ETSI TS 101 909-13-1 V1.1.1 (2002-03)

Technical Specification

Digital Broadband Cable Access to the PublicTelecommunications Network; IP Multimedia Time Critical Services; Part 13: Trunking Gateway Control Protocol; Sub-part 1: H.248 option

Reference

DTS/SPAN-120085

Keywords

gateway, H.248, IP, profile

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Services and Protocols for Advanced Networks (SPAN).

The present document is part 13, sub-part 1 of a multi-part deliverable. Full details of the entire series can be found in part 1 [12].

Introduction

The present document defines a solution based on H.248. The solution based on MGCP is defined in TS 101 909-13-2 [13].

Where alternative solutions for the same interface are being considered, interoperability issues between the various IPCablecom system components need to be addressed.

1 Scope

The present document specifies a profile of the H.248 protocol [1] for controlling media gateways between cable networks and the PSTN. This profile is known as Trunking Gateway Control Protocol (TGCP) version 1.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ITU-T Recommendation H.248: "Gateway Control Protocol".

[2] ETSI TS 101 909-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 2: Architectural framework for the delivery of time critical services over cable Television networks using cable modems".

[3] ETSI TS 101 909-3: "Digital Broadband Cable access to the public telecommunications network; IP Multimedia Time Critical Services; Part 3: Audio Codec Requirements for the Provision of Bi-Directional Audio Service over Cable Television Networks using Cable Modems".

[4] ETSI TS 101 909-11: "Digital Broadband Cable access to the public telecommunications network; IP Multimedia Time Critical Services; Part 11: Security".

[5] IETF/RFC 2327 (1988): "SDP: Session Description Protocol".

[6] IETF/RFC 2401 (1998): "Security Architecture for the Internet Protocol".

[7] IETF/RFC 2402 (1998): "IP Authentication Header".

[8] IETF/RFC 1889 (1996): "RTP: A Transport Protocol for Real-Time Applications".

[9] IETF/RFC 2543: "Session Initiation Protocol".

[10] IETF/RFC 2234: "Augmented BNF for Syntax Specifications: ABNF".

[11] IETF/RFC 1890: "RTP Profile for Audio and Video Conferences with Minimal Control".

[12] ETSI TS 101 909-1: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 1: General".

[13] ETSI TS 101 909-13-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 13: Trunking Gateway Control Protocol; Sub-part 2: MGCP option."

[14] IETF/RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASCII	American Standard Code for Information Interchange
AVP	Audio Video Profile
DNS	Domain Name System
IANA	Internet Assigned Number Authority
IP	Internet Protocol
MG	Media Gateway
MGC	Media Gateway Controller
MTA	Message Transfer Agent
PSTN	Public Switched Telephone Network.
RTCP	Real-time Transfer Control Protocol
RTP	Real-time Transfer Protocol
SDP	Session Description Protocol
SPI	Security Parameters Index
TGCP	Trunking Gateway Control Protocol
UDP	User Data Protocol
URI	Universal Ressource Identifier

4 Architectural assumptions

The present document applies to the interface between a Media Gateway Controller and a Media Gateway sitting at the boundary between a packet cable network and the PSTN.

The overall architecture for interconnecting packet cable networks with the PSTN is described in TS 101 909-2 [2].

5 Profile definition

This profile shall be entitled "TGCP". The version number shall be 1.0. This name shall be returned by conforming gateways when sending a ServiceChange command as part of the initial registration of the MG.

5.1 Support of packages

5.1.1 Mandatory packages

The following packages shall be supported:

Table 1: Mandatory packages

Package Name	Id	Version	Defined in
Generic	g	1	ITU Recommendation H.248 [1], annex E
Base Root	root	1	ITU Recommendation H.248 [1], annex E
Continuity	ct	1	ITU Recommendation H.248 [1], annex E
Network	nt	1	ITU Recommendation H.248 [1], annex E
TDM Circuit	tdmc	1	ITU Recommendation H.248 [1], annex E
Tone Detect	tonedet	1	ITU Recommendation H.248 [1], annex E
Call Progress Detect	cd	1	ITU Recommendation H.248 [1], annex E
Tone Generator	tonegen	1	ITU Recommendation H.248 [1], annex E
Call Progress Generator	cg	1	ITU Recommendation H.248 [1], annex E

5.1.2 Optional packages

The following packages may be supported:

