</i> means the data transmission where the actor receives the data, and <i>outbound</i> means the data transmission where the actor transmits the data.	Mandatory	Word	Inbound Outbound

⁵ See [ITUE800].

unit	The unit in which the value is represented. Bits/s means bits per seconds. Kbits/s means kilobits per seconds. One kilobit is 2 ¹⁰ bits. Mbits/s means megabits per second. One megabit is 2 ²⁰ bits. Gbits/s means gigabits per second. One gigabit is 2 ³⁰ bits.	Mandatory	Word	GBits/s Mbits/s KBits/s Bits/s
value	The rate value.	Mandatory	Number	

274

275 **3.1.3 Time Value**

276 This type of object represents a time value.

277

Frame Ontology	time-value FIPA-MTS-QoS			
Parameter	Description	Presence	Type	Reserved Values
direction	The direction in which this value is measured. Inbound means the data transmission where the actor receives the data, and outbound means the data transmission where the actor transmits the data.	Optional ⁶	Word	Inbound Outbound
unit	The unit in which the value is represented. h means hours, m means minutes, s means seconds, and ms means milliseconds.	Mandatory	Word	h m s ms
value	The time value.	Mandatory	Number	

278

279 **3.1.4 Probability Value**

280 This type of object represents a probability value.

281

Frame Ontology	probability-value FIPA-MTS-QoS			
Parameter	Description	Presence	Type	Reserved Values
direction	The direction in which this value is measured. Inbound means the data transmission where the actor receives the data, and outbound means the data transmission where the actor transmits the data.	Optional	Word	Inbound Outbound
value	The probability value which obeys the following axiom: 0 • value • 1	Mandatory	Number	

282

283

⁶ This parameter is mandatory for those QoS values that have a different value depending upon the direction.

283 **3.1.5 Change Constraint**

284 This type of object represents constraints that limit quality of service notifications.

285

Frame Ontology	change-constraint FIPA-MTS-QoS			
Parameter	Description	Presence	Type	Reserved Values
value	The description of the constraints.	Mandatory	Expression	

286

287 **3.1.6 Time Constraint**

288 This type of object represents constraints that limit quality of service notifications.

289

Frame Ontology	time-constraint FIPA-MTS-QoS			
Parameter	Description	Presence	Type	Reserved Values
type	The type of the constraint. If the type <code>Every</code> is used, then the expression becomes true after <code>value</code> and thereafter at intervals of <code>value</code> . If the type <code>After</code> is used, then the expression becomes true only after <code>value</code> .	Mandatory	Word	Every After
value	The time value.	Mandatory	time-value	

290

291 **3.1.7 Communication Channel Description**

292 This type of object represents a communication channel.

293

Frame Ontology	comm-channel FIPA-Communication-Management			
Parameter	Description	Presence ⁷	Type	Reserved Values
name	The logical name of the communication channel.	Optional	Word	
target-addr	The target transport address of the communication channel. This may also be the address of a gateway ACC.	Optional	URL	
options	A list of optional parameters for the communication channel.	Optional	Set of property (see [FIPA00023])	

294

295

⁷ Either the `:name` parameter or the `:target-addr` parameter must be present in this object.

295 **3.1.8 Transport Protocol Description**

296 This type of object represents a transport protocol.

297

Frame Ontology	transport-protocol FIPA-Communication-Management			
Parameter	Description	Presence	Type	Reserved Values
Name	The logical name of the transport protocol.	Mandatory	Word	
gw-addr	The transport address of the gateway ACC.	Optional	URL	
dest-addr	The transport address of the ultimate destination. If this address is present, but gw-addr is not, then the Control Agent may select the most appropriate gateway transport address to use.	Optional	URL	
options	A list of optional parameters for the transport protocol.	Optional	Set of property	

298

299 **3.1.9 Transport Protocol Selection**

300 This type of object represents a selection of transport protocol.

301

Frame Ontology	transports FIPA-Communication-Management			
Parameter	Description	Presence	Type	Reserved Values
send	A list of transport protocols supported for sending messages.	Mandatory	Sequence of transport-protocol	
recv	A list of transport protocols supported for receiving messages.	Mandatory	Sequence of transport-protocol	

302

303 **3.1.10 Message Representation Description**

304 This type of object represents an ACL message representation.

305

Frame Ontology	msg-representation FIPA-Message-Representation			
Parameter	Description	Presence	Type	Reserved Values
Name	The name of the message representation.	Mandatory	Word	See [FIPA00068]
Options	A list of parameters for the message representation.	Optional	Set of property	

306

307

307 **3.1.11 Message Representation Selection**

308 This type of object represents a selection of message representations.

309

Frame Ontology	msg-rep-selection FIPA-Message-Representation			
Parameter	Description	Presence	Type	Reserved Values
send	A list of message representations supported for sending messages.	Mandatory	Sequence of msg-representation	
recv	A list of message representations supported for receiving messages.	Mandatory	Sequence of msg-representation	

310

311

312

3.2 Function and Predicate Descriptions

The following tables define usage and semantics of the functions and the predicates that are part of the FIPA-Nomadic-Application ontology.

The following terms are used to describe the functions of the FIPA-Nomadic-Application domain:

Function. This is the symbol that identifies the function in the ontology.

Predicate. This is the symbol that identifies the predicate in the ontology.

Ontology. This is the name of the ontology, whose domain of discourse includes the function or the predicate described in the table.

Supported by. This is the type of agent that supports this function or predicate.

Description. This is a natural language description of the semantics of the function or the predicate.

Domain. This indicates the domain over which the function predicate is defined. The arguments passed to the function or predicate must belong to the set identified by the domain.

Range. This indicates the range to which the function maps the symbols of the domain. The result of the function is a symbol belonging to the set identified by the range.

Arity. This indicates the number of arguments that a function or a predicate takes. If a function or a predicate can take an arbitrary number of arguments, then its arity is undefined.

3.2.1 Request Monitoring Information

Predicate	qos-information
Ontology	FIPA-Nomadic-Application
Supported by	MA
Description	<p>An agent asks for quality of service information from an MA using the FIPA-Query interaction protocol (see [FIPA00027]). The agent may specify either a communication channel or transport protocol to request quality of service information from.</p> <p>The predicate is true, when the values of the QoS parameters defined in the QoS object are true for given communication channel or transport protocol (i.e., the QoS of communication channel or transport protocol is what stated in the QoS object). Otherwise the predicate is false.</p>
Domain	comm-channel ⁸ / transport-protocol, ⁹ qos
Arity	2

⁸ Where '/' is "exclusive or".

⁹ Where ';' is "and".

340 **3.2.2 Subscribe to Changes**

Predicate	qos-notification
Ontology	FIPA-Nomadic-Application
Supported by	MA
Description	<p>An agent subscribes to notifications about changes to the quality of service from an MA using the FIPA-Subscribe interaction protocol (see [FIPA00035]).</p> <p>The predicate is true, when the values of the QoS parameters defined in the QoS object are true for given communication channel or transport protocol, and the given constraints are met. Otherwise the predicate is false.</p>
Domain	comm-channel, qos, change-constraints / time-constraints
Arity	3

341

342 **3.2.3 Open Communication Channel**

Function	open-comm-channel
Ontology	FIPA-Nomadic-Application
Supported by	CA
Description	<p>An agent can request that a CA open a communication channel. The communication channel description should contain enough information for a CA to be able to choose the right communication channel, that is, either the :name parameter or the :target-addr parameter must be present. The agent may also supply additional communication channel information by using the :options parameter.</p>
Domain	comm-channel
Range	The execution of this function results in a change of the state, but it has no explicit result. Therefore there is no range set.
Arity	1

343

344 **3.2.4 Close Communication Channel**

Function	close-comm-channel
Ontology	FIPA-Nomadic-Application
Supported by	CA
Description	<p>An agent can request that a CA close a communication channel. The communication channel description should contain enough information for a CA to be able to choose the right communication channel, that is, either the :name parameter or the :target-addr parameter must be present.</p>
Domain	comm-channel
Range	The execution of this function results in a change of the state, but it has no explicit result. Therefore there is no range set.
Arity	1

345

346

346 **3.2.5 Activate a Message Transport Protocol**

Function	activate
Ontology	FIPA-Nomadic-Application
Supported by	CA
Description	An agent can request that a CA activate a Message Transport Protocol (MTP). The transport protocol description should contain enough information to allow the CA to identify the correct transport protocol. Additionally, the agent may supply address information to where the transport protocol connection should be opened. It is possible to give the address of the gateway and/or the address of the destination AP.
Domain	Sequence of transport-protocol
Range	transport-protocol
Arity	1

347

348 **3.2.6 Deactivate a Message Transport Protocol**

Function	deactivate
Ontology	FIPA-Nomadic-Application
Supported by	CA
Description	An agent can request that a CA deactivate an MTP.
Domain	transport-protocol
Range	The execution of this function results in a change of the state, but it has no explicit result. Therefore there is no range set.
Arity	1

349

350 **3.2.7 Select a Message Transport Protocol**

Function	use
Ontology	FIPA-Nomadic-Application
Supported by	CA
Description	An CA can request another CA to select an MTP for use between Agent Communication Channels (ACCs) using the FIPA-Propose interaction protocol (see [FIPA00036]). The requesting CA shall provide enough information to establish a working MTP connection. The direction of communication (either send, receive or both) and the list of MTPs must be present. The list of MTPs is an ordered list where the highest priority is the first item and the lowest priority is the last item in the list. The receiving CA shall select at most one MTP for the proposed direction of communication (either send, receive or both)
Domain	transports
Range	transports
Arity	1

351

352 **3.3 Exceptions**

353 The exceptions for the FIPA-Nomadic-Application ontology follow the same form and rules as specified in
 354 [FIPA00023].

