



**Implementation Agreement for MGCP IA Call
Agent <-> User Agent Security Addendum
(Version 2)**

MSF-IA-MGCP.002v2-FINAL

MultiService Forum Implementation Agreement

Contribution Number: msf2007.002.00

Document Filename: MSF-IA-MGCP.002v2-FINAL

Working Group: Protocol and Control

Title: Implementation Agreement for MGCP IA Call Agent <-> User Agent Security Addendum (Version 2)

Editor: Jon Rowland
MetaSwitch
jon.rowland@metaswitch.com

Working Group Chairperson: Chris Gallon, Fujitsu

Date: 24 May 2007

Abstract: This contribution is an updated version of the existing MSF-IA-MGCP.002-FINAL MGCP IA Call Agent <-> User Agent Security Addendum (msf 2004.008.002). It proposes updates to deal with an illegal MGCP syntax used in the original IA.

The MultiService Forum (MSF) is responsible for developing Implementation Agreements or Architectural Frameworks which can be used by developers and network operators to ensure interoperability between components from different vendors. MSF Implementation Agreements are formally ratified via a Straw Ballot and then a Principal Member Ballot.

Draft MSF Implementation Agreements or Architectural Framework may be published before formal ratification via Straw or Principal Member Ballot. In order for this to take place, the MSF Technical Committee must formally agree that a draft Implementation Agreement or Architectural Framework should be progressed through the balloting process. A Draft MSF Implementation Agreement or Architectural Framework is given a document number in the same manner as an Implementation Agreement.

Draft Implementation Agreements may be revised before or during the full balloting process. The revised document is allocated a new major or minor number and is published. The original Draft Implementation Agreement or Architectural Framework remains published until the Technical Committee votes to withdraw it.

After being ratified by a Principal Member Ballot, the Draft Implementation Agreement or Architectural Framework becomes final. Earlier Draft Implementation Agreements or Architectural Frameworks remain published until the Technical Committee votes to withdraw them.

The use of capitalization of the key words "MUST", "SHALL", "REQUIRED", "MUST NOT", "SHOULD NOT", "SHOULD", "RECOMMENDED", "NOT RECOMMENDED", "MAY" or "OPTIONAL" is as described in section V-B of the MSF Technical Committee Operating Procedures.

The goal of the MSF is to promote multi-vendor interoperability as part of a drive to accelerate the deployment of next generation networks. To this end the MSF looks to adopt pragmatic solutions in order to maximize the chances for early deployment in real world networks.

To date the MSF has defined a number of detailed Implementation Agreements and detailed Test Plans for the signaling protocols between network components and is developing additional Implementation Agreements and Test Plans addressing some of the other technical issues such as QoS and Security to assist vendors and operators in deploying interoperable solutions.

The MSF welcomes feedback and comment and would encourage interested parties to get involved in this work program. Information about the MSF and membership options can be found on the MSF website <http://www.msforum.org/>

Note: Attention is called to the possibility that use or implementation of this MSF Implementation Agreement may require use of subject matter covered by intellectual property rights owned by parties who have not authorized such use. By publication of this Implementation Agreement, no position is taken by MSF as its Members with respect to the existence or validity of any intellectual property rights in connection therewith, nor does any warranty, express or implied, arise by reason of the publication by MSF of this Implementation Agreement. Moreover, the MSF shall not have any responsibility whatsoever for determining the existence of IPR for which a license may be required for the use or implementation of an MSF Implementation Agreement, or for conducting inquiries into the legal validity or scope of such IPR that is brought to its attention.

DISCLAIMER

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and the MultiService Forum is not responsible for any errors or omissions. The MultiService Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything to the contrary, neither the MultiService Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind whether based on theories of tort, contract, strict liability or otherwise, shall be assumed or incurred by the MultiService Forum, its member companies, or the publisher as a result of reliance or use by any party upon any information contained in this publication. All liability for any implied or express warranty of merchantability or fitness for a particular purpose is hereby disclaimed.

The receipt or any use of this document or its contents does not in any way create by implication or otherwise:

Any express or implied license or right to or under any MultiService Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

Any warranty or representation that any MultiService Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

Any commitment by a MultiService Forum company to purchase or otherwise procure any product(s) and/or service(s) that embody any or all of the ideas, technologies, or concepts contained herein; nor

Any form of relationship between any MultiService Forum member companies and the recipient or user of this document.

Implementation or use of specific MultiService Forum Implementation Agreements, Architectural Frameworks or recommendations and MultiService Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in the MultiService Forum.

