

FOUNDATION FOR INTELLIGENT PHYSICAL AGENTS

FIPA Nomadic Application Support Overview Specification

Document title	FIPA Nomadic Application Support Overview Specification		
Document number	OC00066D	Document source	FIPA Nomadic Application Support
Document status	Obsolete	Date of this status	2001/08/10
Supersedes	None		
Contact	fab@fipa.org		
Change history			
2000/08/04	Document made obsolete by FIPA00014		
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.

19 **Foreword**

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

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

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

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

38 **Contents**

39	1	Scope	1
40	2	General Analysis	2
41	2.1	Overview	2
42	2.2	Monitoring and Controlling Quality of Service	3
43	2.3	Negotiation of Message Transport Requirements	4
44	2.3.1	Negotiation About Message Transport Protocols	4
45	2.3.2	Negotiation About Message Representation	4
46	3	Scenarios	5
47	3.1	Negotiating Message Transport Protocols	5
48	3.2	Negotiating Message Representations	9
49	3.3	Message Exchange Over a WAP Message Transport Protocol	11
50	3.3.1	Message Exchange Activation by an Agent in a Mobile Host	11
51	3.3.2	Message Exchange Termination to an Agent in a Mobile Host	14
52	4	Informative Annex A - Paramedic Scenario	17
53	4.1	Overview	17
54	4.2	Seamless Roaming	19
55	4.2.1	Disconnection and Reconnection of an Message Transport Connection	19
56	4.2.2	Example Negotiation of a Message Transport Protocol	24
57	4.2.3	Example Negotiation of a Message Representation	27
58	5	References	30
59			

59 **1 Scope**

60 This document is part of the FIPA specifications and deals with agent middleware to support applications in nomadic
61 environment. This specification also forms part of the FIPA Nomadic Application Support Specification and gives an
62 overview of the Nomadic Application Support area.

63

63 2 General Analysis

64 2.1 Overview

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

76
 77 Confronted with these circumstances, the nomadic end-user would benefit from having the following functionality
 78 provided by the infrastructure: information about expected performance, agent monitoring and controlling the transfer
 79 operations, and adaptability.

80
 81 The ability to automatically adjust to changes in a transparent and integrated fashion is essential for *nomadicity*;
 82 nomadic end-users are usually professionals in areas other than computing. Furthermore, today's mobile computer
 83 systems are already very complex to use as productivity tools. Thus, nomadic end-users need all the support that a
 84 FIPA agent-based distributed system can deliver and adaptability to the changes in the environment of nomadic end-
 85 users is an important issue.

86
 87 FIPA uses the Wireless Application Protocol (WAP) [WAP99] as its wireless Message Transport Protocol (MTP - see
 88 [FIPA00076]). The WAP Forum has developed industry-wide specifications for low bandwidth wireless services (such
 89 as GSM, GPRS, etc.) and wireless devices (such as mobile telephones and personal digital assistants). The WAP
 90 specifications address the characteristics of wireless networks by adapting low bandwidth wireless services and low-
 91 end mobile devices to the special requirements of information services. The WAP specification defines a set of standard
 92 components that can be used in agent message communication, such as standard data formats and standard data
 93 communication protocols.

94
 95 The adaptation of applications to various nomadic computing environments is an important area. There are several
 96 tasks that agents need to carry out during application adaptation:

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

105
 106 The FIPA Nomadic Application Support specifications define agent middleware to:

107
 108 Monitor [FIPA00062] and control [FIPA00063] an MTP and the underlying MTC, and,

109
 110 An ontology [FIPA00065] for representing the quality of service of the Message Transport Service (MTS - see
 111 [FIPA00065]) in the context of nomadic application support.

116
117
118

In addition, this specification gives examples of the use of the above scenarios in section 3, *Scenarios*.

119 **2.2 Monitoring and Controlling Quality of Service**

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

122

- 123 1. Observing the quality of service of MTPs and MTCs,
- 124
- 125 2. Measuring (if there are no other means to obtain the required information) the quality of service of an MTP and
126 MTC,
- 127
- 128 3. Collecting information from the observing and measuring sources,
- 129
- 130 4. Analysing the information, and,
- 131
- 132 5. Controlling an MTC and selecting an MTP.

133

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

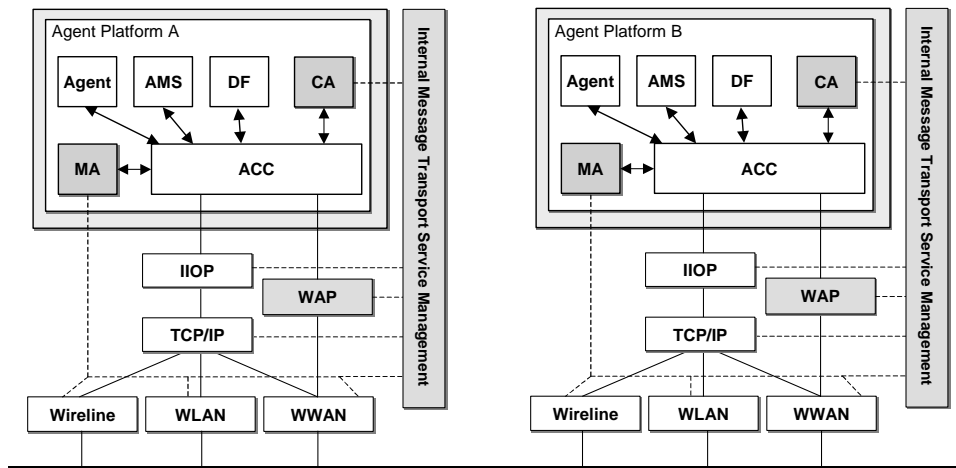
135

136 A **Monitor Agent** (MA - see [FIPA00062]) which carries out tasks 1 through 4, and,

137

138 A **Control Agent** (CA - see [FIPA00063]) which carries out task 5.

139



140

141

142

143

Figure 1: Reference Model of Agent Adaptation

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

147

148 An MA may:

149

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

151

152 Provide a repository for the measurement data collected,

153

154 Perform first level analysis of the collected data, and,

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

155
 156 Send the results of the analysis to CA, if requested to do so.
 157 A CA may:

158
 159 May manage (establish, close, suspend, activate, etc.) an MTC².
 160

161 In some cases there is a need for MAs and CAs in heterogeneous APs to communicate with each other; therefore,
 162 interaction protocols and ontologies to achieve this are specified in this document.
 163

164 **2.3 Negotiation of Message Transport Requirements**

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

167
 168 Communicating entities know a peer entity's preferences beforehand and use them.

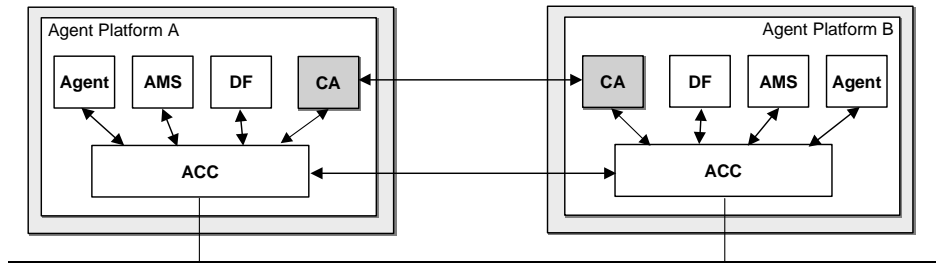
169
 170 The activating entity tries to use a method and if the peer entity is not capable of using the suggested method, then
 171 the activating entity may try another one (and so on).
 172

173 The communicating entities negotiate about a method to be used.
 174

175 **2.3.1 Negotiation About Message Transport Protocols**

176 Previous FIPA specifications have implicitly assumed that the MTC is operational all the time (meaning that the MTC
 177 has been established before the agent message exchange and that it is reliable). However, this is not always the case
 178 within a nomadic environment.
 179