Table 2: Optinal packages

Package Name	Id	Version	Defined in
Announcement	an	1	ITU Recommendation H.248 [1], annex K
Modem	mdm	1	ITU Recommendation H.248 [1], annex F
FaxModem	ftmd	1	ITU Recommendation H.248 [1], annex F
Fax	Fax	1	ITU Recommendation H.248 [1], annex F
Security	sec	1	TS 101 909-13-1 [12], clause A.1

5.1.3 Conditional packages

The following optional packages shall be supported under the specified conditions:

Table 3: Conditional packages

Package Name	Condition (e.g. trunk type supported)
Modem	Some of the codec supported by the cable networks are not transparent to modem signals.
FaxModem	Some of the codec supported by the cable networks are not transparent to modem signals.
Fax	Some of the codec supported by the cable networks are not transparent to modem signals.
Security	The RTP/RTCP services defined in TS 101 909-11 [4] are supported.
NOTE: A list of permissible ciphersuites are specified in the IPCablecom Security Specification TS 101 909-11 [4].	

5.2 Compatibility rules

This profile is based on ITU-T Recommendation H.248 [1] version 1 (06/00). The compatibility rules for packages, signals, events, properties and statistics and the H.248 protocol are defined in ITU-T Recommendation H.248 [1].

5.3 Naming conventions

5.3.1 MG and MGC names

MG and MGC names shall be in the form of a domain name. An example MGC name is: `mgc1.whatever.net`

Reliability is provided by the following precautions:

- MGs and MGCs are identified by their domain name, not their network addresses. Several addresses can be associated with a domain name. If a command cannot be forwarded to one of the network addresses, implementations shall retry the transmission using another address.

- MGs and MGCs may move to another platform. The association between a logical name (domain name) and the actual platform are kept in the Domain Name Service (DNS). MG and MGC shall keep track of the record's time-to-live read from the DNS. They shall query the DNS to refresh the information if the time-to-live has expired.

5.3.2 Termination identifiers

Termination identifiers representing physical trunks or trunks groups shall adhere to the following conventions:

- Termination names shall consist of a series of terms each separated by a slash ("/") that describe the physical hierarchy within the gateway:

  ds/<unit-type1>-<unit #>/<unit-type2>-<unit #>/…/<channel #>

- The first term (ds) identifies the termination naming scheme used and the basic termination type.

- The last term is a decimal number that indicates the *channel* number at the lowest level of the hierarchy.

- Intermediate terms between the first term (ds) and last term (channel number) represent intermediate levels of the hierarchy and consist of <unit-type> and <unit #> separated by a hyphen ("-") where:

  - the <unit-type> identifies the particular hierarchy level. Values of <unit-type> presently defined are: "s", "su", "oc3", "ds3", "e3", "ds2", "e2", "ds1", "e1" where "s" indicates a slot number and "su" indicates a sub-unit within a slot. Other values representing physical hierarchy levels that have not been included in this list but which follow the same basic naming rules will also be allowed;

  - the <unit #> is a decimal number which is used to reference to a particular instance of a <unit-type> at that level of the hierarchy.

- The number of levels and naming of those levels is based on the physical hierarchy within the media gateway, as illustrated by the following examples:

  - a Media Gateway that has some number of DS1 interfaces:

    ds/ds1-#/#

  - a Media Gateway that has some number of OC3 interfaces, that contain channelized DS3 and DS1 hierarchies:

    ds/oc3-#/ds3-#/ds1-#/#

  - a Media Gateway that contains some number of slots with each slot having some number of DS3 interfaces:

    ds/s-#/ds3-#/ds1-#/#

- Some terminations may not contain all possible levels of a hierarchy, however all levels supported by a given termination are contained in the termination naming scheme. For example, a DS3 without DS1 framing could be represented by the following naming scheme:

  ds/s-#/ds3-#/#

  - however, a DS3 *with* DS1 framing could not be represented by that naming scheme.

5.4 Topology descriptor

A Gateway conforming to the present document need not to implement topology. MGCs that expect control gateway conforming to the present document shall not assume that topology is supported.

5.5 Transaction timers

All transaction timers as specified in ITU-T Recommendation H.248 [1] shall be supported here.

5.6 Transport

Media Gateways shall implement UDP/ALF.

Media Gateway Controllers shall implement UDP/ALF.

5.7 Service change procedures

The Media Gateway shall allow one primary and one or more secondary MGCs to be provisioned for registration.

5.8 Security

Media Gateways and Media Gateways Controllers shall implement IPsec (see IETF/RFC 2401 [6]) and shall use IKE (see IETF/RFC 2402 [7]) for key management.

5.9 Encoding

Conforming Media Gateways shall support text encoding.