For addition information contact:

MultiService Forum
 48377 Fremont Blvd., Suite 117
 Fremont, CA 94538 USA
 Phone: +1 510 492-4050
 Fax: +1 510 492-4001
info@msforum.org
<http://www.msforum.org>

TABLE OF CONTENTS

1	MULTISERVICE FORUM	5
2	APPLICABILITY AND SCOPE	5
3	ENHANCED HTTP DIGEST SECURITY.....	5
APPENDIX A MGCP CALL FLOWS.....		8
A.1	START-UP	9
A.2	START-UP WITH AUTHENTICATION	12
A.3	CALL SET-UP AND TEAR-DOWN	13
APPENDIX B HISTORICAL ERRATA		19
B.1	SYNTAX OF WWW-AUTHENTICATE HEADER.....	19

1 MultiService Forum

The goal of the MSF is to promote multi-vendor interoperability as part of a drive to accelerate the deployment of next generation networks. To this end the MSF looks to adopt pragmatic solutions in order to maximize the chances for early interoperability in real world networks.

To date the MSF has defined a number of detailed Implementation Agreements and detailed Test Plans for the signaling protocols between network components and is developing additional Implementation Agreements and Test Plans addressing some of the other technical issues such as QoS and Security to assist vendors and operators in deploying interoperable solutions.

The MSF welcomes feedback and comment and would encourage interested parties to get involved in this work program. Information about the MSF and membership options can be found on the MSF website <http://www.msforum.org/>

2 Applicability and Scope

This contribution proposes an addendum to the MGCP Call Agent <-> User Agent Implementation Agreement to add optional support for enhanced authentication using HTTP Digest.

This addendum has the same applicability as the MGCP IA

3 Enhanced HTTP Digest Security

In some circumstances, extensions to MGCP 1.0 may be required for enhanced security using HTTP digest to authenticate MGCP messages from the CPE. For example, when MGCP is used to control CPE that may be moved between different LANs.

HTTP digest security from RFC 2617 is implemented as follows:

- The Call Agent and the CPE are both configured with an MGCP domain-name and password, which provides a shared secret for HTTP digest. The CPE must securely encrypt the stored version of the password.
- If MGCP security extensions are configured for a subscriber line or group of subscriber lines, the Call Agent will challenge any RSIP received without a valid authorization header by rejecting the request with a 401 Unauthorized error code. The challenge takes the form of a WWW-Authenticate header appended to the end of the response to the RSIP specifying the nonce, opaque data. Depending on the options for the subscriber, the Call Agent may specify qop="auth-int" only i.e.authentication and integrity checking is required.

All further RSIP, DLCX or NTFY MGCP (i.e. all non response messages sent to the call agent) messages from the Subscriber Gateway or Broadband Loop Carriers must include an "Authorization" header appended to the end of the MGCP message. The Subscriber Gateway or Broadband Loop Carrier must increment the "nc" field on each subsequent message. Note that if qop="auth-int" integrity checking is used this covers, in particular, the dialed digits specified on a NTFY request.

- The Call Agent may optionally require authentication of AUEP responses by including a WWW-Authenticate header in the AUEP request. If the WWW-Authenticate header is included in the AUEP request the Subscriber Gateway or Broadband Loop Carrier must include an “Authorization” header appended to the end of the MGCP response. The CA will not include WWW-Authenticate headers in other non-AUEP requests nor challenge any responses to requests it has sent to the CPE.
- The Call Agent may issue a new challenge containing a new nonce and opaque value at any time in response to an RSIP, DLCX or NTFY request or an AUEP request.
- The Call Agent may run a session timer to force re-authentication of the CPE. When the timer expires it may send an AUEP request with a new challenge containing a new nonce and opaque value or wait for the next RSIP, DLCX or NTFY request and issue the new challenge on the response.
- Only Digest security from RFC 2617 is supported. “basic” authentication is not supported and must not be used.

For the purposes of clarification, the following definitions must be used for the HTTP digest flows in place of the standard values in RFC 2617.