180 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
 181 CA to either accept or reject the proposal based on whether it is possible to use the proposed MTP. CAs negotiate with
 182 peer CAs to use proposed MTPs which is illustrated in *Figure 2*.
 183



184
 185
 186 **Figure 2: Control Agents Negotiating About a Message Transport Protocol**
 187

188 CAs use the FIPA-Propose interaction protocol [FIPA00036] and the use action [FIPA00063] to negotiate about an
 189 MTP. An example negotiation is given in section 3.1, *Negotiating Message Transport Protocols*.
 190

191 **2.3.2 Negotiation About Message Representation**

192 In the environment of nomadic applications, it may be necessary to switch from one ACL representation to another; for
 193 example, when a mobile host roams from a wireline network to a wireless network. Application agents may use the
 194 FIPA-Propose interaction protocol and the use action to negotiate about the representation of ACL. Examples of this
 195 negotiation are given in section 3.2, *Negotiating Message Representation*.
 196

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

196 **3 Scenarios**

197 **3.1 Negotiating Message Transport Protocols**

198 This example shows a scenario, where an application agent requests the use of either the WAP MTP [FIPA00076] or a
 199 proprietary MTP (for example, x.uh.mdcp). The message flow of a successful negotiation is illustrated in *Figure 3*.
 200

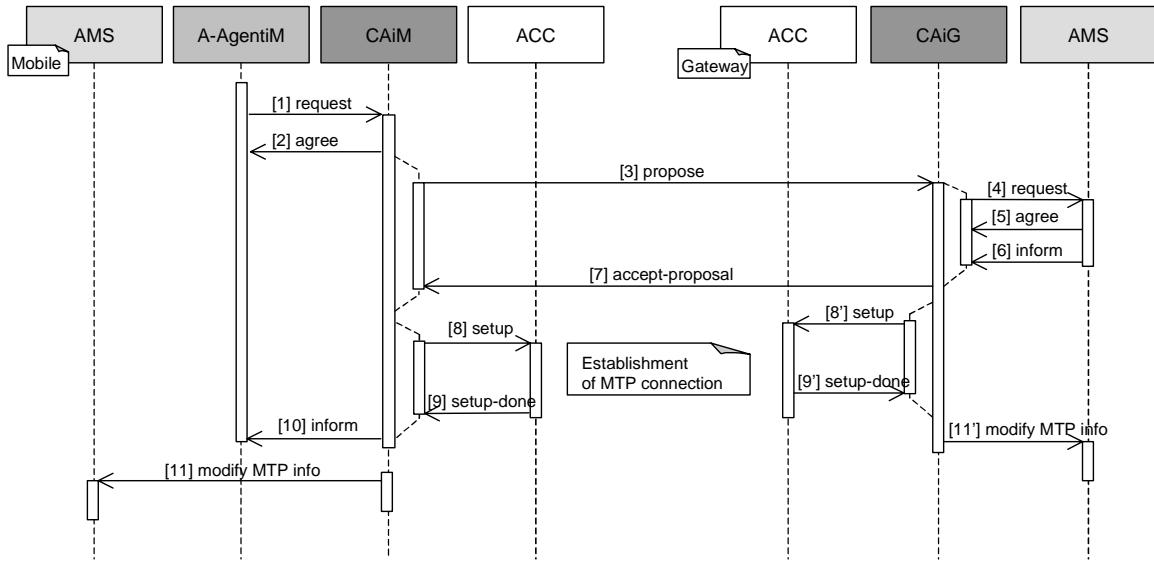


Figure 3: Flow of Message Transport Protocol Negotiation

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

```

207 (request
208   :sender
209     (agent-identifier3
210       :name A-AgentiM@mobile.com4)
211   :receiver (set
212     (agent-identifier
213       :name CaiM@mobile.com))
214   :ontology FIPA-Nomadic-Application
215   :language FIPA-SL0
216   :protocol FIPA-Request
217   :content
218     (action
219       (agent-identifier
220         :name CAiM@mobile.com)
221       (activate (sequence
222         (transport-protocol
223           :name x.uh.mdcp)
224         (transport-protocol
225           :name fipa.mts.mtp.wap.std
226           :dest-addr wap://gateway.com:1234/acc))))))
227
228
229
    
```

³ In most of the examples in this section, the :address parameters of AIDs have been omitted for clarity, except where absolutely necessary.

⁴ 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.

- 229 2. Message 2 agree: The CA agrees to activate an MTP. The decision to agree or disagree to activate an MTP might
 230 be based on the internal state of the CA (that is, the CA knows whether a requested MTP can be activated or not)
 231 or the CA might ask for an AP description from an AMS (see messages 4, 5 and 6 as an example).

```

232
233 (agree
234   :sender
235     (agent-identifier
236       :name CAiM@mobile.com)
237   :receiver (set
238     (agent-identifier
239       :name A-AgentiM@mobile.com))
240   :ontology FIPA-Nomadic-Application
241   :language FIPA-SL0
242   :protocol FIPA-Request
243   :content
244     ((action
245       (agent-identifier
246         :name CAiM@mobile.com))
247     (activate (sequence
248       (transport-protocol
249         :name x.uh.mdcp)
250       (transport-protocol
251         :name fipa.mts.mtp.wap.std
252         :dest-addr wap://gateway.com:1234/acc))))
253   true))
254
```

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

```

257
258 To: (agent-identifier :name CAiG@gateway.com)
259 From: (agent-identifier :name CAiM@mobile.com)
260 ACL-representation: fipa.acl.rep.string.std
261 Date: 20000606T100900000
262
```

```

263 (propose
264   :sender
265     (agent-identifier
266       :name CAiM@mobile.com)
267   :receiver (set
268     (agent-identifier
269       :name CAiG@gateway.com))
270   :ontology FIPA-Nomadic-Application
271   :language FIPA-SL0
272   :protocol FIPA-Propose
273   :content
274     ((action
275       (agent-identifier
276         :name CAiM@mobile.com)
277       (use
278         (transports
279           :send (sequence
280             (transport-protocol
281               :name x.uh.mdcp)
282             (transport-protocol
283               :name fipa.mts.mtp.wap.std)))
284         :recv (sequence
285           (transport-protocol
286             :name x.uh.mdcp)
287           (transport-protocol
288             :name fipa.mts.mtp.wap.std))))))
289   true))
290
291
```

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

```

296
297 (request
298   :sender
299     (agent-identifier
300       :name CAiG@gateway.com)
301   :receiver (set
302     (agent-identifier
303       :name ams@gateway.com))
304   :ontology FIPA-Agent-Management
305   :language FIPA-SL0
306   :protocol FIPA-Request
307   :content
308     (action
309       (agent-identifier
310         :name ams@gateway.com)
311       get-description))
312
313 (agree
314   :sender
315     (agent-identifier
316       :name ams@gateway.com)
317   :receiver (set
318     (agent-identifier
319       :name CAiG@gateway.com))
320   :ontology FIPA-Agent-Management
321   :language FIPA-SL0
322   :protocol FIPA-Request
323   :content
324     ((action
325       (agent-identifier
326         :name ams@gateway.com)
327       get-description)
328     true))
329
330 (inform
331   :sender
332     (agent-identifier
333       :name ams@gateway.com
334       :addresses (sequence http://gateway.com/acc))
335   :receiver (set
336     (agent-identifier
337       :name CAiG@gateway.com
338       :addresses (sequence http://gateway.com/acc)))
339   :ontology FIPA-Agent-Management
340   :language FIPA-SL0
341   :protocol FIPA-Request
342   :content
343     (ap-description
344       :name sonera-platform
345       :transport-profile
346       (ap-transport-description
347         :available-mtps
348         (set
349           (mtp-description
350             :profile fipa.profile.mts.alpha
351             :mtp-name fipa.mts.mtp.iiop.std
352             :addresses (sequence iiop://gateway.com/acc))
353           (mtp-description