5.10 Use of SDP

Strict conformance to IETF/RFC 2327 [5] is required. However, trunking gateways may make certain simplifying assumptions about the session description as specified in the following.

SDP usage depends on the type of session, as specified in the "media" parameter. The present document only supports media of type "audio".

The SDP profile provided describes the use of the session description protocol in TGCP. The general description and explanation of the individual parameters can be found in IETF/RFC 2327 [5], however below we detail what values TGCP endpoints need to provide for these fields (send) and what TGCP endpoints should do with values supplied or not supplied for these fields (receive).

Any parameter not specified below should not be provided by any TGCP endpoint, and if such a parameter is received, it should be ignored.

5.10.1 Protocol version (v=)

v= <version>
v= 0

Send: shall be provided in accordance with IETF/RFC 2327 [5] (i.e. v=0).

Receive: shall be provided in accordance with IETF/RFC 2327 [5].

5.10.2 Origin (o=)

The origin field consists (o=) of 6 sub-fields in IETF/RFC 2327 [5]:

o=	*<username>*	*<session-ID>*	*<version>*	*<network-type>*	*<address-type>*	*<address>*
o=	*-*	*2987933615*	*2987933615*	*IN*	*IP4*	*A3C47F2146789F0*

Username:

Send: Hyphen shall be used as username when privacy is requested. Hyphen should be used otherwise.

Receive: This field should be ignored.

Session-ID:

Send: shall be in accordance with IETF/RFC 2327 [5] for interoperability with non-IPCablecom clients.

Receive: This field should be ignored.

Version:

Send: In accordance with IETF/RFC 2327 [5].

Receive: This field should be ignored.

Network Type:

Send: Type "IN" shall be used.

Receive: This field should be ignored.

Address Type:

Send: Type "IP4" shall be used.

Receive: This field should be ignored.

Address:

Send: shall be in accordance with IETF/RFC 2327 [5] for interoperability with non-IPCablecom clients.

Receive: This field shall be ignored.

5.10.3 Session name (s=)

s= <session-name>
s= -

Send: Hyphen shall be used as session name.

Receive: This field shall be ignored.

5.10.4 Session and media information (i=)

i= <session-description>

Send: For TGCP, the field shall not be used.

Receive: This field shall be ignored.

5.10.5 URI (u=)

u= <URI>

Send: For TGCP, the field shall not be used.

Receive: This field shall be ignored.

5.10.6 E-mail address and phone number (e=, p=)

e= <e-mail-address>
p= <phone-number>

Send: For TGCP, the field shall not be used.

Receive: This field shall be ignored.

5.10.7 Connection data (c=)

The connection data consists of 3 sub-fields:

c= <network-type> <address-type> <connection-address>

c= IN IP4 10.10.111.11

Network Type:

Send: Type "IN" shall be used.

Receive: Type "IN" shall be present.

Address Type:

Send: Type "IP4" shall be used.

Receive: Type "IP4" shall be present.

Connection Address:

Send: This field shall be filled with a unicast IP address at which the application will receive the media stream. Thus a TTL value shall not be present and a "number of addresses" value shall not be present. The field shall not be filled with a fully-qualified domain name instead of an IP address. A non-zero address specifies both the send and receive address for the media stream(s) it covers.

Receive: A unicast IP address or a fully qualified domain name shall be present. A non-zero address specifies both the send and receive address for the media stream(s) it covers.

5.10.8 Bandwidth (b=)

b= <modifier>: <bandwidth-value>
b= AS : 64

Send: Bandwidth information is optional in SDP but it should always be included. When an rtpmap or a non well-known codec (i.e. not defined in TS 101 909-3 [3]) is used, the bandwidth information shall be used.

Receive: Bandwidth information should be included. If a bandwidth modifier is not included, the receiver shall assume reasonable default bandwidth values for well-known codecs.

Modifier:

Send: Type "AS" shall be used.

Receive: Type "AS" shall be present.

Bandwidth Value:

Send: The field shall be filled with the maximum bandwidth requirement of the Media stream in kbits/s.

Receive: The maximum bandwidth requirement of the media stream in kbits/s shall be present.

5.10.9 Time, repeat times and time zones (t=, r=, z=)

t= <start-time> <stop-time>
t= 36124033 0
r= <repeat-interval> <active-duration> <list-of-offsets-from-start-time>
z= <adjustment-time> <offset>

Send: Time shall be present; start time may be zero, but should be the current time, and stop time should be zero. Repeat Times, and Time Zones should not be used, if they are used it should be in accordance with IETF/RFC 2327 [5].