- A WWW-Authenticate header is carried in MGCP using the “X+WWWAuthenticate” header and has the same BNF (apart from the name) as the WWW-Authenticate header in RFC 2617.
- An Authorization header is carried in MGCP using the “X+Authorization” header and have the same BNF (apart from the name) as the Authorization header in RFC 2617.
- URI = “MGCP”
- The realm value a server name configured on the VCA. It is sent in the WWW-Authenticate header and must be returned in the Authorization header sent by the CPE.
- algorithm = “algorithm” “=” “MD5”
- The method value is the MGCP transaction name in upper case (“NTFY”, “DLCX” or “RSIP”). This is the case even though the MGCP protocol is generally case insensitive, and the transaction name is not taken out of the MGCP message received.
- The example procedure for choosing a nonce value based on Etag does not apply to MGCP and is not used by the CA.
- The text in RFC 2617 regarding cache operation does not apply to MGCP.
- H(entity body) is calculated on the entire MGCP message excluding the Authorization header, the transaction identifier in the command line (including any space delimiter following this field) and the Request Identifier (X:) line (for NTFY requests, and including any CR/LF terminating this line). These exclusions allow this HTTP digest security to operate correctly when deployed in conjunction with a session border controller. See the colour-coded examples in Appendix A.
- Proxy-authenticate mechanisms and headers are not applicable to MGCP and must not be used.
- To comply with MGCP formatting rules, all parameters for an authenticate or authorization header must be sent on a single line terminated by carriage return. They cannot be split across separate lines as shown in the examples in RFC 2617.

- Cnonce is not supported, as it is not necessary for authentication of the CPE to the CA. The cnonce parameter must be sent as a null string for compatibility with the formats listed in RFC 2617.

Sample flows using HTTP Authentication are given in appendix A.

Appendix A MGCP Call Flows

This appendix contains some example MGCP call flows using enhanced MGCP security.

- Start-up
- Call Set-up and Tear-Down

The flows just present the MGCP flows and ignore interactions with the PSTN. The term Subscriber Gateway is used generically for any MGCP Media Gateway, whether it is an IAD, MGCP Phone or Broadband Loop Carrier.

A.1 Start-up

The following call flow diagram depicts the MGCP messaging for start-up processing, including setting each line termination to detect off-hook events and collect digits according to a digit map.

```
CA                               Subscriber Gateway

----->
AUEP 334 AALN/*@[192.168.19.11] MGCP 1.0

<-----
RSIP 16838 aaln/1@[192.168.19.11] MGCP 1.0
RM: restart

<-----
RSIP 16839 aaln/2@[192.168.19.11] MGCP 1.0
RM: restart

<-----
RSIP 16840 aaln/3@[192.168.19.11] MGCP 1.0
RM: restart

----->
200 16838 OK

<-----
RSIP 16841 aaln/4@[192.168.19.11] MGCP 1.0
RM: restart

----->
200 16839 OK

----->
200 16840 OK

----->
200 16841 OK

<-----
200 334 OK
Z: aaln/1@[192.168.19.11]
Z: aaln/2@[192.168.19.11]
Z: aaln/3@[192.168.19.11]
Z: aaln/4@[192.168.19.11]

----->
DLCX 335 AALN/1@[192.168.19.11] MGCP 1.0

<-----
```

Implementation Agreement for MGCP IA Call Agent <-> User Agent Security Addendum (Version 2)

250 335 Connection was deleted

----->
DLCX 336 AALN/2@[192.168.19.11] MGCP 1.0

<-----
250 336 Connection was deleted

----->
DLCX 337 AALN/3@[192.168.19.11] MGCP 1.0

<-----
250 337 Connection was deleted

----->
DLCX 338 AALN/4@[192.168.19.11] MGCP 1.0

<-----
250 338 Connection was deleted

----->
RQNT 339 AALN/1@[192.168.19.11] MGCP 1.0
X: 1
R: L/HD(E(R(L/HU(N),D/[0-9A-D#*T](D),L/OC(N)),S(L/DL),
D((0T|00|01T|011XXXXX.T|01XXXXX.T|0[2-9]T|0[2-9]11|0[2-9]XXXXXXT|
0[2-9]XXXXXXXX|10T|100|101T|101XXXX|10[2-9]|11T|11[2-4]XX|
11[015-9]X|1[2-9]11|1[2-9]XXXXXXXX|[23]11|[23]XXXXXX|456|
[2-9]XT|[4-9]11|[4-9]XXXXXX|[2-4]XX|[015-9]X|[2-9]T))) ,A)
S:
Q: STEP
T: L/HU,L/HD,L/HF,D/[0-9A-D#*T]