355

356 **3.3.1 Not Understood Exception Propositions**

357 The same set of "Not Understood Exception Propositions" as in the FIPA-Agent-Management ontology is used in the
 358 FIPA-Nomadic-Application ontology (see [FIPA00023]).

359

360 **3.3.2 Refusal Exception Propositions**

361 The same set of “*Refusal Exception Propositions*” as defined in the FIPA-Agent-Management ontology is used in
 362 FIPA-Nomadic-Application ontology (see [FIPA00023]). In addition, the FIPA-Nomadic-Application ontology
 363 defines the propositions given below.
 364

Communicative Act Ontology	Refuse FIPA-Nomadic-Application	
Predicate symbol	Arguments	Description
already-open	String	The specified communication channel is already open; the string identifies the communication channel.
not-open	String	The specified communication channel is not open; the string identifies the communication channel.
already-activated	String	The specified transport protocol is already activated; the string identifies the transport protocol.
not-active	String	The specified transport protocol is not active; the string identifies the transport protocol.
unrecognised-comm-channel	String	The specified communication channel is not recognised; the string identifies the communication channel.
unsupported-protocol	String	The specified transport protocol is not supported; the string identifies the transport protocol.

365

366 **3.3.3 Failure Exception Propositions**

Communicative Act Ontology	failure FIPA-Agent-Management	
Predicate symbol	Arguments	Description
internal-error	String	See [FIPA00023].
open-failed	String	The opening of a communication channel failed; the string identifies the failure reason.
transient-failed	String	The opening/closing of a communication channel or the activation/deactivation of a transport protocol failed; the string identifies the failure reason.
close-failed	String	The closing of a communication channel failed; the string identifies the failure reason.
activation-failed	String	The activation of a transport protocol failed; the string identifies the failure reason.
deactivation-failed	String	The deactivation of a transport protocol failed; the string identifies the failure reason.

367

4 Registration of the Control Agent and Monitor Agent with the DF

In order for a Control Agent and Monitor Agent to advertise its willingness to provide its services to an agent domain, it must register with a DF (as described in [FIPA00023]).

As part of this registration process following of constant values are introduced that universally identify the services the agent provides:

The name slot in `service-description` frame of a Control Agent must be declared as a constant `fipa-mts-control`.

The type slot in `service-description` frame of a Control Agent must be declared as a constant `fipa-ca`.

The ontology slot in `service-description` frame of a Control Agent should be declared as a constant `fipa-nomadic-application` or a constant `fipa-communication-management`.

The type slot in `service-description` frame of a Monitor Agent must be declared as a constant `fipa-mts-monitor`.

The type slot in `service-description` frame of a Monitor Agent must be declared as a constant `fipa-ma`.

The ontology slot in `service-description` frame of a Monitor Agent should be declared as a constant `fipa-nomadic-application`.

Below is given an example content of a agent `df-agent-description` frame which provides both MA and CA functionality:

```
(df-agent-description
  :name
    (agent-identifier
      :name monitor&control_agent@iiop://foo.com/acc
      :addresses (sequence iiop://foo.com/acc))
  :protocols (set fipa-request fipa-propose fipa-subscribe)
  :ontology (set fipa-nomadic-application)
  :language (set fipa-sl0)
  :services (set
    (service-description
      :name fipa-mts-control
      :type fipa-ca
      :ontology fipa-nomadic-application)
    (service-description
      :name fipa-mts-monitor
      :type fipa-ma
      :ontology fipa-nomadic-application))
  :ownership (set Sonera))))
```

411 **5 Scenarios**412 **5.1 Registration with a DF**

413 1. A CA registers with a DF (see [FIPA00023]):

```

414
415 (request
416   :sender
417     (agent-identifier
418       :name ca@foo.com
419       :addresses (sequence http://foo.com/acc))
420   :receiver (set
421     (agent-identifier
422       :name df@foo.com
423       :addresses (sequence http://foo.com/acc)))
424   :language FIPA-SL0
425   :protocol FIPA-Request
426   :ontology FIPA-Agent-Management
427   :content
428     (action
429       (agent-identifier
430         :name df@foo.com
431         :addresses (sequence http://foo.com/acc))
432       (register
433         (df-agent-description
434           :name
435             (agent-identifier
436               :name ca@foo.com
437               :addresses (sequence http://foo.com/acc))
438           :services (set
439             (service-description
440               :name fipa-mts-control
441               :type fipa-ca
442               :ontology (set FIPA-Nomadic-Application))))))))))
443

```

444 2. A MA registers with a DF:

```

445 (request
446   :sender
447     (agent-identifier
448       :name ma@foo.com
449       :addresses (sequence http://foo.com/acc))
450   :receiver (set
451     (agent-identifier
452       :name df@foo.com
453       :addresses (sequence http://foo.com/acc)))
454   :language FIPA-SL0
455   :protocol FIPA-Request
456   :ontology FIPA-Agent-Management
457   :content
458     (action
459       (agent-identifier
460         :name df@foo.com
461         :addresses (sequence http://foo.com/acc))
462       (register
463         (df-agent-description
464           :name
465             (agent-identifier
466               :name ma@foo.com
467               :addresses (sequence http://foo.com/acc))
468           :services (set
469             (service-description

```

```

470         :name fipa-mts-monitor
471         :type fipa-ma
472         :ontology (set FIPA-Nomadic-Application)))))))))
    
```

5.2 Negotiating Message Transport Protocols

This example shows a scenario, where an application agent requests the use of either the WAP MTP [FIPA00076] or a proprietary MTP (for example, x.uh.mdcP). The message flow of a successful negotiation is illustrated in Figure 3.

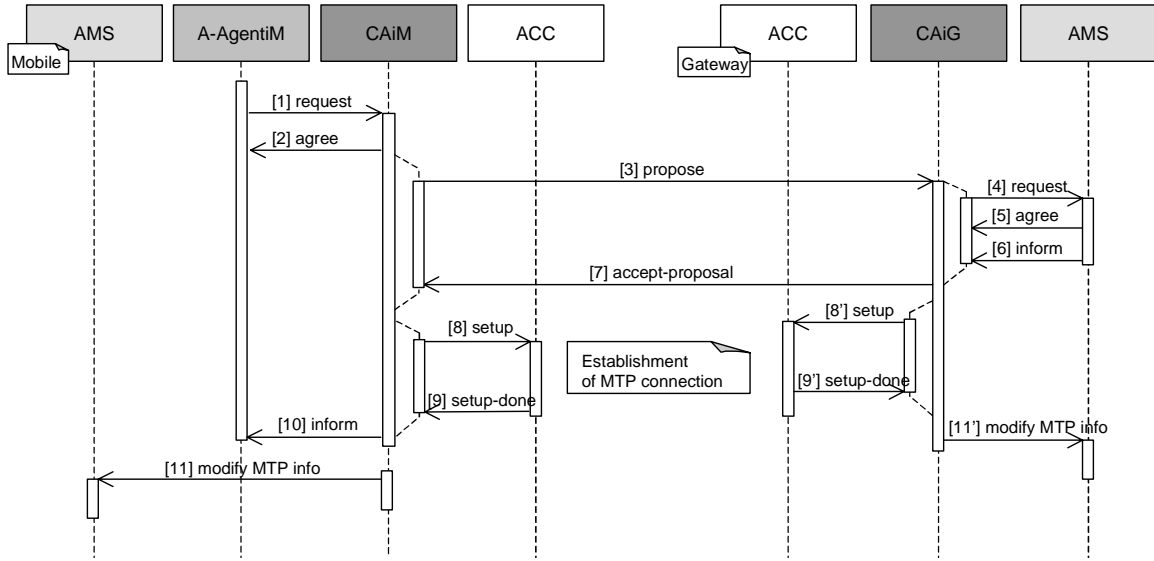


Figure 3: Flow of Message Transport Protocol Negotiation

1. Message 1 request: An application agent issues a request to the CA to activate either the fipa.mts.mtp.wap.std or x.uh.mdcP MTPs.

```

484 (request
485   :sender
486     (agent-identifier
487       :name A-AgentiM@mobile.com10)
488   :receiver (set
489     (agent-identifier
490       :name CaiM@mobile.com))
491   :ontology FIPA-Nomadic-Application
492   :language FIPA-SL0
493   :protocol FIPA-Request
494   :content
495     (action
496       (agent-identifier
497         :name CAiM@mobile.com)
498       (activate (sequence
499         (transport-protocol
500           :name x.uh.mdcP)
501         (transport-protocol
502           :name fipa.mts.mtp.wap.std
503           :dest-addr wap://gateway.com:1234/acc))))))
504
505
    
```

¹⁰ In all of the examples in this specification, the suffix of iM in an agent's name represents a mobile host, that is, an agent that is located on a mobile AP. Similarly, the suffix iG represents a gateway host and the suffix iF represents a fixed network host.