Receive: If any of these fields are present, they should be ignored.

5.10.10 Encryption keys

k= <method>
k= <method>: <encryption-keys>

Security services for IPCablecom are defined by the IPCablecom Security TS 101 909-11 [4]. The security services specified for RTP and RTCP do not comply with those of IETF/RFC 1889 [8], IETF/RFC 1890 [11], and IETF/RFC 2327 [5]. In the interest of interoperability with non-IPCablecom devices, the "k" parameter will therefore not be used to convey security parameters.

Send: shall not be used.

Receive: This field should be ignored.

5.10.11 Attributes (a=)

a= <attribute>: <value>
a= rtpmap: <payload type> <encoding name>/<clock rate>
[/<encoding parameters>]
a= rtpmap : 0 PCMU / 8000
a= X-pc-codecs: <alternative 1> <alternative 2> …
a= X-pc-secret: <method>:<encryption key>
a = X-pc-csuites-rtp: <alternative 1> <alternative 2> …
a = X-pc-csuites-rtcp: <alternative 1> <alternative 2> …
a = X-pc-spi-rtcp: <value>
a = X-pc-bridge: <number-ports>

a= <attribute>
a= recvonly
a= sendrecv
a= sendonly
a= ptime

Send: One or more of the "a" attribute lines specified below may be included. An attribute line not specified below should not be used.

Receive: One or more of the "a" attribute lines specified below may be included and shall be acted upon accordingly. "a" attribute lines not specified below may be present but shall be ignored.

rtpmap:

Send: When used, the field shall be used in accordance with IETF/RFC 2327 [5]. It may be used for well-known as well as well as non well-known codecs. The encoding names used are provided in a separate IPCablecom specification (see TS 101 909-3 [3] and TS 101 909-11 [4]).

Receive: The field shall be used in accordance with IETF/RFC 2327 [5].

X-pc-codecs:

Send: The field contains a list of alternative codecs that the endpoint is capable of using for this connection. The list is ordered by decreasing degree of preference, i.e. the most preferred alternative codec is the first one in the list. A codec is encoded similarly to "encoding name" in rtpmap.

Receive: Conveys a list of codecs that the remote endpoint is capable of using for this connection. The codecs shall not be used until signalled through a media (m=) line.

X-pc-secret:

Send: The field contains an end-to-end secret to be used for RTP and RTCP security. The secret is encoded similarly to the encryption key (k=) parameter of IETF/RFC 2327 [5] with the following constraints:

The encryption key shall not contain a ciphersuite, only a passphrase.

The <method> specifying the encoding of the pass-phrase shall be either "clear" or "base64" as defined in IETF/RFC 2045 [14], except for the maximum line length which is not specified here. The method "clear" shall not be used if the secret contains any characters that are prohibited in SDP.

Receive: Conveys the end-to-end secret to be used for RTP and RTCP security.

X-pc-csuites-rtp:
X-pc-csuites-rtcp:

Send: The field contains a list of ciphersuites that the endpoint is capable of using for this connection (respectively RTP and RTCP). The first ciphersuite listed is what the endpoint is currently expecting to use. Any remaining ciphersuites in the list represent alternatives ordered by decreasing degree of preference, i.e. the most preferred alternative ciphersuite is the second one in the list. A ciphersuite is encoded as specified below:

ciphersuite = [AuthenticationAlgorithm] "/" [EncryptionAlgorithm]

AuthenticationAlgorithm = 1*(ALPHA/DIGIT/"-"/"_")

EncryptionAlgorithm = 1*(ALPHA/DIGIT/"-"/"_")

where ALPHA, and DIGIT are defined in IETF/RFC 2234 [10]. Whitespaces are not allowed within a ciphersuite. The following example illustrates the use of ciphersuite:

62/51

The actual list of ciphersuites is provided in the IPCablecom Specification TS 101 909-11 [4].

Receive: Conveys a list of ciphersuites that the remote endpoint is capable of using for this connection. Any other ciphersuite than the first in the list cannot be used until signalled through a new ciphersuite line with the desired ciphersuite listed first.

X-pc-spi-rtcp:

Send: The field contains the IPSEC Security Parameter Index (SPI) to be used when sending RTCP packets to the termination for the media stream in question. The SPI is a 32-bit identifier encoded as a string of up to 8 hex characters. The field shall be supplied when RTCP security is used.

Receive: Conveys the IPSEC SPI to be used when sending RTCP packets over IPSEC. The field shall be present when RTCP security is used.