<-----
200 339 OK

----->
RQNT 340 AALN/2@[192.168.19.11] MGCP 1.0
X: 1
R: L/HD(E(R(L/HU(N),D/[0-9A-D#*T](D),L/OC(N)),S(L/DL),
D((0T|00|01T|011XXXXX.T|01XXXXX.T|0[2-9]T|0[2-9]11|0[2-9]XXXXXXT|
0[2-9]XXXXXXXX|10T|100|101T|101XXXX|10[2-9]|11T|11[2-4]XX|
11[015-9]X|1[2-9]11|1[2-9]XXXXXXXX|[23]11|[23]XXXXXX|456|
[2-9]XT|[4-9]11|[4-9]XXXXXX|[2-4]XX|[015-9]X|[2-9]T))) ,A)
S:
Q: STEP
T: L/HU,L/HD,L/HF,D/[0-9A-D#*T]

<-----

200 340 OK

```

----->
RQNT 341 AALN/3@[192.168.19.11] MGCP 1.0
X: 1
R: L/HD(E(R(L/HU(N),D/[0-9A-D#*T](D),L/OC(N)),S(L/DL),
  D((0T|00|01T|011XXXXX.T|01XXXXX.T|0[2-9]T|0[2-9]11|0[2-9]XXXXXXT|
  0[2-9]XXXXXXXX|10T|100|101T|101XXXX|10[2-9]|11T|11[2-4]XX|
  11[015-9]X|1[2-9]11|1[2-9]XXXXXXXX|[23]11|[23]XXXXXX|456|
  [2-9]XT|[4-9]11|[4-9]XXXXXX|[2-4]XX|[015-9]X|[2-9]T))) ,A)
S:
Q: STEP
T: L/HU,L/HD,L/HF,D/[0-9A-D#*T]

```

```

<-----
200 341 OK

```

```

----->
RQNT 342 AALN/4@[192.168.19.11] MGCP 1.0
X: 1
R: L/HD(E(R(L/HU(N),D/[0-9A-D#*T](D),L/OC(N)),S(L/DL),
  D((0T|00|01T|011XXXXX.T|01XXXXX.T|0[2-9]T|0[2-9]11|0[2-9]XXXXXXT|
  0[2-9]XXXXXXXX|10T|100|101T|101XXXX|10[2-9]|11T|11[2-4]XX|
  11[015-9]X|1[2-9]11|1[2-9]XXXXXXXX|[23]11|[23]XXXXXX|456|
  [2-9]XT|[4-9]11|[4-9]XXXXXX|[2-4]XX|[015-9]X|[2-9]T))) ,A)
S:
Q: STEP
T: L/HU,L/HD,L/HF,D/[0-9A-D#*T]

```

```

<-----
200 342 OK

```

A.2 Start-up with Authentication

The following call flow diagram depicts the MGCP messaging for start-up processing, including HTTP Digest Authentication. The fields highlighted in yellow are excluded from the HTTP digest calculation.

Note that the X+WWWAuthenticate and X+Authorization headers actually flow in the MGCP messages as a single line terminated by EOL but are shown as multiple lines below for clarity in this document.

CA	Subscriber Gateway
----->	
AUEP 334 AALN/*@[192.168.19.11] MGCP 1.0	
<-----	
RSIP 16838 aaln/1@[192.168.19.11] MGCP 1.0	
RM: restart	
----->	
401 16838 Unauthorized	
X+WWWAuthenticate: Digest realm="testvoiceservice",qop="auth-int",	
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",	
opaque="5ccc069c403ebaf9f0171e9517f40e41"	
<-----	
RSIP 16839 aaln/1@[192.168.19.11] MGCP 1.0	
RM: restart	
X+Authorization: Digest username="[192.168.19.11]",	
realm="testvoiceservice",nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",	
uri="MGCP",qop=auth-int,nc=00000001,cnonce="",	
response="6629fae49393a05397450978507c4ef1",	
opaque="5ccc069c403ebaf9f0171e9517f40e41"	
----->	
200 16839 OK	

```

<-----
200 334 OK
Z: aaln/1@[192.168.19.10]

----->
DLCX 335 AALN/1@[192.168.19.10] MGCP 1.0

<-----
250 335 Connection was deleted

----->
RQNT 336 AALN/1@[192.168.19.10] MGCP 1.0
X: 1
R: L/HD(E(R(L/HU(N),D/[0-9A-D#*T](D),L/OC(N)),S(L/DL),
D((0T|00|01T|011XXXXX.T|01XXXXX.T|0[2-9]T|0[2-9]11|0[2-9]XXXXXXT|
0[2-9]XXXXXXXX|10T|100|101T|101XXXX|10[2-9]|11T|11[2-4]XX|
11[015-9]X|1[2-9]11|1[2-9]XXXXXXXX|[23]11|[23]XXXXXX|456|
[2-9]XT|[4-9]11|[4-9]XXXXXX|[2-4]XX|[015-9]X|[2-9]T)),A)
S:
Q: STEP
T: L/HU,L/HD,L/HF,D/[0-9A-D#*T]

<-----
200 336 OK