- 505 2. Message 2 agree: The CA agrees to activate an MTP. The decision to agree or disagree to activate an MTP might
 506 be based on the internal state of the CA (that is, the CA knows whether a requested MTP can be activated or not)
 507 or the CA might ask for an AP description from an AMS.

```

508
509 (agree
510   :sender
511     (agent-identifier
512       :name CAiM@mobile.com)
513   :receiver (set
514     (agent-identifier
515       :name A-AgentiM@mobile.com))
516   :ontology FIPA-Nomadic-Application
517   :language FIPA-SL0
518   :protocol FIPA-Request
519   :content
520     ((action
521       (agent-identifier
522         :name CAiM@mobile.com))
523      (activate (sequence
524        (transport-protocol
525          :name x.uh.mdcp)
526        (transport-protocol
527          :name fipa.mts.mtp.wap.std
528          :dest-addr wap://gateway.com:1234/acc))))
529     true))
530
```

- 531 3. Message 3 propose: The CA in the mobile host proposes to its peer CA in the gateway host that either the
 532 fipa.mts.mtp.wap.std or x.uh.mdcp MTPs should be used in communication between the APs.

```

533 <?xml version="1.0"?>11
534 <envelope>
535
536 <params index="1">
537
538   <to>
539     <agent-identifier>
540       <name>CAiG@gateway.com</name>
541     </agent-identifier>
542   </to>
543   <from>
544     <agent-identifier>
545       <name>CAiM@mobile.com</name>
546     </agent-identifier>
547   </from>
548
549   <acl-representation>fipa.acl.rep.string.std</acl-representation>
550
551   <date>20000606T100900000</date>
552
553 </params>
554 </envelope>
555
556 (propose
557   :sender
558     (agent-identifier
559       :name CAiM@mobile.com)
560   :receiver (set
561     (agent-identifier
```

¹¹ In most of the examples, the envelope part has been omitted for clarity.

```

565         :name CAiG@gateway.com))
566 :ontology FIPA-Nomadic-Application
567 :language FIPA-SL0
568 :protocol FIPA-Propose
569 :content
570 ((action
571   (agent-identifier
572     :name CAiM@mobile.com)
573   (use
574     (transports
575       :send (sequence
576         (transport-protocol
577           :name x.uh.mdcp)
578         (transport-protocol
579           :name fipa.mts.mtp.wap.std)))
580       :recv (sequence
581         (transport-protocol
582           :name x.uh.mdcp)
583         (transport-protocol
584           :name fipa.mts.mtp.wap.std))))))
585 true))
586

```

4. Message 4 request, message 5 agree and message 6 inform: The CA in the gateway host requests the AP description from the local AMS (see [FIPA00023]) to determine whether the `x.uh.mdcp` or `fipa.mts.mtp.wap.std` MTPs are supported. The AMS informs the CA that both MTPs are supported and the CA decides to use `fipa.mts.mtp.wap.std` MTP based on the current quality of service requirements of the MTC.

```

592
593 (request
594   :sender
595     (agent-identifier
596       :name CAiG@gateway.com)
597   :receiver (set
598     (agent-identifier
599       :name ams@gateway.com))
600   :ontology FIPA-Agent-Management
601   :language FIPA-SL0
602   :protocol FIPA-Request
603   :content
604     (action
605       (agent-identifier
606         :name ams@gateway.com)
607       get-description))
608
609 (agree
610   :sender
611     (agent-identifier
612       :name ams@gateway.com)
613   :receiver (set
614     (agent-identifier
615       :name CAiG@gateway.com))
616   :ontology FIPA-Agent-Management
617   :language FIPA-SL0
618   :protocol FIPA-Request
619   :content
620     ((action
621       (agent-identifier
622         :name ams@gateway.com)
623       get-description)
624     true))
625
626 (inform
627   :sender

```

```

628     (agent-identifier
629       :name ams@gateway.com
630       :addresses (sequence http://gateway.com/acc))
631 :receiver (set
632   (agent-identifier
633     :name CAiG@gateway.com
634     :addresses (sequence http://gateway.com/acc)))
635 :ontology FIPA-Agent-Management
636 :language FIPA-SL0
637 :protocol FIPA-Request
638 :content
639   (ap-description
640     :name sonera-platform
641     :transport-profile
642     (ap-transport-description
643       :available-mtps
644       (set
645         (mtp-description
646           :profile fipa.profile.mts.alpha
647           :mtp-name fipa.mts.mtp.iiop.std
648           :addresses (sequence iiop://gateway.com/acc))
649         (mtp-description
650           :profile fipa.profile.mts.beta
651           :mtp-name fipa.mts.mtp.wap.std
652           :addresses (sequence wap://gateway.com:1234/acc))
653         (mtp-description
654           :profile x.uh.profile
655           :mtp-name x.uh.mdc
656           :addresses (set mdc://gateway.com/acc))))))
657

```

5. Message 7 accept-proposal: The CA in the gateway host accepts the proposal to use the fipa.mts.mtp.wap.std MTP and sends the response to the CA in the mobile host informing it about the preferred MTP.

```

661
662 (accept-proposal
663   :sender
664     (agent-identifier
665       :name CAiG@gateway.com)
666   :receiver (set
667     (agent-identifier
668       :name CAiM@mobile.com))
669   :ontology FIPA-Nomadic-Application
670   :language FIPA-SL0
671   :protocol FIPA-Propose
672   :content
673     (action
674       (agent-identifier
675         :name CAiM@mobile.com)
676       (use
677         (transports
678           :send (sequence
679             (transport-protocol
680               :name x.uh.mdc
681             (transport-protocol
682               :name fipa.mts.mtp.wap.std)))
683           :rcv (sequence
684             (transport-protocol
685               :name x.uh.mdc
686             (transport-protocol
687               :name fipa.mts.mtp.wap.std))))))
688     (transports
689       :send (sequence
690         (transport-protocol

```

```

691         :name fipa.mts.mtp.wap.std))
692     :recv (sequence
693         (transport-protocol
694         :name fipa.mts.mtp.wap.std))))
695

```

- 696 6. Messages 8 and 8' setup: The CAs request their respective ACCs to setup the `fipa.mts.mtp.wap.std` MTP. This is an implementation issue.
- 697
- 698
- 699 7. Message 9 and 9' setup-done: The ACCs inform their respective CAs that the `fipa.mts.mtp.wap.std` MTP has been established between the mobile host and the gateway host.
- 700
- 701
- 702 8. Message 10 inform: The CA informs the application agent that the MTC is established.

```

703 (inform
704 :sender
705   (agent-identifier
706   :name CAiM@mobile.com)
707 :receiver (set
708   (agent-identifier
709   :name A-AgentiM@mobile.com))
710 :ontology FIPA-Nomadic-Application
711 :language FIPA-SL0
712 :protocol FIPA-Request
713 :content
714   (result
715   (action
716   (agent-identifier
717   :name CaiM@mobile.com)
718   (activate (sequence
719   (transport-protocol
720   :name x.uh.mdcp)
721   (transport-protocol
722   :name fipa.mts.mtp.wap.std
723   :dest-addr wap://gateway.com:1234/acc))))
724   (transport-protocol
725   :name fipa.mts.mtp.wap.std))
726

```

- 727
- 728 9. Message 11 and 11' set-description: CAiM (/CAiG) modifies the AP description to show that the `fipa.mts.mtp.wap.std` is now active.
- 729
- 730

5.3 Negotiating Message Representations

This example shows a scenario where an application agent in a mobile host proposes to its peer application agent in a fixed host the use of the `fipa.acl.rep.bitefficient.std` representation of ACL [FIPA00069] for their communication. The message flow is illustrated in *Figure 4*.