```

```

354         :profile fipa.profile.mts.beta
355         :mtp-name fipa.mts.mtp.wap.std
356         :addresses (sequence wap://gateway.com:1234/acc))
357     (mtp-description
358       :profile x.uh.profile
359       :mtp-name x.uh.mdc
360       :addresses (set mdc://gateway.com/acc))))))
361

```

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

```

365 To: (agent-identifier :name CAiM@mobile.com)
366 From: (agent-identifier :name CAiG@gateway.com)
367 ACL-representation: fipa.acl.rep.string.std
368 Date: 20000606T100900000
369

```

```

370 (accept-proposal
371   :sender
372     (agent-identifier
373       :name CAiG@gateway.com)
374   :receiver (set
375     (agent-identifier
376       :name CAiM@mobile.com))
377   :ontology FIPA-Nomadic-Application
378   :language FIPA-SL0
379   :protocol FIPA-Propose
380   :content
381     (action
382       (agent-identifier
383         :name CAiM@mobile.com)
384       (use
385         (transports
386           :send (sequence
387             (transport-protocol
388               :name x.uh.mdc)
389             (transport-protocol
390               :name fipa.mts.mtp.wap.std)))
391           :rcv (sequence
392             (transport-protocol
393               :name x.uh.mdc)
394             (transport-protocol
395               :name fipa.mts.mtp.wap.std))))))
396     (transports
397       :send (sequence
398         (transport-protocol
399           :name fipa.mts.mtp.wap.std))
400       :rcv (sequence
401         (transport-protocol
402           :name fipa.mts.mtp.wap.std))))))
403

```

404 6. Messages 8 and 8' setup: The CAs request their respective ACCs to setup the fipa.mts.mtp.wap.std MTP.
405 This is an implementation issue.

406 7. Message 9 and 9' setup-done: The ACCs inform their respective CAs that the fipa.mts.mtp.wap.std MTP
407 has been established between the mobile host and the gateway host.

408
409
410
411

411 8. Message 10 inform: The CA informs the application agent that the MTC is established.

```

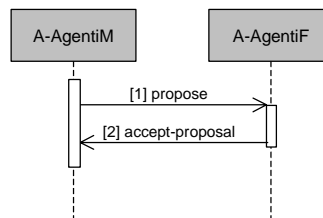
412
413 (inform
414   :sender
415   (agent-identifier
416    :name CAiM@mobile.com)
417   :receiver (set
418    (agent-identifier
419     :name A-AgentiM@mobile.com))
420   :ontology FIPA-Nomadic-Application
421   :language FIPA-SL0
422   :protocol FIPA-Request
423   :content
424   (result
425    (action
426     (agent-identifier
427      :name CaiM@mobile.com)
428     (activate (sequence
429      (transport-protocol
430       :name x.uh.mdcp)
431      (transport-protocol
432       :name fipa.mts.mtp.wap.std
433       :dest-addr wap://gateway.com:1234/acc))))
434   (transport-protocol
435    :name fipa.mts.mtp.wap.std))
436

```

437 3.2 Negotiating Message Representations

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

441



442

443

444

445

446 1. Message (1) propose: The agent in the mobile host proposes the use of the `fipa.acl.rep.bitefficient.std`
 447 representation of ACL.

448

```

449 To: (agent-identifier :name A-AgentiF@fixed.com
450      :addresses (sequence iiop://fixed.com/acc))
451 From: (agent-identifier :name A-AgentiM@mobile.com
452        :addresses (sequence wap://mobile.com:1234/acc))
453 ACL-representation: fipa.acl.rep.string.std
454 Date: 20000606T101000000
455

```

456

```

456 (propose
457   :sender
458   (agent-identifier
459    :name A-AgentiM@mobile.com)
460   :receiver (set
461    (agent-identifier
462     :name A-AgentiF@fixed.com))
463   :ontology FIPA-Message-Representation
464   :language FIPA-SL0

```

```

465 :protocol FIPA-Propose
466 :content
467   ((action
468     (agent-identifier
469       :name A-AgentiM@mobile.com)
470     (use
471       (msg-rep-selection
472         :send (sequence
473           (msg-representation
474             :name fipa.acl.rep.bitefficient.std))
475         :recv (sequence
476           (msg-representation
477             :name fipa.acl.rep.bitefficient.std))))))
478   true))
479

```

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

```

480
481 To: (agent-identifier :name A-AgentiM@mobile.com
482       :addresses (sequence wap://fixed.com:1234/acc))
483
484 From: (agent-identifier :name A-AgentiF@iioop://fixed.com
485       :addresses (sequence iioop://fixed.com/acc))
486
487 ACL-representation: fipa.acl.rep.string.std
488
489 Date: 20000606T101000000
490
491 (accept-proposal
492   :sender
493     (agent-identifier
494       :name A-AgentiF@fixed.com)
495   :receiver (set
496     (agent-identifier
497       :name A-AgentiM@mobile.com))
498   :ontology FIPA-Message-Representation
499   :language FIPA-SL0
500   :protocol FIPA-Propose
501   :content
502     (action
503       (agent-identifier
504         :name A-AgentiM@mobile.com)
505       (use
506         (msg-rep-selection
507           :send (sequence
508             (msg-representation
509               :name fipa.acl.rep.bitefficient.std))
510           :recv (sequence
511             (msg-representation
512               :name fipa.acl.rep.bitefficient.std))))))
513       (msg-rep-selection
514         :send (sequence
515           (msg-representation
516             :name fipa.acl.rep.bitefficient.std))
517         :recv (sequenc
518           (msg-representation
519             :name fipa.acl.rep.bitefficient.std))))))
519

```

3.3 Message Exchange Over a WAP Message Transport Protocol

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

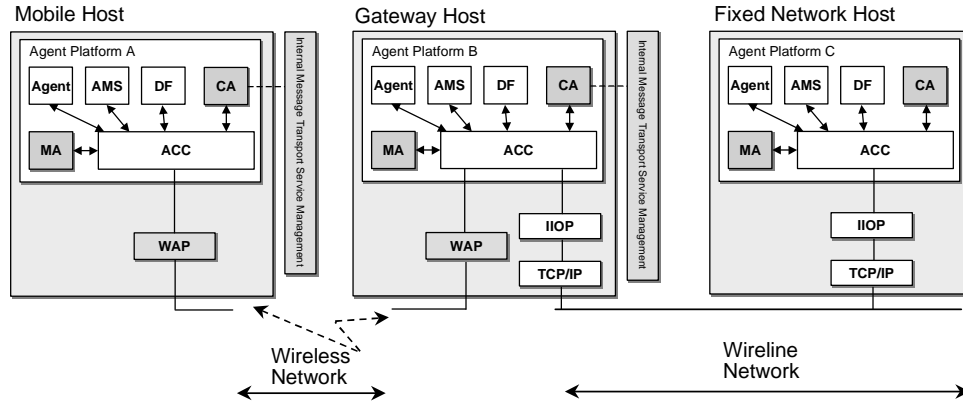


Figure 5: Gateway-Based Nomadic Application Architecture

3.3.1 Message Exchange Activation by an Agent in a Mobile Host

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

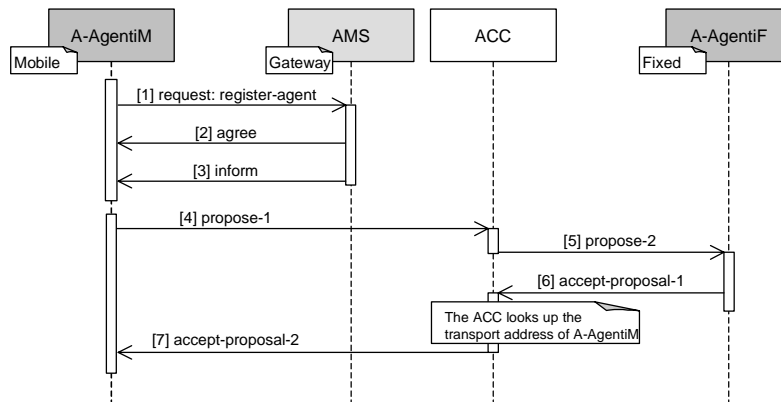


Figure 6: Mobile Originated Message Exchange Over Gateway Host

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

```
To: (agent-identifier :name ams@gateway.com
      :addresses (sequence wap://gateway.com:1234/acc))
From: (agent-identifier :name A-AgentIM@mobile.com
      :addresses (sequence wap://mobile.com:1234/acc))
ACL-representation: fipa.acl.rep.string.std
Date: 20000606T10100000
```

```

549 (request
550   :sender
551     (agent-identifier
552       :name A-AgentiM@mobile.com)
553   :receiver (set
554     (agent-identifier
555       :name ams@gateway.com))
556   :language FIPA-SL0
557   :protocol FIPA-Request
558   :ontology FIPA-Agent-Management
559   :content
560     (action
561       (agent-identifier
562         :name ams@gateway.com)
563       (register
564         (ams-agent-description
565           :name
566             (agent-identifier
567               :name A-AgentiM@mobile.com
568               :addresses (sequence wap://mobile.com:1234/acc))
569           :state active))))))
570
571