```

A.3 Call Set-Up and Tear-down

This call flow diagram depicts the MGCP messaging for a call set-up and tear-down for a call placed by user1 connected to one Subscriber Gateway1 to user2 connected to a different Subscriber Gateway2. The call is routed by the Call Agent via its internal Access gateway, but for simplicity this is not shown. Bearer data is carried over an IP network.

Call flows to and from the PSTN are just one half or the other of the flow given below.

In the example below, SG1 is using HTTP digest authentication but SG2 has been configured to allow connection without use of digest authentication in order to show the differences between the two cases. The fields highlighted in yellow are excluded from the HTTP digest calculation.

Note that the X+WWWAuthenticate and X+Authorization headers actually flow in the MGCP messages as a single line terminated by EOL but are shown as multiple lines below for clarity in this document.

SG1

CA

SG2

User 1 dials User 2

```

----->
NTFY 16862 aaln/1@[192.168.19.10] MGCP 1.0

```

X: 1

O: 1/hd,d/2,d/0,d/0,d/0,d/4,d/0,d/6
 X+Authorization: Digest username="[192.168.19.10]",
 realm="testvoiceservice",nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
 uri="MGCP",qop=auth-int,nc=00000002,cnonce="",
 response="7ad64431b6723c9188eea7500823b794",
 opaque="5ccc069c403ebaf9f0171e9517f40e7d"

<-----
 200 16862 OK

<-----
 RQNT 161 AALN/1@[192.168.19.10] MGCP 1.0
 X: 1
 R: L/HU(N)
 Q: STEP
 T: L/HU,L/HD,L/HF,D/[0-9A-D#*T]

----->
 200 161 OK

<-----
 CRCX 163 AALN/1@[192.168.19.10] MGCP 1.0
 C: 5
 L: A:PCMU,P:20,E:ON,S:OFF,T:00
 M: RECVONLY

----->
 200 163 OK
 I: 1687

v=0
 o=SG1 5767 163 IN IP4 192.168.19.10
 s=SG1
 c=IN IP4 192.168.19.10
 b=AS:64
 t=0 0
 m=audio 3456 RTP/AVP 0
 a=recvonly
 a=ptime:20

----->
 CRCX 164 AALN/3@[192.168.25.2] MGCP 1.0
 C: 9
 L: A:PCMU,P:10,E:ON,S:OFF,T:00
 M: RECVONLY

```
<-----  
200 164 OK  
I: 1831426C  
  
v=0  
o=- 2209081772 2209081772 IN IP4  
192.168.25.2  
  
s=SG2  
c=IN IP4 192.168.25.2  
t=0 0  
m=audio 5004 RTP/AVP 0 96  
a=rtpmap:96 G726-32/8000
```

```
----->  
MDCX 165 AALN/3@[192.168.25.2] MGCP 1.0  
C: 9  
I: 1831426C  
L: A:PCMU,P:10,E:ON,S:OFF,T:00  
M: SENDRECV
```

```
v=0  
o=- 1039626063657 1039626063657 IN IP4  
192.168.18.16  
  
s=-  
c=IN IP4 192.168.18.16  
t=0 0  
m=audio 4110 RTP/AVP 0
```

```
<-----  
200 165 OK  
  
v=0  
o=- 2209081772 2209081772 IN IP4  
192.168.25.2  
  
s=SG2  
c=IN IP4 192.168.25.2  
t=0 0  
m=audio 5004 RTP/AVP 0
```

```
----->  
RQNT 166 AALN/3@[192.168.25.2] MGCP 1.0  
X: 1  
R: L/HD(N)  
S: L/CI(12/11/17/01,2012000400,O),L/RG,  
G/RT@*  
Q: STEP
```

T: L/HU,L/HD,L/HF,D/[0-9A-D#*T]

<-----
200 166 OK

User 2 Phone is ringing and Caller ID Presented

<-----
MDCX 168 AALN/1@[192.168.19.10] MGCP 1.0
C: 5
I: 1687
L: A:PCMU,P:20,E:ON,S:OFF,T:00
M: SENDRECV

v=0
o=- 1039626063785 1039626063785 IN IP4 192.168.18.17
s=-
c=IN IP4 192.168.18.17
t=0 0
m=audio 4080 RTP/AVP 0