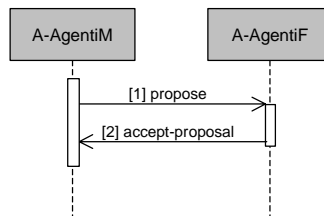


Figure 4: Flow of Message Representation Negotiation

- 736
- 737
- 738
- 739
- 740 1. Message 1 propose: The agent in the mobile host proposes the use of the `fipa.acl.rep.bitefficient.std` representation of ACL.
- 741
- 742


```

743 (propose
744   :sender
745     (agent-identifier
746       :name A-AgentiM@mobile.com)
747   :receiver (set
748     (agent-identifier
749       :name A-AgentiF@fixed.com))
750   :ontology FIPA-Message-Representation
751   :language FIPA-SL0
752   :protocol FIPA-Propose
753   :content
754     ((action
755       (agent-identifier
756         :name A-AgentiM@mobile.com)
757       (use
758         (msg-rep-selection
759           :send (sequence
760             (msg-representation
761               :name fipa.acl.rep.bitefficient.std))
762           :recv (sequence
763             (msg-representation
764               :name fipa.acl.rep.bitefficient.std))))))
765     true))

```

2. Message 2 accept-proposal: The agent in the fixed host accepts the proposal.

```

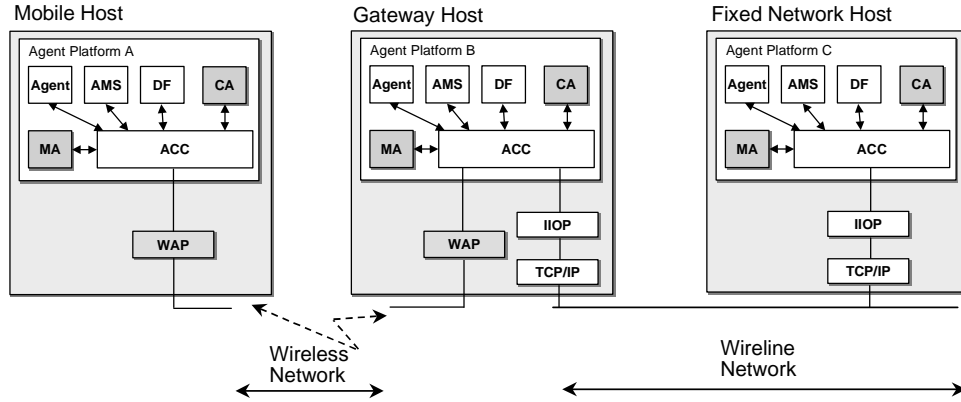
768 (accept-proposal
769   :sender
770     (agent-identifier
771       :name A-AgentiF@fixed.com)
772   :receiver (set
773     (agent-identifier
774       :name A-AgentiM@mobile.com))
775   :ontology FIPA-Message-Representation
776   :language FIPA-SL0
777   :protocol FIPA-Propose
778   :content
779     (action
780       (agent-identifier
781         :name A-AgentiM@mobile.com)
782       (use
783         (msg-rep-selection
784           :send (sequence
785             (msg-representation
786               :name fipa.acl.rep.bitefficient.std))
787           :recv (sequence
788             (msg-representation
789               :name fipa.acl.rep.bitefficient.std))))))
790     (msg-rep-selection
791       :send (sequence
792         (msg-representation
793           :name fipa.acl.rep.bitefficient.std))
794       :recv (sequenc
795         (msg-representation
796           :name fipa.acl.rep.bitefficient.std))))))
797
798

```

799 5.4 Message Exchange Over a WAP Message Transport Protocol

800 *Figure 5* refers to reference architecture for message exchange in context of nomadic applications. Messages between
801 the mobile host and gateway host are delivered mainly using the `fipa.mts.mtp.wap.std` MTP and messages
802 between gateway host and other APs in the fixed network are delivered using the `fipa.mts.mtp.iiop.std` MTP
803 (see [FIPA00075]).

804



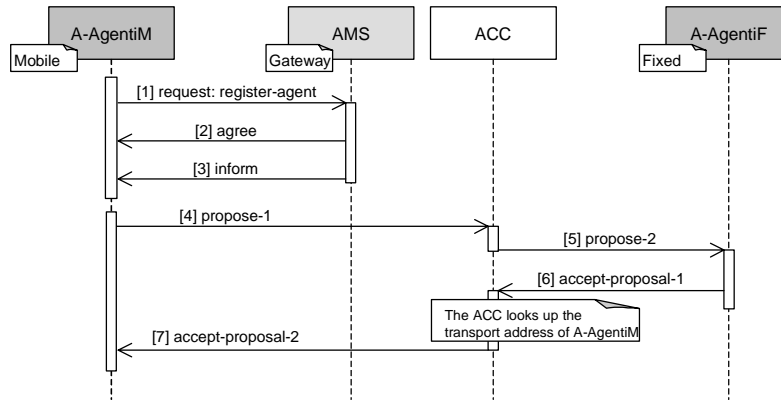
805
806
807
808

Figure 5: Gateway-Based Nomadic Application Architecture

809 **5.4.1 Message Exchange Activation by an Agent in a Mobile Host**

810 This example shows the scenario where an agent in a mobile host has a WAP address and an agent in fixed host has
811 an IIOIP address. In this example, there are three specific APs involved; one running in a mobile host, one running in a
812 gateway host and the last one running in a host situated in a fixed network which represents the rest of the network. An
813 example of the flow of a message exchange is illustrated in Figure 6.

814



815
816
817
818

Figure 6: Mobile Originated Message Exchange Over Gateway Host

- 819 1. Message 1 request, message 2 agree and message 3 inform: In order to be reachable from an AP operating in
820 a fixed network environment, an agent in the mobile host must register with the AP running in the gateway host.
821 Subsequently, the ACC in the gateway host AP can forward messages intended for the agent operating in the
822 mobile host to the ACC.

```
824 (request
825   :sender
826     (agent-identifier
827       :name A-AgentiM@mobile.com)
828   :receiver (set
829     (agent-identifier
830       :name ams@gateway.com))
831   :language FIPA-SL0
832   :protocol FIPA-Request
833   :ontology FIPA-Agent-Management
834   :content
835     (action
836       (agent-identifier
837         :name ams@gateway.com))
```

```

838     (register
839       (ams-agent-description
840         :name
841         (agent-identifier
842           :name A-AgentiM@mobile.com
843           :addresses (sequence wap://mobile.com:1234/acc))
844         :state active))))

```

The AMS informs A-AgentiM that registration was completed successfully and after registration, A-AgentiM can be reached via the gateway host using, for example, the following to envelope parameter:

```

849 <to>
850   <agent-identifier>
851     <name>A-AgentiM@mobile.com</name>
852     <addresses>
853       <url>iiop://gateway.com/acc</url>
854     </addresses>
855   </agent-identifier>
856 </to>

```

If the gateway host is not operational, then the direct WAP address (wap://mobile.com:1234/acc) could be used.

2. Message 4 propose 1: A-AgentiM sends a propose message to A-AgentiF. In the from envelope parameter, A-AgentiM informs A-AgentiF that its primary return address is its address in the gateway host.

```

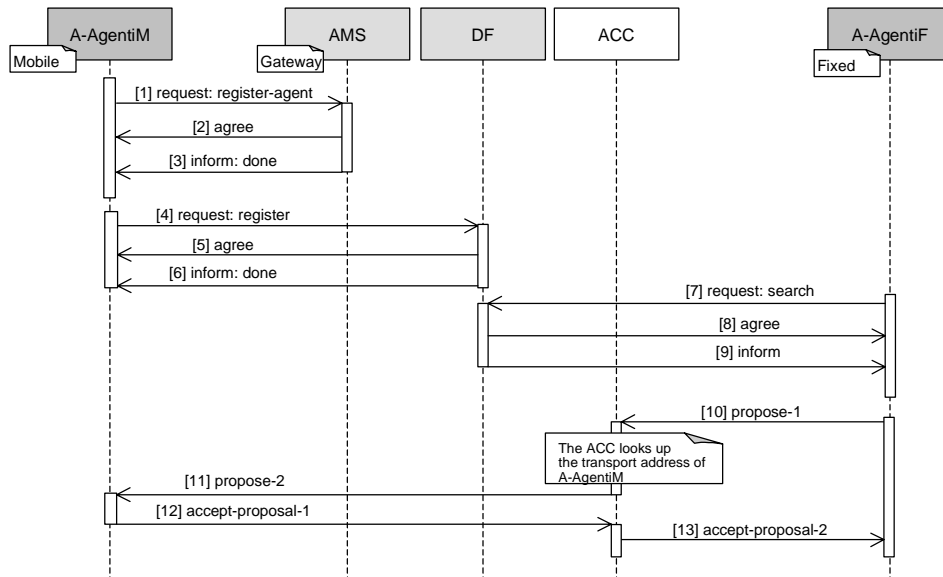
863 <?xml version="1.0"?>
864 <envelope>
865   <params index="1">
866     <to>
867       <agent-identifier>
868         <name>A-AgentiF@fixed.com</name>
869         <addresses>
870           <url>iiop://fixed.com/acc</name>
871         </addresses>
872       </agent-identifier>
873     </to>
874     <from>
875       <agent-identifier>
876         <name>A-AgentiM@mobile.com</name>
877         <addresses>
878           <url>iiop://gateway.com/acc</url>
879           <url>wap://mobile.com:1234/acc</url>
880         </addresses>
881       </agent-identifier>
882     </from>
883     <acl-representation>fipa.acl.rep.string.std</acl-representation>
884     <date>20000606T100900000</date>
885   </params>
886 </envelope>
887
888 (propose
889   :sender
890     (agent-identifier
891       :name A-AgentiM@mobile.com)
892   :receiver (set
893     (agent-identifier
894       :name A-AgentiF@fixed.com))
895   :language FIPA-SL0
896   :content
897     (action
898       (agent-identifier
899         :name A-AgentiM@mobile.com)
900       (compress-data (> object-size 1kb))))