```

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

```

574 To: (agent-identifier :name A-AgentiM@mobile.com
575       :addresses (sequence iiop://gateway.com/acc))
576
577

```

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

579
580 2. Message 4 propose-1: A-AgentiM sends a propose message to A-AgentiF. In the From parameter, A-
581 AgentM informs A-AgentiF that its primary return address is its address in the gateway host.

```

582 To: (agent-identifier :name A-AgentiF@fixed.com
583       :addresses (sequence iiop://fixed.com/acc))
584 From: (agent-identifier :name A-AgentiM@mobile.com
585       :addresses (sequence iiop://gateway.com/acc wap://mobile.com:1234/acc))
586 ACL-representation: fipa.acl.rep.string.std
587 Date: 20000606T101000000
588
589

```

```

590 (propose
591   :sender
592     (agent-identifier
593       :name A-AgentiM@mobile.com)
594   :receiver (set
595     (agent-identifier
596       :name A-AgentiF@fixed.com))
597   :language FIPA-SL0
598   :content
599     (action
600       (agent-identifier
601         :name A-AgentiM@mobile.com)
602       (compress-data (> object-size 1kb)))
603
604

```

604 The ACC in the mobile host forwards the message to the ACC in the gateway host using fipa.mts.mtp.wap.std
605 MTP⁵.

⁵ The actual way in which this is achieved is not a subject of standardisation within FIPA.

- 607 3. Message 5 propose-2: The ACC in the gateway host forwards the message to A-AgentiF using
608 fipa.mts.mtp.iiop.std MTP. The ACC may change the encoding of the message.
609
610

610 4. Message 6 accept-proposal-1: A-AgentiF accepts A-AgentiM's proposal by sending an accept-
 611 proposal message to A-AgentiM using its gateway host address.

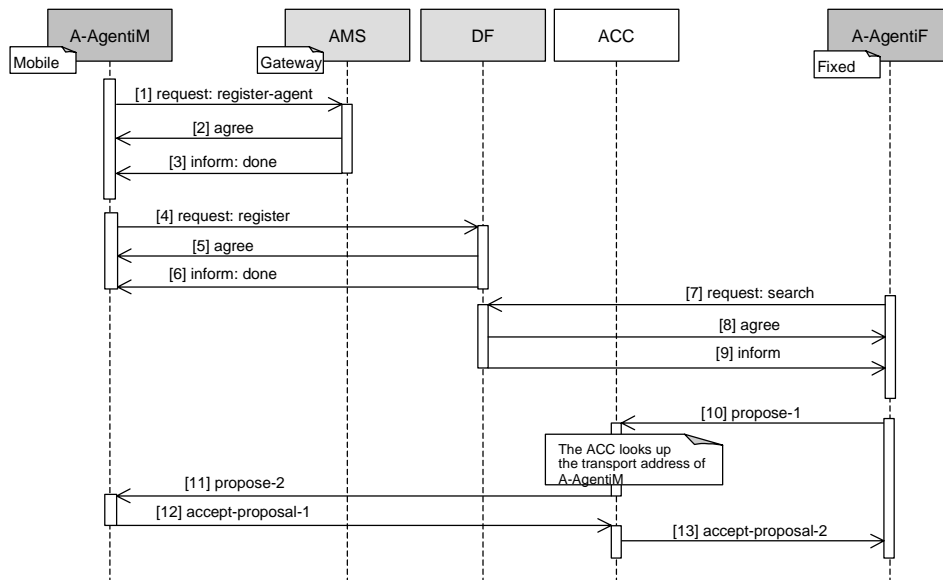
```

612
613 To: (agent-identifier :name A-AgentiM@mobile.com
614         :addresses (sequence iiop://gateway.com/acc))
615 From: (agent-identifier :name A-AgentiF@iiop://fixed.com
616         :addresses (sequence iiop://fixed.com/acc))
617 ACL-representation: fipa.acl.rep.string.std
618 Date: 20000606T101100000
619
620 (accept-proposal
621   :sender
622     (agent-identifier
623       :name A-AgentiF@fixed.com)
624   :receiver (set
625     (agent-identifier
626       :name A-AgentiM@mobile.com))
627   :language FIPA-SL0
628   :content
629     ((action
630       (agent-identifier
631         :name A-AgentiM@mobile.com)
632       (compress-data (> object-size 1kb)))
633     true)
    
```

635 5. Message 7 accept-proposal-2: The ACC in the gateway host forwards the message to the ACC in the mobile
 636 host using the fipa.mts.mtp.wap.std MTP. The ACC may change the encoding of the message.
 637

638 **3.3.2 Message Exchange Termination to an Agent in a Mobile Host**

639 This example shows the scenario where an agent in a fixed host activates a conversation. The message flow is
 640 illustrated in Figure 7.
 641



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

643
 644 1. Message 1 request, message 2 agree and message 3 inform: See section 3.3.1, *Message Exchange*
 645 *Activation by an Agent in a Mobile Host.*
 646
 647
 648
 649

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

```
651
652 To: (agent-identifier :name df@gateway.com)
653 From: (agent-identifier :name A-AgentiM@mobile.com)
654 ACL-representation: fipa.acl.rep.string.std
655 Date: 20000606T101100000
656
657 (request
658   :sender
659     (agent-identifier
660       :name A-AgentiM@mobile.com)
661   :receiver (set
662     (agent-identifier
663       :name df@gateway.com))
664   :ontology FIPA-Agent-Management
665   :language FIPA-SL0
666   :protocol FIPA-Request
667   :content
668     (action
669       (agent-identifier
670         :name df@gateway.com)
671       (register
672         (df-agent-description
673           :name
674             (agent-identifier
675               :name A-AgentiM@mobile.com
676               :addresses (sequence iiop://gateway.com/acc wap://mobile.com:1234/acc))
677           :services (set
678             (service-description
679               :name Field-Warrior
680               :type field-information
681               :ontology (set field-service)
682               :properties (set
683                 (property
684                   :name availability
685                   :value 24h))))
686           :language (set FIPA-SL0))))))
687
```

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

```
690
691 (inform
692   :sender
693     (agent-identifier
694       :name df@gateway.com)
695   :receiver (set
696     (agent-identifier
697       :name A-AgentiM@mobile.com))
698   :language FIPA-SL0
699   :protocol FIPA-Request
700   :ontology FIPA-Agent-Management
701   :content
702     (done
703       (action
704         (agent-identifier :name df@gateway.com)
705         (register
706           (df-agent-description
707             :name
708               (agent-identifier
709                 :name A-AgentiM@mobile.com
710                 :addresses (sequence iiop://gateway.com/acc wap://mobile.com:1234/acc))
711             :services
```

```
712         (service-description (set
713           :name Field-Warrior
714           :type field-information
715           :ontology field-service
716           :properties (set
717             (property
718               :name availability
719               :value 24h))))
720         :language (set FIPA-SL0))))))
```

721

722 4. Message 7 request, message 8 agree and message 9 inform: When A-Agent_{iM} needs the Field-Warrior
723 service, it searches the gateway host DF which informs it that A-Agent_{iM} offers such a service (see [FIPA00023]).