----->
200 168 OK

User 2 picks up

<-----
ntfy 51 aaln/3@[192.168.25.2] MGCP 1.0
X: 1
O: 1/HD

----->
200 51 OK

----->
RQNT 169 AALN/3@[192.168.25.2] MGCP 1.0
X: 1
R: L/HU(N)
S:
Q: STEP
T: L/HU,L/HD,L/HF,D/[0-9A-D#*T]

<-----
200 169 OK

User 1 Hangs Up

```

----->
NTFY 16863 aaln/1@[192.168.19.10]
MGCP 1.0
X: 1
O: l/hu
X+Authorization: Digest username="[192.168.19.10]",
realm="testvoiceservice",nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
uri="MGCP",qop=auth-int,nc=00000003,cnonce="",
response="723c9188eea7500823b7947ad64431b6",
opaque="5ccc069c403ebaf9f0171e9517f40e7d"

<-----
200 16863 OK

<-----
DLCX 171 AALN/1@[192.168.19.10] MGCP 1.0
C: 5
I: 1687

----->
250 171 Connection was deleted
P: PS=1530, OS=244440, PR=1537, OR=245920, PL=0, JI=23, LA=56

----->
DLCX 172 AALN/3@[192.168.25.2] MGCP 1.0
C: 9
I: 1831426C

<-----
250 172 OK
P: PS=2047, OS=245640, PR=1543,
OR=246880, PL=0, JI=0, LA=25

----->
RQNT 173 AALN/3@[192.168.25.2] MGCP 1.0
X: 1
R: L/HU(N)
S: L/RO
Q: STEP
T: L/HU,L/HD,L/HF,D/[0-9A-D#*T]

<-----
200 173 OK

<-----
RQNT 174 AALN/1@[192.168.19.10] MGCP 1.0
X: 1
R: L/HD(E(R(L/HU(N),D/[0-9A-D#*T](D),L/OC(N)),S(L/DL),
D((OT|00|01T|011XXXXX.T|01XXXXX.T|0[2-9]T|0[2-9]11|0[2-9]XXXXXT|

```

```

0[2-9]XXXXXXXXXX|10T|100|101T|101XXXX|10[2-9]|11T|11[2-4]XX|
11[015-9]X|1[2-9]11|1[2-9]XXXXXXXXXX|[23]11|[23]XXXXXX|456|
[2-9]XT|[4-9]11|[4-9]XXXXXX|*[2-4]XX|*[015-9]X|[2-9]T)) ,A)

```

S:

Q: STEP

T: L/HU,L/HD,L/HF,D/[0-9A-D#*T]

```

----->
200 174 OK

```

User 2 Hangs Up

```

<-----
ntfy 52 aaln/3@[192.168.25.2] MGCP 1.0
X: 1
O: L/HU

```

```

----->
200 52 OK

```

```

----->
RQNT 176 AALN/3@[192.168.25.2] MGCP 1.0
X: 1
R: L/HD(E(R(L/HU(N),D/[0-9A-
D#*T](D),L/OC(N)),S(L/DL),
D((0T|00|01T|011XXXXX.T|01XXXXX.T|
0[2-9]T|0[2-9]11|0[2-9]XXXXXXT|
0[2-9]XXXXXXXXXX|10T|100|101T|
101XXXX|10[2-9]|11T|11[2-4]XX|
11[015-9]X|1[2-9]11|1[2-9]XXXXXXXXXX|
[23]11|[23]XXXXXX|456|[2-9]XT|
[4-9]11|[4-9]XXXXXX|*[2-4]XX|
*[015-9]X|[2-9]T)) ,A)
S:
Q: STEP
T: L/HU,L/HD,L/HF,D/[0-9A-D#*T]

```

```

<-----
200 176 OK

```

Appendix B Historical Errata

B.1 Syntax of WWW-Authenticate Header

In version 1 of this specification, the MGCP implementation of the WWW-Authenticate header had the syntax “X+WWW-Authenticate”. The presence of the hyphen in the “X+” extension header is illegal in MGCP, and so it has been removed in this updated specification (version 2), so the header becomes “X+WWWAuthenticate”.

It is believed that there are no existing implementations of version 1 of this specification, but implementations may wish to support the old-style header with the hyphen in order to maximize the chance of interoperability.