```

- 901
 902 The ACC in the mobile host forwards the message to the ACC in the gateway host using `fipa.mts.mtp.wap.std`
 903 `MTP`¹².
 904
 905 3. Message 5 `propose 2`: The ACC in the gateway host forwards the message to `A-AgentiF` using
 906 `fipa.mts.mtp.iiop.std` MTP. The ACC may change the encoding of the message.
 907
 908 4. Message 6 `accept-proposal 1`: `A-AgentiF` accepts `A-AgentiM`'s proposal by sending an `accept-`
 909 `proposal` message to `A-AgentiM` using its gateway host address.
 910
 911 `(accept-proposal`
 912 `:sender`
 913 `(agent-identifier`
 914 `:name A-AgentiF@fixed.com)`
 915 `:receiver (set`
 916 `(agent-identifier`
 917 `:name A-AgentiM@mobile.com))`
 918 `:language FIPA-SL0`
 919 `:content`
 920 `((action`
 921 `(agent-identifier`
 922 `:name A-AgentiM@mobile.com)`
 923 `(compress-data (> object-size 1kb)))`
 924 `true))`
 925
 926 5. Message 7 `accept-proposal 2`: The ACC in the gateway host forwards the message to the ACC in the mobile
 927 host using the `fipa.mts.mtp.wap.std` MTP. The ACC may change the encoding of the message.
 928

929 **5.4.2 Message Exchange Termination to an Agent in a Mobile Host**

930 This example shows the scenario where an agent in a fixed host activates a conversation. The message flow is
 931 illustrated in *Figure 7*.
 932



933 **Figure 7: Mobile Terminated Message Exchange Over Gateway Hosts**

- 934
 935
 936
 937 1. Message 1 `request`, message 2 `agree` and message 3 `inform`: See *Section 5.4.1, Message Exchange*
 938 *Activation by an Agent in a Mobile Host*.

¹² The actual way in which this is achieved is not a subject of standardisation within FIPA.

939

940

2. Message 4 request: A-AgentiM needs to register its services with the DF in the gateway host in order to be able to publicise its services even when the mobile host itself is disconnected from the fixed network.

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

3. Message 5 agree and message 6 inform: The DF in the gateway host AP informs A-AgentiM that registration was successful.

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

1001

```
(inform
:sender
  (agent-identifier
:name df@gateway.com)
:receiver (set
  (agent-identifier
:name A-AgentiM@mobile.com))
:language FIPA-SL0
:protocol FIPA-Request
:ontology FIPA-Agent-Management
:content
  (done
  (action
  (agent-identifier :name df@gateway.com)
  (register
  (df-agent-description
:name
  (agent-identifier
:name A-AgentiM@mobile.com
:addresses (sequence iiop://gateway.com/acc wap://mobile.com:1234/acc))
:services
  (service-description (set
:name Field-Warrior
:type field-information
:ontology (set field-service)
:properties (set
  (property
:name availability
:value 24h))))
:language (set FIPA-SL0))))))
```

```
1002         :properties (set
1003           (property
1004             :name availability
1005             :value 24h))))
1006     :language (set FIPA-SL0))))))
1007
```

- 1008 4. Message 7 request, message 8 agree and message 9 inform: When A-Agent_{iM} needs the Field-Warrior
1009 service, it searches the gateway host DF which informs it that A-Agent_{iM} offers such a service (see [FIPA00023]).
1010
- 1011 5. Message 10, 11, 12 and 13: The messages used and the message flow are similar to the example in *Section 5.4.1,*
1012 *Message Exchange Activation by an Agent in a Mobile Host.*
1013
1014

6 Informative Annex A — Paramedic Scenario

This section illustrates some of the important issues of nomadic application support, using a paramedic application as an example.

6.1 Overview

A paramedic team has several working environments:

- An emergency dispatch centre, which is covered by the hospital ATM network,

- A geographical area, which is wireless wide-area network (e.g. GPRS), and,

- One or more hospitals, which are provided with a wireless local-area network.

When in transit, the paramedic computers are attached to docking stations residing in ambulances. At the dispatch centre, the docking stations are connected to the ATM network. The paramedic application comprises the following services:

- Retrieval of a patient's personal information, such as name, address, phone, and relatives,

- Retrieval of the patient's medical histories,

- Support for paramedic workers, and,

- Informing the hospital receiving the patient about the patient's current injury or illness and medical care given so far.

There are several application agents: Paramedic Support Agents (PSAs) working in the paramedic computers, Dispatching Support Agent (DSA) working at the dispatch centre system, and the Hospital First Aid Support Agent (HFASA) working at the hospital system.

The dispatch centre receives a call regarding a man who has severe chest pain; the symptom of an acute myocardial infarct. The caller identifies the man and gives his personal identification number to the dispatcher. The dispatcher alerts the paramedic team and informs the DSA about the address where the patient is located and his personal identification number. The DSA simultaneously informs the PSA about the address of the attack (and possibly some additional information about the environment of the heart attack) and queries the patient's medical history. Since the results of the query to a local hospital are received before the paramedic unit is dispatched, the DSA (in co-operation with the PSA) begins to load the patient's personal information and medical history into the paramedic computers. The medical history includes several items of text-based information. The transmission time to load the information via the ATM network to the paramedic computers (which are currently docked at the dispatch centre) is less than a second. Before the ambulance leaves the dispatch centre, the docking station is detached from the ATM network and is connected to the wireless wide-area network.

While the ambulance is approaching the location of the incident, the DSA receives more relevant results of the query of the medical histories such as the latest heart operation of the patient. The medical history comprises several parts of textual information and several images and the DSA begins loading the information. As the loading takes place when the ambulance is in motion, the DSA finds out that the quality of transport service is too low for loading some textual parts and any of the images of the medical history. It would take at least 40 minutes to download the images. Therefore, the DSA informs the PSA that images are not required for the paramedic unit. During downloading, the ambulance drives into a tunnel that causes the wireless link to be disconnected. After the tunnel, a CA re-establishes the connection and downloading continues.

At the scene, the ambulance is stationary and the quality of transmission service increases to a level at which the DSA is able to load the most relevant images (the ECGs) using an efficient compression method which is negotiated

1066 between the DSA and the PSA to the paramedic computer. The paramedic team detaches the computers from the
 1067 docking station and carries them to the patient.
 1068

1069 The paramedic team realises that they need the assistance of a medical expert located at the university hospital to
 1070 stabilise the patient's condition. Therefore, they attach electrodes to the patient and the PSA starts transmitting the data
 1071 of measurement such as SpO2 (oxygen saturation), cardiac rhythm, ECG, end tidal CO2 and temperature to the
 1072 hospital. After successfully stabilising the patient's condition, the paramedic team moves the patient to the ambulance
 1073 and sets off for the hospital. As the quality of the transport service decreases because of the motion, the PSA finds out
 1074 that not all the on-going measurement data can be transmitted on-line to the hospital. Therefore, the PSA decides to
 1075 transmit the most relevant data (SpO2 and cardiac rhythm). The PSA stores the rest of the data (ECG, end tidal CO2
 1076 and temperature) into a cache of the paramedic computer.
 1077

1078 After the ambulance arrives at the hospital, the patient is transferred immediately to an operating room. Simultaneously,
 1079 the paramedic team connects their paramedic computer to the wireless LAN of the hospital and the PSA transmits (in
 1080 co-operation with the HFASA) all the measurement data to the hospital's system. A surgeon retrieves and analyses the
 1081 measurement data before surgery.
 1082