724

725 5. Message 10, 11, 12 and 13: The messages used and the message flow are similar to the example in section 3.3.1,
726 *Message Exchange Activation by an Agent in a Mobile Host*.

727

728

728 4 Informative Annex A - Paramedic Scenario

729 This section illustrates some of the important issues of nomadic application support, using a paramedic application as
730 an example.
731

732 4.1 Overview

733 A paramedic team has several working environments:

734 An emergency dispatch centre, which is covered by the hospital ATM network,
735

736 A geographical area, which is wireless wide-area network (e.g. GPRS), and,
737

738 One or more hospitals, which are provided with a wireless local-area network.
739

740
741 When in transit, the paramedic computers are attached to docking stations residing in ambulances. At the dispatch
742 centre, the docking stations are connected to the ATM network. The paramedic application comprises the following
743 services:

744 Retrieval of a patient's personal information, such as name, address, phone, and relatives,
745

746 Retrieval of the patient's medical histories,
747

748 Support for paramedic workers, and,
749

750 Informing the hospital receiving the patient about the patient's current injury or illness and medical care given so far.
751

752
753 There are several application agents: Paramedic Support Agents (PSAs) working in the paramedic computers,
754 Dispatching Support Agent (DSA) working at the dispatch centre system, and the Hospital First Aid Support Agent
755 (HFASA) working at the hospital system.
756

757 The dispatch centre receives a call regarding a man who has severe chest pain; the symptom of an acute myocardial
758 infarct. The caller identifies the man and gives his personal identification number to the dispatcher. The dispatcher
759 alerts the paramedic team and informs the DSA about the address where the patient is located and his personal
760 identification number. The DSA simultaneously informs the PSA about the address of the attack (and possibly some
761 additional information about the environment of the heart attack) and queries the patient's medical history. Since the
762 results of the query to a local hospital are received before the paramedic unit is dispatched, the DSA (in co-operation
763 with the PSA) begins to load the patient's personal information and medical history into the paramedic computers. The
764 medical history includes several items of text-based information. The transmission time to load the information via the
765 ATM network to the paramedic computers (which are currently docked at the dispatch centre) is less than a second.
766 Before the ambulance leaves the dispatch centre, the docking station is detached from the ATM network and is
767 connected to the wireless wide-area network.
768

769 While the ambulance is approaching the location of the incident, the DSA receives more relevant results of the query of
770 the medical histories such as the latest heart operation of the patient. The medical history comprises several parts of
771 textual information and several images and the DSA begins loading the information. As the loading takes place when
772 the ambulance is in motion, the DSA finds out that the quality of transport service is too low for loading some textual
773 parts and any of the images of the medical history. It would take at least 40 minutes to download the images. Therefore,
774 the DSA informs the PSA that images are not required for the paramedic unit. During downloading, the ambulance
775 drives into a tunnel that causes the wireless link to be disconnected. After the tunnel, a CA re-establishes the
776 connection and downloading continues.
777

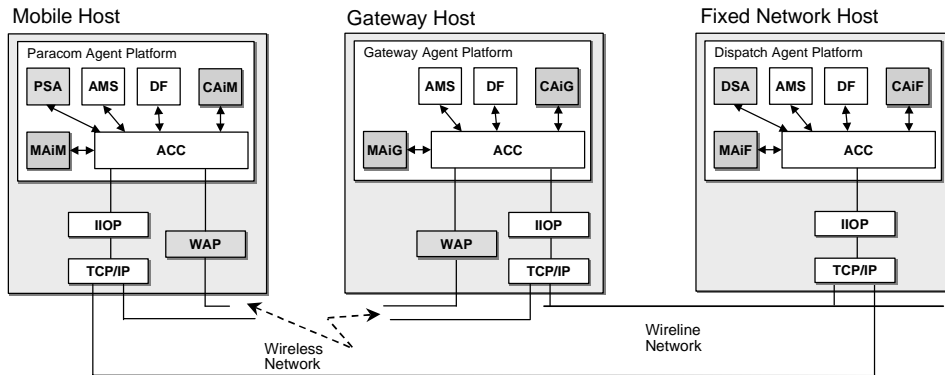
778 At the scene, the ambulance is stationary and the quality of transmission service increases to a level at which the DSA
779 is able to load the most relevant images (the ECGs) using an efficient compression method which is negotiated

780 between the DSA and the PSA to the paramedic computer. The paramedic team detaches the computers from the
 781 docking station and carries them to the patient.
 782

783 The paramedic team realises that they need the assistance of a medical expert located at the university hospital to
 784 stabilise the patient's condition. Therefore, they attach electrodes to the patient and the PSA starts transmitting the data
 785 of measurement such as SpO2 (oxygen saturation), cardiac rhythm, ECG, end tidal CO2 and temperature to the
 786 hospital. After successfully stabilising the patient's condition, the paramedic team moves the patient to the ambulance
 787 and sets off for the hospital. As the quality of the transport service decreases because of the motion, the PSA finds out
 788 that not all the on-going measurement data can be transmitted on-line to the hospital. Therefore, the PSA decides to
 789 transmit the most relevant data (SpO2 and cardiac rhythm). The PSA stores the rest of the data (ECG, end tidal CO2
 790 and temperature) into a cache of the paramedic computer.
 791

792 After the ambulance arrives at the hospital, the patient is transferred immediately to an operating room. Simultaneously,
 793 the paramedic team connects their paramedic computer to the wireless LAN of the hospital and the PSA transmits (in
 794 co-operation with the HFASA) all the measurement data to the hospital's system. A surgeon retrieves and analyses the
 795 measurement data before surgery.
 796

797 This example illustrates a future agent-based distributed system that offers its services at the best obtainable quality of
 798 service in a wide variety of environments. A possible agent architecture is illustrated in *Figure 8* which refers to three
 799 separate APs: *Dispatch*, *Gateway* and *Paracom*. In addition, there are several hospital APs which are not illustrated.
 800



801
 802
 803 **Figure 8: Paramedic Scenario Architecture**
 804

805 The agents in the scenario are:

806
 807 MAiM, MAiG and MAiF are MAs which monitor the quality of the communication service,
 808

809 CAiM, CAiG and CAiF are CAs which manage the establishment, teardown, suspension, activation, etc. of the
 810 connection between the PAs. The MA informs application agents about the status and changes of the network
 811 services.
 812

813 When the mobile host is connected either to the ATM network or to the wireless LAN, the *fipa.mts.mtp.iioop.std*
 814 MTP is used directly between the *Paracom* AP and the *Dispatch* AP. When the mobile host is connected to the wireless
 815 WAN, all agent message communication takes place through the gateway host. The *fipa.mts.mtp.wap.std* MTP is
 816 primarily used between the *Paracom* AP and the *Gateway* AP. The *fipa.mts.mtp.iioop.std* MTP is used between
 817 the *Gateway* AP and the *Dispatch* AP.
 818
 819