X-pc-bridge:

Send: TGCP endpoints shall not use this attribute.

Receive: TGCP endpoints shall ignore this attribute if received.

recvonly:

Send: The field shall be used in accordance with IETF/RFC 2543 [9].

Receive: The field shall be used in accordance with IETF/RFC 2543 [9].

sendrecv:

Send: The field shall be used in accordance with IETF/RFC 2543 [9].

Receive: The field shall be used in accordance with IETF/RFC 2543 [9].

sendonly:

Send: The field shall be used in accordance with IETF/RFC 2543 [9], except that the IP address and port number shall not be zeroed.

Receive: The field shall be used in accordance with IETF/RFC 2543 [9].

ptime:

Send: The ptime should always be provided and when used it shall be used in accordance with IETF/RFC 2327 [5]. When an rtpmap or non well-known codec is used, the ptime shall be provided.

Receive: The field shall be used in accordance with IETF/RFC 2327 [5]. When "ptime" is present, the MTA shall use the ptime in the calculation of QoS reservations. If "ptime" is not present, the MTA shall assume reasonable default values for well-known codecs.

5.10.12 Media announcements (m=)

Media Announcements (m=) consists of 3 sub-fields:

M= <media> <port> <transport> <format>
M= audio 3456 RTP/AVP 0

Media:

Send: The "audio" media type shall be used.

Receive: The type received shall be "audio".

Port:

Send: shall be filled in accordance with IETF/RFC 2327 [5]. The port specified is the receive port, regardless of whether the stream is unidirectional or bidirectional. The sending port may be different.

Receive: shall be used in accordance with IETF/RFC 2327 [5]. The port specified is the receive port. The sending port may be different.

Transport:

Send: The transport protocol "RTP/AVP" shall be used.

Receive: The transport protocol shall be "RTP/AVP".

Media Formats:

Send: Appropriate media type as defined in IETF/RFC 2327 [5] shall be used.

Receive: In accordance with IETF/RFC 2327 [5].

5.11 Timestamp

Media Gateways are not required to include timestamps in every notify command.

5.12 Digits maps

Media Gateways are not required to support digit maps.

Annex A (normative): Specific package definitions

A.1 Security package

PackageID: sec (0x000 – to be allocated by IANA).

- Version: 1.
- Extends: none.

This package is used to provide the MG with security related parameters for RTP/RTPC.

A.1.1 Properties

Secret:

- PropertyID: sc-st (0x0001).
- Type: String.
- Possible Value: any.
- Defined in LocalControlDescriptor.
- Characteristics: Read/Write.

RTP Ciphering suite:

- PropertyID: sc-rtp (0x0002).
- Type: String.
- Possible Value: any.
- Defined in LocalControlDescriptor.
- Characteristics: Read/Write.

RTCP Ciphering Suite:

- PropertyID: sc-rtcp (0x0003).
- Type: String.
- Possible Value: any.
- Defined in LocalControlDescriptor.
- Characteristics: Read/Write.

A.1.2 Events

None.

A.1.3 Signals

None.

A.1.4 Statistics

None.

A.1.5 Procedures

- **Secret:** the optional secret is a seed value that shall be used to derive end-to-end encryption keys for the RTP and RTCP security services. The secret should be encoded as clear-text if it only contains values in the ASCII character range 21_H to $7E_H$. Otherwise, the secret shall be encoded using base64 encoding. If no value is supplied, or the parameter is omitted and security services are to be used, the termination shall generate a secret on its own. When a secret is supplied by the MGC, the secret should be used.

- **RTP ciphersuite:** a list of ciphersuites for RTP security in order of preference. The entries in the list are ordered by preference where the first ciphersuite is the preferred choice. The termination shall choose exactly one of the ciphersuites. The termination should additionally indicate which of the remaining ciphersuites it is willing to support as alternatives. Each ciphersuite is represented as ASCII strings consisting of two (possibly empty) substrings separated by a slash ("/"), where the first substring identifies the authentication algorithm, and the second substring identifies the encryption algorithm.

- **RTCP ciphersuite:** a list of ciphersuites for RTCP security in order of preference. The entries in the list are ordered by preference where the first ciphersuite is the preferred choice. The termination shall choose exactly one of the ciphersuites. The termination should additionally indicate which of the remaining ciphersuites it is willing to support as alternatives. Each ciphersuite is represented as ASCII strings consisting of two (possibly empty) substrings separated by a slash ("/"), where the first substring identifies the authentication algorithm, and the second substring identifies the encryption algorithm.

History

Document history		
V1.1.1	March 2002	Publication