1083 This example illustrates a future agent-based distributed system that offers its services at the best obtainable quality of
 1084 service in a wide variety of environments. A possible agent architecture is illustrated in *Figure 8* which refers to three
 1085 separate APs: *Dispatch*, *Gateway* and *Paracom*. In addition, there are several hospital APs which are not illustrated.
 1086

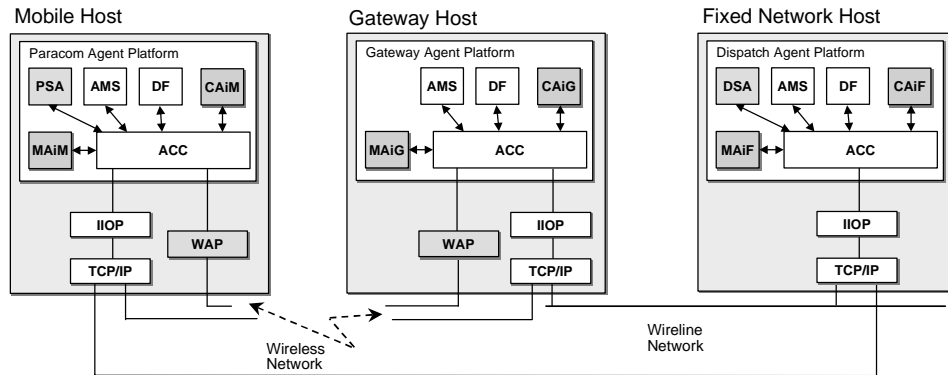


Figure 8: Paramedic Scenario Architecture

1087

1088

1089

1090

1091 The agents in the scenario are:

1092

1093 `MAiM`, `MAiG` and `MAiF` are MAs which monitor the quality of the communication service,

1094

1095 `CAiM`, `CAiG` and `CAiF` are CAs which manage the establishment, teardown, suspension, activation, etc. of the
 1096 connection between the PAs. The MA informs application agents about the status and changes of the network
 1097 services.
 1098

1098

1099 When the mobile host is connected either to the ATM network or to the wireless LAN, the `fipa.mts.mtp.iio.p.std`
 1100 MTP is used directly between the *Paracom* AP and the *Dispatch* AP. When the mobile host is connected to the wireless
 1101 WAN, all agent message communication takes place through the gateway host. The `fipa.mts.mtp.wap.std` MTP is
 1102 primarily used between the *Paracom* AP and the *Gateway* AP. The `fipa.mts.mtp.iio.p.std` MTP is used between
 1103 the *Gateway* AP and the *Dispatch* AP.
 1104

1104

1105

6.2 Seamless Roaming

The Seamless Roaming scenario describes the process, when the paramedic computer roams from the ATM network to the UMTS network. The scenario is split into following events:

- Disconnection and reconnection of MTCs,
- Negotiation of MTPs, and,
- Negotiation of message representations.

6.2.1 Disconnection and Reconnection of an Message Transport Connection

The message exchange between the agents is illustrated in Figure 9.

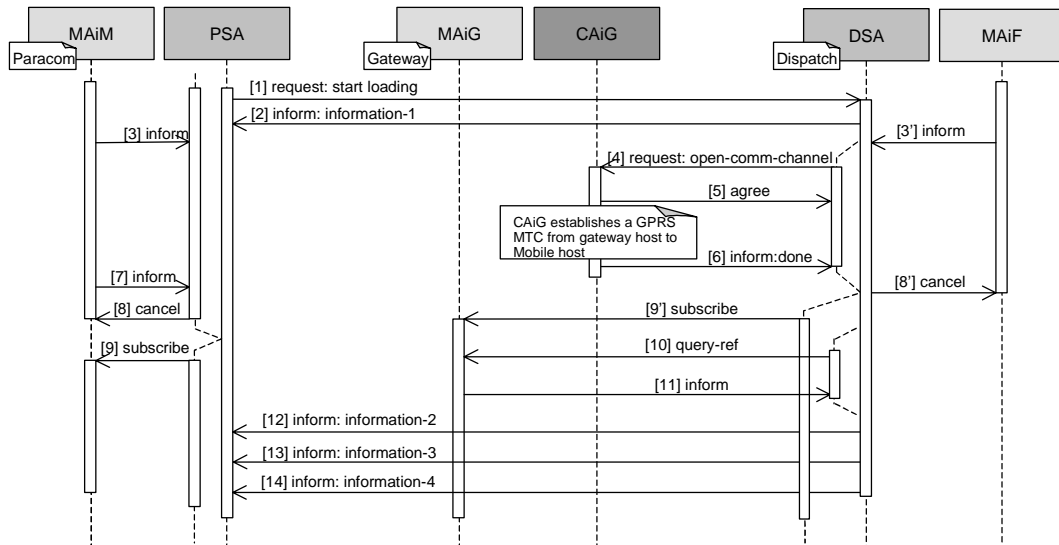


Figure 9: Disconnection and Reconnection of an Message Transport Connection

1. Message 1 *request*: The PSA starts loading data from the DSA by sending a *request* message. This message is application specific and thus not shown here.
2. Message 2 *inform*: The DSA starts sending information by first sending an *inform* message.
3. Messages 3 and 3' *inform*: MAiM (/ MAiF) informs the PSA (/ DSA) that the ATM connection has broken.

```
(inform
:sender
  (agent-identifier
    :name MAiM@paracom.com)
:receiver (set
  (agent-identifier
    :name PSA@paracom.com))
:ontology FIPA-Nomadic-Application
:language FIPA-SL2
:protocol FIPA-Subscribe
:content
  (= (iota ?x
    (qos-information
      (comm-channel
        :name ATM
```

```

1142         :target-addr iiop://dispatch.com/acc)
1143     (qos
1144         :status ?x)))
1145     disconnected))
1146

```

4. Message 4 request: The DSA requests CAiG to open a wireless wide-area MTC.

```

1148
1149 (request
1150     :sender
1151     (agent-identifier
1152         :name DSA@dispatch.com)
1153     :receiver (set
1154         (agent-identifier
1155             :name CAiG@gateway.com))
1156     :ontology FIPA-Nomadic-Application
1157     :language FIPA-SL0
1158     :protocol FIPA-Request
1159     :content
1160     (action
1161         (agent-identifier
1162             :name CAiG@gateway.com)
1163         (open-comm-channel
1164             (comm-channel
1165                 :name GPRS
1166                 :target-addr iiop://paramedic.com/acc))))))
1167

```

5. Message 5 agree: CAiG agrees that it will try to open the GPRS connection.

```

1168
1169 (agree
1170     :sender
1171     (agent-identifier
1172         :name CAiG@gateway.com)
1173     :receiver (set
1174         (agent-identifier
1175             :name DSA@dispatch.com))
1176     :ontology FIPA-Nomadic-Application
1177     :language FIPA-SL0
1178     :protocol FIPA-Request
1179     :content
1180     ((action
1181         (agent-identifier
1182             :name CAiG@gateway.com)
1183         (open-comm-channel
1184             (comm-channel
1185                 :name GPRS
1186                 :target-addr iiop://paramedic.com/acc))))))
1187     true))
1188

```

Next CAiG establishes a GPRS MTC from the gateway host to the mobile host. This is an implementation issue.

6. Message 6 inform: After successful establishment, CAiG informs the DSA.

```

1191
1192
1193 (inform
1194     :sender
1195     (agent-identifier
1196         :name CAiG@gateway.com)
1197     :receiver (set
1198         (agent-identifier
1199             :name DSA@dispatch.com))
1200     :ontology FIPA-Nomadic-Application
1201     :language FIPA-SL0
1202     :protocol FIPA-Request
1203

```

```

1204 :content
1205   (done
1206     (action
1207       (agent-identifier
1208         :name CAiG@gateway.com)))
1209   (open-comm-channel
1210     (comm-channel
1211       :name GPRS
1212       :target-addr iiop://paramedic.com/acc))))))
1213

```

7. Message 7 inform: MAiM informs the PSA that a new MTC has been established.

```

1214
1215 (inform
1216   :sender
1217     (agent-identifier
1218       :name MAiM@paracom.com)
1219   :receiver (set
1220     (agent-identifier
1221       :name PSA@paracom.com))
1222   :ontology FIPA-Nomadic-Application
1223   :language FIPA-SL2
1224   :protocol FIPA-Subscribe
1225   :content
1226     (= (iota ?x
1227       (qos-information
1228         (comm-channel
1229           :name GPRS
1230           :target-addr wap://paramedic.com:1234/acc)
1231         (qos
1232           :status ?x))))
1233     connected))
1234
1235