819 **4.2 Seamless Roaming**

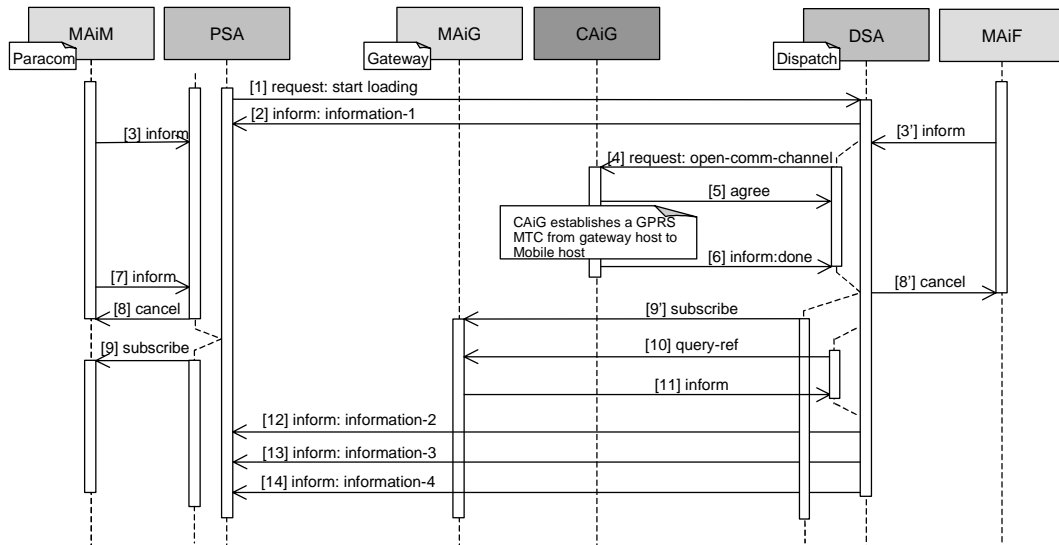
820 The Seamless Roaming scenario describes the process, when the paramedic computer roams from the ATM network
 821 to the UMTS network. The scenario is split into following events:

- 823 Disconnection and reconnection of MTCs,
- 824
- 825 Negotiation of MTPs, and,
- 826
- 827 Negotiation of message representations.
- 828

829 **4.2.1 Disconnection and Reconnection of an Message Transport Connection**

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

831



832

833

834

835

836

837

838

839

840

841

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.

841 3. Messages 3 and 3' inform: MAiM (/ MAiF) informs the PSA (/DSA) that the ATM connection has broken.

```
842 (inform
843   :sender
844     (agent-identifier
845      :name MAiM@paracom.com)
846   :receiver (set
847     (agent-identifier
848      :name PSA@paracom.com))
849   :ontology FIPA-Nomadic-Application
850   :language FIPA-SL2
851   :protocol FIPA-Subscribe
852   :content
853     (= (iota ?x
854        (qos-information
855         (comm-channel
856          :name ATM
857          :target-addr iiop://dispatch.com/acc)
858         (qos
859          :status ?x)))
860        disconnected))
861
```

862

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

864

```
865 To: (agent-identifier :name CAiG@gateway.com)
866 From: (agent-identifier :name DSA@dispatch.com)
867 ACL-representation: fipa.acl.rep.string.std
868 Date: 20000606T101100000
```

869

```
870 (request
871   :sender
872     (agent-identifier
873      :name DSA@dispatch.com)
874   :receiver (set
875     (agent-identifier
876      :name CAiG@gateway.com))
877   :ontology FIPA-Nomadic-Application
878   :language FIPA-SL0
879   :protocol FIPA-Request
880   :content
881     (action
882      (agent-identifier
883       :name CAiG@gateway.com)
884      (open-comm-channel
885       (comm-channel
886        :name GPRS
887        :target-addr iiop://paramedic.com/acc))))
888
```

889

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

```
890
891 To: (agent-identifier :name DSA@dispatch.com)
892 From: (agent-identifier :name CAiG@gateway.com)
893 ACL-representation: fipa.acl.rep.string.std
894 Date: 20000606T101200000
895
896 (agree
897   :sender
898     (agent-identifier
899       :name CAiG@gateway.com)
900   :receiver (set
901     (agent-identifier
902       :name DSA@dispatch.com))
903   :ontology FIPA-Nomadic-Application
904   :language FIPA-SL0
905   :protocol FIPA-Request
906   :content
907     ((action
908       (agent-identifier
909         :name CAiG@gateway.com)
910       (open-comm-channel
911         (comm-channel
912           :name GPRS
913           :target-addr iiop://paramedic.com/acc))))
914   true)
```

915
916 Next CAiG establishes a GPRS MTC from the gateway host to the mobile host. This is an implementation issue.

917
918 6. Message 6 inform: After successful establishment, CAiG informs the DSA.

```
919
920 To: (agent-identifier :name DSA@dispatch.com)
921 From: (agent-identifier :name CAiG@gateway.com)
922 ACL-representation: fipa.acl.rep.string.std
923 Date: 20000606T101200000
924
925 (inform
926   :sender
927     (agent-identifier
928       :name CAiG@gateway.com)
929   :receiver (set
930     (agent-identifier
931       :name DSA@dispatch.com))
932   :ontology FIPA-Nomadic-Application
933   :language FIPA-SL0
934   :protocol FIPA-Request
935   :content
936     (done
937       (action
938         (agent-identifier
939           :name CAiG@gateway.com))
940       (open-comm-channel
941         (comm-channel
942           :name GPRS
943           :target-addr iiop://paramedic.com/acc))))))
944
945
```


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

```

946 (inform
947   :sender
948     (agent-identifier
949       :name MAiM@paracom.com)
951   :receiver (set
952     (agent-identifier
953       :name PSA@paracom.com))
954   :ontology FIPA-Nomadic-Application
955   :language FIPA-SL2
956   :protocol FIPA-Subscribe
957   :content
958     (= (iota ?x
959       (qos-information
960         (comm-channel
961           :name GPRS
962           :target-addr wap://paramedic.com:1234/acc)
963         (qos
964           :status ?x))))
965     connected))

```

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

```

968 (cancel
969   :sender
970     (agent-identifier
971       :name PSA@paracom.com)
973   :receiver (set
974     (agent-identifier
975       :name MAiM@paracom.com))
976   :ontology FIPA-Nomadic-Application
977   :language FIPA-SL0
978   :protocol FIPA-Subscribe
979   :content
980     (subscribe
981       :sender
982         (agent-identifier
983           :name PSA@paracom.com)
984       :receiver (set
985         (agent-identifier
986           :name MAiM@paracom.com))
987       :ontology FIPA-Nomadic-Application
988       :language FIPA-SL2
989       :protocol FIPA-Subscribe
990       :content
991         (iota ?x
992           (qos-information
993             (comm-channel
994               :name GPRS
995               :target-addr wap://paramedic.com:1234/acc)
996             (qos
997               :status ?x))))))
998
999

```

999 9. Message 9 and 9' subscribe: The DSA (/PSA) subscribes to MAiG (/MAiM) for notifications about the changes in
 1000 the GPRS MTC.

```

1001 (subscribe
1002   :sender
1003     (agent-identifier
1004      :name DSA@dispatch.com)
1005   :receiver (set
1006     (agent-identifier
1007      :name MAiG@gateway.com))
1008   :ontology FIPA-Nomadic-Application
1009   :language FIPA-SL2
1010   :protocol FIPA-Subscribe
1011   :content
1012     (iota ?x
1013      (qos-information
1014       (comm-channel
1015        :name GPRS
1016        :target-addr iiop://paramedic.com/acc)
1017       (qos
1018        :status ?x))))
1019
1020

```

1021 10. Message 10 query-ref: The DSA requests current quality of service of the GPRS MTC from MAiG.

```

1022 (query-ref
1023   :sender
1024     (agent-identifier
1025      :name DSA@dispatch.com)
1026   :receiver (set
1027     (agent-identifier
1028      :name MAiG@gateway.com))
1029   :ontology FIPA-Nomadic-Application
1030   :language FIPA-SL2
1031   :protocol FIPA-Query
1032   :content
1033     (iota ?x
1034      (qos-information
1035       (comm-channel
1036        :name GPRS)
1037       (qos
1038        :throughput ?x)))
1039
1040

```

1041 11. Message 11 inform: MAiG informs the DSA the current quality of service of the GPRS MTC.

```

1042 (inform
1043   :sender
1044     (agent-identifier
1045      :name MAiG@gateway.com)
1046   :receiver (set
1047     (agent-identifier
1048      :name DSA@dispatch.com))
1049   :ontology FIPA-Nomadic-Application
1050   :language FIPA-SL2
1051   :protocol FIPA-Query
1052   :content
1053     (= (iota ?x
1054        (qos-information
1055         (comm-channel
1056          :name GPRS)
1057         (qos
1058          :throughput ?x)))
1059        (rate-value
1060         :direction Outbound)
1061

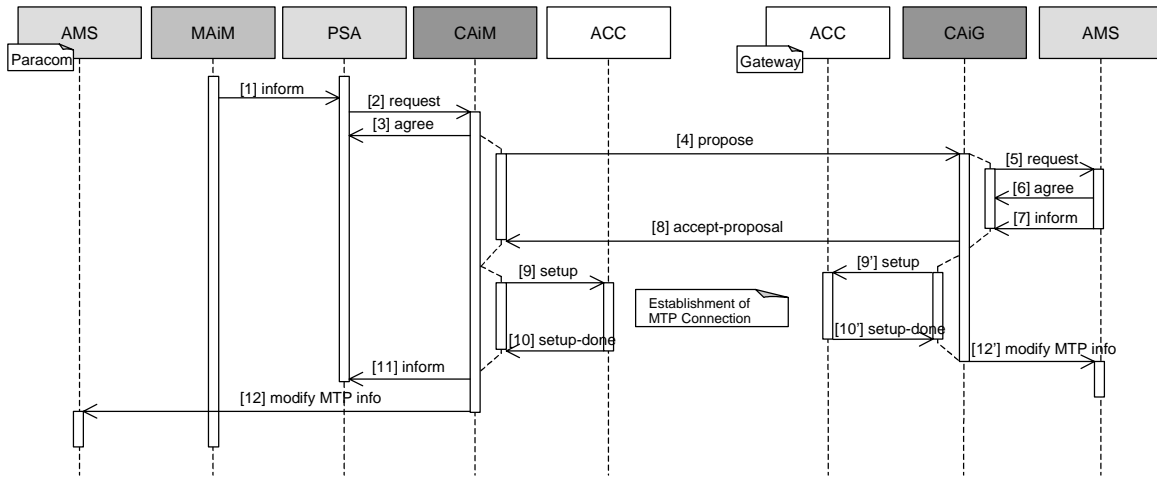
```

```
1062 :unit Kbits/s
1063 :value 20)))
1064
```

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

1067 **4.2.2 Example Negotiation of a Message Transport Protocol**

1068 When the mobile host roams from the ATM network to the GPRS network – after the reconnection – the PSA receives
 1069 the information from MAiM that the *Paracom* AP is now connected to the GPRS MTC. The PSA reasons that the
 1070 *fipa.mts.mtp.wap.std* MTP is better in that environment and it requests the CAiM to establish this MTP between
 1071 ACCiM and ACCiG. Also, CAiM proposes the establishment of this MTP to CAiG which accepts and they command their
 1072 respective ACCs to set it up. As a last action, both CAiF and CAiG modify the AP descriptions of their APs. The
 1073 message flow is illustrated in *Figure 10*.
 1074



1075 **Figure 10: Example Negotiation of a Message Transport Protocol**
 1076
 1077

1079 1. Message 1 *inform*: MAiM informs the PSA that the *Paracom* AP is now connected to the GPRS network.

```
1081 (inform
1082 :sender
1083 (agent-identifier
1084 :name MAiM@paracom.com)
1085 :receiver (set
1086 (agent-identifier
1087 :name PSA@paracom.com))
1088 :ontology FIPA-Nomadic-Application
1089 :language FIPA-SL2
1090 :protocol FIPA-Subscribe
1091 :content
1092 (= (iota ?x
1093 (qos-information
1094 (comm-channel
1095 :name GPRS
1096 :target-addr wap://paramedic.com:1234/acc)
1097 (qos
1098 :status ?x))))
1099 connected))
1100
1101
```

1101 2. Message 2 request and message 3 agree: The PSA requests CAiM to establish the fipa.mts.mtp.wap.std
 1102 MTP between ACCiM and ACCiG.

```
1103
1104 (request
1105   :sender
1106     (agent-identifier
1107       :name PSA@paracom.com)
1108   :receiver (set
1109     (agent-identifier
1110       :name CAiM@paracom.com))
1111   :ontology FIPA-Nomadic-Application
1112   :language FIPA-SL0
1113   :protocol FIPA-Request
1114   :content
1115     (action
1116       (agent-identifier
1117         :name CAiM@paracom.com)
1118       (activate (sequence
1119         (transport-protocol
1120           :name fipa.mts.mtp.wap.std
1121           :gw-addr wap://gateway.com:1234/acc))))))
1122
```

1123 3. Message 4 propose: CAiM sends a propose message to the CAiG.

```
1124
1125 To: (agent-identifier :name CAiG@gateway.com)
1126 From: (agent-identifier :name CAiM@paracom.com)
1127 ACL-representation: fipa.acl.rep.string.std
1128 Date: 20000606T101200000
1129
```

```
1130 (propose
1131   :sender
1132     (agent-identifier
1133       :name CAiM@paracom.com)
1134   :receiver (set
1135     (agent-identifier
1136       :name CAiG@gateway.com))
1137   :ontology FIPA-Nomadic-Application
1138   :language FIPA-SL0
1139   :protocol FIPA-Propose
1140   :content
1141     ((action
1142       (agent-identifier
1143         :name CAiM@paracom.com)
1144       (use
1145         (transports
1146           :send (sequence
1147             (transport-protocol
1148               :name fipa.mts.mtp.wap.std))
1149           :recv (sequence
1150             (transport-protocol
1151               :name fipa.mts.mtp.wap.std))))))
1152     true))
1153
```

1154 4. Message 5 request, message 6 agree and message 7 inform: CAiG requests the local AP description to find
 1155 out if the fipa.mts.mtp.wap.std MTP is supported (see [FIPA00023]).
 1156
 1157

1157 5. Message (8) accept-proposal: CAiG accepts CAiM's proposal to use the fipa.mts.mtp.wap.std MTP.

```
1158 To: (agent-identifier :name CAiM@paracom.com)
1159 From: (agent-identifier :name CAiG@gateway.com)
1160 ACL-representation: fipa.acl.rep.string.std
1161 Date: 20000606T101200000
```

```
1163
1164 (accept-proposal
1165   :sender
1166     (agent-identifier
1167       :name CAiG@gateway.com)
1168   :receiver (set
1169     (agent-identifier
1170       :name CAiM@paracom.com))
1171   :ontology FIPA-Nomadic-Application
1172   :language FIPA-SL0
1173   :protocol FIPA-Propose
1174   :content
1175     (action
1176       (agent-identifier
1177         :name CAiM@paracom.com)
1178       (use
1179         (transports
1180           :send (sequence
1181             (transport-protocol
1182               :name fipa.mts.mtp.wap.std))
1183           :recv (sequence
1184             (transport-protocol
1185               :name fipa.mts.mtp.wap.std))))))
1186     (transports
1187       :send (sequence
1188         (transport-protocol
1189           :name fipa.mts.mtp.wap.std))
1190       :recv (sequence
1191         (transport-protocol
1192           :name fipa.mts.mtp.wap.std))))))
1193
```

1194 6. Messages 9 and 9' setup and messages 10 and 10' setup-done: CAiM (CAiG) commands ACCiM (ACCiG) to
 1195 setup the fipa.mts.mtp.wap.std MTP. As this is intra-platform communication between CAiM (CAiG) and
 1196 ACCiM (ACCiG), this is an implementation issue.