```

8. Message 8 and 8' cancel: The PSA (/DSA) cancels subscription notifications about the changes in the ATM MTC.

```

1236
1237 (cancel
1238   :sender
1239     (agent-identifier
1240       :name PSA@paracom.com)
1241   :receiver (set
1242     (agent-identifier
1243       :name MAiM@paracom.com))
1244   :ontology FIPA-Nomadic-Application
1245   :language FIPA-SL0
1246   :protocol FIPA-Subscribe
1247   :content
1248     (subscribe
1249       :sender
1250         (agent-identifier
1251           :name PSA@paracom.com)
1252       :receiver (set
1253         (agent-identifier
1254           :name MAiM@paracom.com))
1255       :ontology FIPA-Nomadic-Application
1256       :language FIPA-SL2
1257       :protocol FIPA-Subscribe
1258       :content
1259         (iota ?x
1260           (qos-information
1261             (comm-channel
1262               :name GPRS
1263               :target-addr wap://paramedic.com:1234/acc)
1264             (qos
1265               :status ?x))))))
1266

```

1267
1268

1268 9. Message 9 and 9' subscribe: The DSA (/PSA) subscribes to MAiG (/MAiM) for notifications about the changes in
 1269 the GPRS MTC.

```
1270
1271 (subscribe
1272   :sender
1273     (agent-identifier
1274       :name DSA@dispatch.com)
1275   :receiver (set
1276     (agent-identifier
1277       :name MAiG@gateway.com))
1278   :ontology FIPA-Nomadic-Application
1279   :language FIPA-SL2
1280   :protocol FIPA-Subscribe
1281   :content
1282     (iota ?x
1283       (qos-information
1284         (comm-channel
1285           :name GPRS
1286           :target-addr iiop://paramedic.com/acc)
1287         (qos
1288           :status ?x))))))
1289
```

1290 10. Message 10 query-ref: The DSA requests current quality of service of the GPRS MTC from MAiG.

```
1291
1292 (query-ref
1293   :sender
1294     (agent-identifier
1295       :name DSA@dispatch.com)
1296   :receiver (set
1297     (agent-identifier
1298       :name MAiG@gateway.com))
1299   :ontology FIPA-Nomadic-Application
1300   :language FIPA-SL2
1301   :protocol FIPA-Query
1302   :content
1303     (iota ?x
1304       (qos-information
1305         (comm-channel
1306           :name GPRS)
1307         (qos
1308           :throughput ?x))))
1309
```

1310 11. Message 11 inform: MAiG informs the DSA the current quality of service of the GPRS MTC.

```
1311
1312 (inform
1313   :sender
1314     (agent-identifier
1315       :name MAiG@gateway.com)
1316   :receiver (set
1317     (agent-identifier
1318       :name DSA@dispatch.com))
1319   :ontology FIPA-Nomadic-Application
1320   :language FIPA-SL2
1321   :protocol FIPA-Query
1322   :content
1323     (= (iota ?x
1324       (qos-information
1325         (comm-channel
1326           :name GPRS)
1327         (qos
1328           :throughput ?x))))
1329     (rate-value
1330       :direction Outbound
```

```
1331 :unit Kbits/s
1332 :value 20)))
1333
```

12. Messages 12, 13 and 14 inform: The DSA sends the rest of the requested information to the PSA.

6.2.2 Example Negotiation of a Message Transport Protocol

When the mobile host roams from the ATM network to the GPRS network – after the reconnection – the PSA receives the information from MAiM that the Paracom AP is now connected to the GPRS MTC. The PSA reasons that the fipa.mts.mtp.wap.std MTP is better in that environment and it requests the CAiM to establish this MTP between ACCiM and ACCiG. Also, CAiM proposes the establishment of this MTP to CAiG, which accepts the proposal, and they command their respective ACCs to set it up. As a last action, both CAiF and CAiG modify the AP descriptions of their APs. The message flow is illustrated in Figure 10.

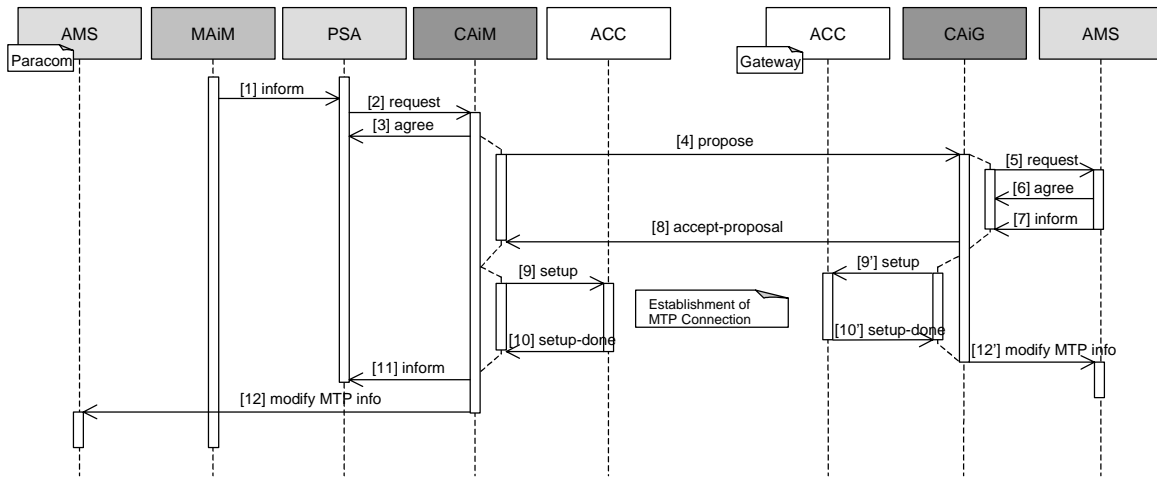


Figure 10: Example Negotiation of a Message Transport Protocol

1. Message 1 inform: MAiM informs the PSA that the Paracom AP is now connected to the GPRS network.

```
1344 (inform
1345 :sender
1346 (agent-identifier
1347 :name MAiM@paracom.com)
1348 :receiver (set
1349 (agent-identifier
1350 :name PSA@paracom.com))
1351 :ontology FIPA-Nomadic-Application
1352 :language FIPA-SL2
1353 :protocol FIPA-Subscribe
1354 :content
1355 (= (iota ?x
1356 (qos-information
1357 (comm-channel
1358 :name GPRS
1359 :target-addr wap://paramedic.com:1234/acc)
1360 (qos
1361 :status ?x)))
1362 connected))
1363
1364
1365
1366
1367
1368
1369
1370
```

1370 2. Message 2 request and message 3 agree: The PSA requests CAiM to establish the fipa.mts.mtp.wap.std
 1371 MTP between ACCiM and ACCiG.

```
1372 (request
1373   :sender
1374     (agent-identifier
1375      :name PSA@paracom.com)
1376   :receiver (set
1377     (agent-identifier
1378      :name CAiM@paracom.com))
1379   :ontology FIPA-Nomadic-Application
1380   :language FIPA-SL0
1381   :protocol FIPA-Request
1382   :content
1383     (action
1384      (agent-identifier
1385       :name CAiM@paracom.com)
1386      (activate (sequence
1387        (transport-protocol
1388         :name fipa.mts.mtp.wap.std
1389         :gw-addr wap://gateway.com:1234/acc))))))
1390
```

1391 3. Message 4 propose: CAiM sends a propose message to the CAiG.

```
1392 (propose
1393   :sender
1394     (agent-identifier
1395      :name CAiM@paracom.com)
1396   :receiver (set
1397     (agent-identifier
1398      :name CAiG@gateway.com))
1399   :ontology FIPA-Nomadic-Application
1400   :language FIPA-SL0
1401   :protocol FIPA-Propose
1402   :content
1403     ((action
1404      (agent-identifier
1405       :name CAiM@paracom.com)
1406      (use
1407       (transports
1408        :send (sequence
1409         (transport-protocol
1410          :name fipa.mts.mtp.wap.std))
1411         :recv (sequence
1412          (transport-protocol
1413           :name fipa.mts.mtp.wap.std))))))
1413      true)))
1414
```

1415 4. Message 5 request, message 6 agree and message 7 inform: CAiG requests the local AP description to find
 1416 out if the fipa.mts.mtp.wap.std MTP is supported (see [FIPA00023]).
 1417