1197
 1198 7. Message 11 inform: CAiM returns the result to the PSA.

```
1199 (inform
1200   :sender
1201     (agent-identifier
1202       :name CAiM@paracom.com)
1203   :receiver (set
1204     (agent-identifier
1205       :name PSA@paracom.com))
1206   :ontology FIPA-Nomadic-Application
1207   :language FIPA-SL0
1208   :protocol FIPA-Request
1209   :content
1210     (result
1211       (action
1212         (agent-identifier
1213           :name CAiM@paracom.com)
1214         (activate (sequence
1215           (transport-protocol
1216             :name fipa.mts.mtp.wap.std
1217             :gw-addr wap://gateway.com:1234/acc))))
1218       (transport-protocol
```

```

1220         :name fipa.mts.mtp.wap.std
1221         :gw-addr wap://gateway.com:1234/acc)))
1222
1223 8. Message 12 and 12' set-description: CAiM (CAiG) modifies the AP description to show that the
1224 fipa.mts.mtp.wap.std is now active.
1225

```

1226 **4.2.3 Example Negotiation of a Message Representation**

1227 MAiM informs the PSA that the quality of the message transport connection has dropped significantly. The PSA reasons
1228 that the ACL representation needs to be changed to `fipa.acl.rep.bitefficient.std` and it proposes that to the
1229 DSA. The DSA accepts the PSA's proposal. The message flow is illustrated in *Figure 11*.
1230

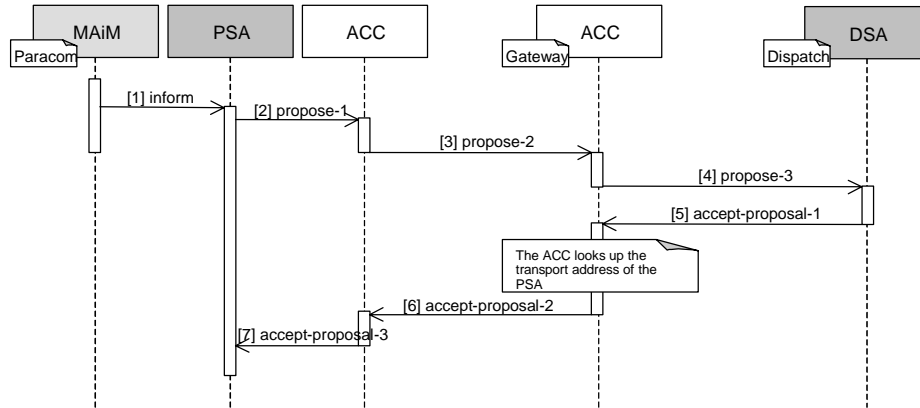


Figure 11: Example Negotiation of a Message Representation

1231 1. Message 1 `inform`: The MA informs the PSA that the outbound throughput has changed.

```

1232
1233
1234
1235
1236
1237 (inform
1238   :sender
1239     (agent-identifier
1240       :name MAiM@paracom.com)
1241   :receiver (set
1242     (agent-identifier
1243       :name PSA@paracom.com))
1244   :ontology FIPA-Nomadic-Application
1245   :language FIPA-SL2
1246   :protocol FIPA-Subscribe
1247   :content
1248     (= (iota ?x (
1249       (qos-notification
1250         (comm-channel
1251           :name GPRS)
1252         (throughput
1253           (rate-value
1254             :unit Kbits/s
1255             :direction Outbound
1256             :value ?x))
1257         (change-constraint
1258           :value (<
1259             (qos
1260               :throughput
1261                 (rate-value
1262                   :unit Kbits/s
1263                   :direction Outbound
1264                   :value 1)))))))
1265     (0.96)))
1266
1267

```

1267 2. Message 2 propose-1: Based on the new throughput value, the PSA decides to change to the message
 1268 representation.

```

1269
1270 To: (agent-identifier :name DSA@dispatch.com)
1271 From: (agent-identifier :name PSA@paracom.com)
1272 ACL-representation: fipa.acl.rep.string.std
1273 Date: 20000606T101200000
1274
1275 (propose
1276   :sender
1277     (agent-identifier
1278       :name PSA@paracom.com)
1279   :receiver (set
1280     (agent-identifier
1281       :name DSA@dispatch.com))
1282   :ontology FIPA-Message-Representation
1283   :language FIPA-SL0
1284   :protocol FIPA-Propose
1285   :content
1286     ((action
1287       (agent-identifier
1288         :name PSA@paracom.com)
1289       (use
1290         (msg-rep-selection
1291           :send (sequence
1292             (msg-representation
1293               :name fipa.acl.rep.bitefficient.std))
1294           :recv (sequence
1295             (msg-representation
1296               :name fipa.acl.rep.bitefficient.std))))))
1297     true))
1298

```

1299 3. Message 3 propose-2: The ACC at the mobile host forwards the same message to the ACC at the gateway host.

1300
 1301 4. Message 4 propose-3: The ACC at the gateway host forwards the same message to the PSA.

1302
 1303 5. Message 5 accept-proposal-1: The PSA accepts the proposal and sends a message back to the DSA.

```

1304
1305 To: (agent-identifier :name PSA@paracom.com)
1306 From: (agent-identifier :name DSA@dispatch.com)
1307 ACL-representation: fipa.acl.rep.string.std
1308 Date: 20000606T101200000
1309
1310 (accept-proposal
1311   :sender
1312     (agent-identifier
1313       :name DSA@dispatch.com)
1314   :receiver (set
1315     (agent-identifier
1316       :name PSA@paracom.com))
1317   :ontology FIPA-Message-Representation
1318   :language FIPA-SL0
1319   :protocol FIPA-Propose
1320   :content
1321     (action
1322       (agent-identifier
1323         :name PSA@paracom.com)
1324       (use
1325         (msg-rep-selection
1326           :send (sequence
1327             (msg-representation
1328               :name fipa.acl.rep.bitefficient.std))

```

```
1329         :recv (sequence
1330             (msg-representation
1331              :name fipa.acl.rep.bitefficient.std))))
1332 (msg-rep-selection
1333  :send (sequence
1334        (msg-representation
1335         :name fipa.acl.rep.bitefficient.std))
1336  :recv (sequence
1337        (msg-representation
1338         :name fipa.acl.rep.bitefficient.std))))))
```

1339
1340 6. Message 6 `accept-proposal-2`: The ACC at the gateway host forwards same message to the ACC at the
1341 mobile host.

1342
1343 7. Message 7 `accept-proposal-3`: The ACC at the mobile host delivers the same message to the PSA.

1344

5 References

- 1344
- 1345 [FIPA00023] FIPA Agent Management Specification. Foundation for Intelligent Physical Agents, 2000.
1346 <http://www.fipa.org/specs/fipa00023/>
- 1347 [FIPA00036] FIPA Agent Management Specification. Foundation for Intelligent Physical Agents, 2000.
1348 <http://www.fipa.org/specs/fipa00036/>
- 1349 [FIPA00062] FIPA Nomadic Application Support Monitor Agent Specification. Foundation for Intelligent Physical
1350 Agents, 2000. <http://www.fipa.org/specs/fipa00062/>
- 1351 [FIPA00063] FIPA Nomadic Application Support Control Agent Specification. Foundation for Intelligent Physical
1352 Agents, 2000. <http://www.fipa.org/specs/fipa00063/>
- 1353 [FIPA00065] FIPA Nomadic Application Support Ontology Specification. Foundation for Intelligent Physical Agents,
1354 2000. <http://www.fipa.org/specs/fipa00065/>
- 1355 [FIPA00069] FIPA ACL Message Representation in Bit-Efficient Encoding Specification. Foundation for Intelligent
1356 Physical Agents, 2000. <http://www.fipa.org/specs/fipa00069/>
- 1357 [FIPA00075] FIPA Agent Message Transport Protocol for IOP Specification. Foundation for Intelligent Physical
1358 Agents, 2000. <http://www.fipa.org/specs/fipa00075/>
- 1359 [FIPA00076] FIPA Agent Message Transport Protocol for WAP Specification. Foundation for Intelligent Physical
1360 Agents, 2000. <http://www.fipa.org/specs/fipa00076/>
- 1361 [WAP99] Wireless Application Protocol Specification Version 1.2. WAP Forum, 1999.
1362 <http://www.wapforum.org/what/technical.htm>