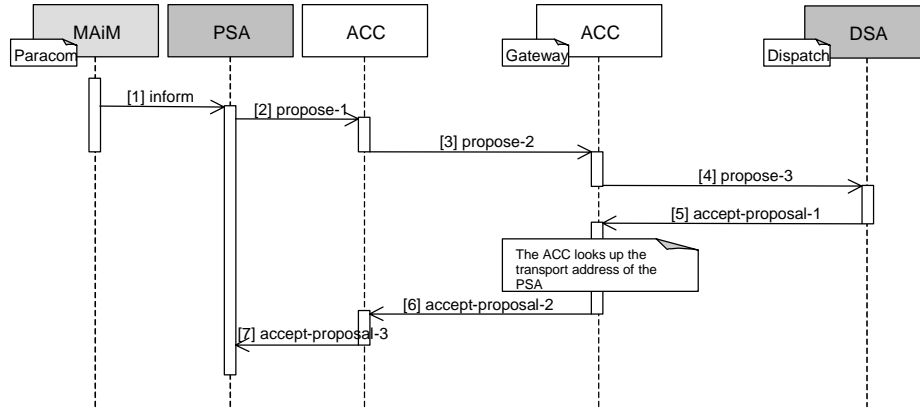
1418
 1419
 1420
 1421

1421 5. Message (8) accept-proposal: CAiG accepts CAiM's proposal to use the `fipa.mts.mtp.wap.std` MTP.
1422
1423 (accept-proposal
1424 :sender
1425 (agent-identifier
1426 :name CAiG@gateway.com)
1427 :receiver (set
1428 (agent-identifier
1429 :name CAiM@paracom.com))
1430 :ontology FIPA-Nomadic-Application
1431 :language FIPA-SL0
1432 :protocol FIPA-Propose
1433 :content
1434 (action
1435 (agent-identifier
1436 :name CAiM@paracom.com)
1437 (use
1438 (transports
1439 :send (sequence
1440 (transport-protocol
1441 :name fipa.mts.mtp.wap.std))
1442 :recv (sequence
1443 (transport-protocol
1444 :name fipa.mts.mtp.wap.std))))))
1445 (transports
1446 :send (sequence
1447 (transport-protocol
1448 :name fipa.mts.mtp.wap.std))
1449 :recv (sequence
1450 (transport-protocol
1451 :name fipa.mts.mtp.wap.std))))))
1452
1453 6. Messages 9 and 9' setup and messages 10 and 10' setup-done: CAiM (CAiG) commands ACCiM (ACCiG) to
1454 setup the `fipa.mts.mtp.wap.std` MTP. As this is intra-platform communication between CAiM (CAiG) and
1455 ACCiM (ACCiG), this is an implementation issue.
1456
1457 7. Message 11 inform: CAiM returns the result to the PSA.
1458
1459 (inform
1460 :sender
1461 (agent-identifier
1462 :name CAiM@paracom.com)
1463 :receiver (set
1464 (agent-identifier
1465 :name PSA@paracom.com))
1466 :ontology FIPA-Nomadic-Application
1467 :language FIPA-SL0
1468 :protocol FIPA-Request
1469 :content
1470 (result
1471 (action
1472 (agent-identifier
1473 :name CAiM@paracom.com)
1474 (activate (sequence
1475 (transport-protocol
1476 :name fipa.mts.mtp.wap.std
1477 :gw-addr wap://gateway.com:1234/acc))))
1478 (transport-protocol
1479 :name fipa.mts.mtp.wap.std
1480 :gw-addr wap://gateway.com:1234/acc))))
1481

1482 8. Message 12 and 12' set-description: CAiM (CAiG) modifies the AP description to show that the
 1483 fipa.mts.mtp.wap.std is now active.
 1484

1485 **6.2.3 Example Negotiation of a Message Representation**

1486 MAiM informs the PSA that the quality of the message transport connection has dropped significantly. The PSA reasons
 1487 that the ACL representation needs to be changed to fipa.acl.rep.bitefficient.std and it proposes that to the
 1488 DSA. The DSA accepts the PSA's proposal. The message flow is illustrated in Figure 11.
 1489



1490 **Figure 11: Example Negotiation of a Message Representation**

1491
 1492
 1493
 1494 1. Message 1 inform: The MA informs the PSA that the outbound throughput has changed.

```

1495 (inform
1496   :sender
1497     (agent-identifier
1498       :name MAiM@paracom.com)
1499   :receiver (set
1500     (agent-identifier
1501       :name PSA@paracom.com))
1502   :ontology FIPA-Nomadic-Application
1503   :language FIPA-SL2
1504   :protocol FIPA-Subscribe
1505   :content
1506     (= (iota ?x (
1507       (qos-notification
1508         (comm-channel
1509           :name GPRS)
1510         (throughput
1511           (rate-value
1512             :unit Kbits/s
1513             :direction Outbound
1514             :value ?x))
1515         (change-constraint
1516           :value (<
1517             (qos
1518               :throughput
1519                 (rate-value
1520                   :unit Kbits/s
1521                   :direction Outbound
1522                   :value 1))))))
1523     (0.96)))
    
```

1524
 1525
 1526 2. Message 2 propose-1: Based on the new throughput value, the PSA decides to change to the message
 1527 representation.
 1528

```

1528
1529 (propose
1530   :sender
1531     (agent-identifier
1532       :name PSA@paracom.com)
1533   :receiver (set
1534     (agent-identifier
1535       :name DSA@dispatch.com))
1536   :ontology FIPA-Message-Representation
1537   :language FIPA-SL0
1538   :protocol FIPA-Propose
1539   :content
1540     ((action
1541       (agent-identifier
1542         :name PSA@paracom.com)
1543       (use
1544         (msg-rep-selection
1545           :send (sequence
1546             (msg-representation
1547               :name fipa.acl.rep.bitefficient.std))
1548           :recv (sequence
1549             (msg-representation
1550               :name fipa.acl.rep.bitefficient.std))))))
1551     true))

```

3. Message 3 propose-2: The ACC at the mobile host forwards the same message to the ACC at the gateway host.

4. Message 4 propose-3: The ACC at the gateway host forwards the same message to the PSA.

5. Message 5 accept-proposal-1: The PSA accepts the proposal and sends a message back to the DSA.

```

1558
1559 (accept-proposal
1560   :sender
1561     (agent-identifier
1562       :name DSA@dispatch.com)
1563   :receiver (set
1564     (agent-identifier
1565       :name PSA@paracom.com))
1566   :ontology FIPA-Message-Representation
1567   :language FIPA-SL0
1568   :protocol FIPA-Propose
1569   :content
1570     (action
1571       (agent-identifier
1572         :name PSA@paracom.com)
1573       (use
1574         (msg-rep-selection
1575           :send (sequence
1576             (msg-representation
1577               :name fipa.acl.rep.bitefficient.std))
1578           :recv (sequence
1579             (msg-representation
1580               :name fipa.acl.rep.bitefficient.std))))))
1581     (msg-rep-selection
1582       :send (sequence
1583         (msg-representation
1584           :name fipa.acl.rep.bitefficient.std))
1585       :recv (sequence
1586         (msg-representation
1587           :name fipa.acl.rep.bitefficient.std))))))

```

6. Message 6 accept-proposal-2: The ACC at the gateway host forwards same message to the ACC at the mobile host.

1591

1592 7. Message 7 `accept-proposal-3`: The ACC at the mobile host delivers the same message to the PSA.

1593

7 References

1593

1594

1595

1596

1597

1598

1599

1600

1601

1602

1603

1604

1605

1606

1607

1608

1609

1610

1611

1612

1613

1614

1615

1616

1617

1618

1619

1620

- [FIPA00023] FIPA Agent Management Specification. Foundation for Intelligent Physical Agents, 2000.
<http://www.fipa.org/specs/fipa00023/>
- [FIPA00027] FIPA Query Interaction Protocol Specification. Foundation for Intelligent Physical Agents, 2000.
<http://www.fipa.org/specs/fipa00027/>
- [FIPA00035] FIPA Subscribe Interaction Protocol Specification. Foundation for Intelligent Physical Agents, 2000.
<http://www.fipa.org/specs/fipa00035/>
- [FIPA00036] FIPA Propose Interaction Protocol Specification. Foundation for Intelligent Physical Agents, 2000.
<http://www.fipa.org/specs/fipa00036/>
- [FIPA00069] FIPA ACL Message Representation in Bit-Efficient Encoding Specification. Foundation for Intelligent Physical Agents, 2000.
<http://www.fipa.org/specs/fipa00069/>
- [FIPA00075] FIPA Agent Message Transport Protocol for IIOP Specification. Foundation for Intelligent Physical Agents, 2000.
<http://www.fipa.org/specs/fipa00075/>
- [FIPA00076] FIPA Agent Message Transport Protocol for WAP Specification. Foundation for Intelligent Physical Agents, 2000.
<http://www.fipa.org/specs/fipa00076/>
- [ITUE800] Recommendation E.800 - Telephone Network and ISDN, Quality of Service, Network Management and Traffic Engineering, Terms and Definitions Related to Quality of Service and Network Performance Including Dependability. International Telecommunication Union, International Telecommunication Union, 1995.
- [ITUX135] Recommendation X.135 - Speed of Service (delay and throughput), Performance Values for Public Data Networks when Providing Packet-Switched Services. International Telegraph and Telephone Consultative Committee, 1993.
- [WAP99] Wireless Application Protocol Specification Version 1.2. WAP Forum, 1999.
<http://www.wapforum.org/what/technical.htm>