International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.812.4

(11/2015)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

E-health multimedia services and applications – Personal health systems

Interoperability design guidelines for personal health systems: WAN interface: Authenticated persistent session device class

Recommendation ITU-T H.812.4

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Telepresence	H.420–H.429
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SERVICES AND APPLICATIONS	
Personal health systems	**H.810–H.819**
Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)	H.820–H.859
Multimedia e-health data exchange services	H.860–H.869

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T H.812.4

Interoperability design guidelines for personal health systems: WAN interface: Authenticated persistent session device class

Summary

The Continua Design Guidelines (CDG) define a framework of underlying standards and criteria that are required to ensure the interoperability of devices and data used for personal connected health. They also contain design guidelines (DGs) that further clarify the underlying standards or specifications by reducing options or by adding missing features to improve interoperability.

This specification defines the additional design guidelines for the Authenticated persistent session CDC (APS), whose function is to provide a secure, long-lived, persistent bidirectional data channel between the WAN application and an AHD application, suitable for sending unsolicited commands to the AHD or to devices connected via the AHD.

Recommendation ITU-T H.812.4 is part of the "ITU-T H.810 interoperability design guidelines for personal health systems" subseries, which is outlined in the table below:

Mapping of CDG 2013, ITU-T H.810 and restructured ITU-T H.810-series

Part	Elements	Clauses in the 2013 CDG "Endorphin"	Clauses in ITU-T H.810 (2013)	Restructured H.810-series (2015)
Part 0	System overview	Up to clause 3, plus Annex A and Appendix G	Up to clause 6, plus Annex A and Appendix V	ITU-T H.810 – System overview
Part 1	TAN/PAN/ LAN	Clauses 4 to 7, Appendices C, D, M	Clauses 7 to 10, Appendices I, II, XI	ITU-T H.811 – TAN-PAN-LAN interface
Part 2	WAN	Clause 8, Appendices H, I, J, K	Clause 11; Appendices VI, VII, VIII, IX	ITU-T H.812 – WAN interface ITU-T H.812.1 – Observation upload ITU-T H.812.2 – Questionnaires ITU-T H.812.3 – Capability exchange ITU-T H.812.4 – Authenticated persistent session
Part 3	HRN	Clause 9, Appendices E, F, L	Clause 12, Appendices III, IV, X	H.813 – HRN interface

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.812.4	2015-11-29	16	11.1002/1000/12657

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

© ITU 2016

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Page

List of Tables

Page

List of Figures

Page

0 Introduction

The Continua Design Guidelines (CDG) define a framework of underlying standards and criteria that are required to ensure the interoperability of devices and data used for personal connected health. They also contain additional design guidelines that further clarify the underlying standards or specifications by reducing options or by adding missing features to improve interoperability.

This specification defines the additional design guidelines for the Authenticated persistent session CDC (APS), whose function is to provide a secure, long-lived, persistent bidirectional data channel between the WAN application and an AHD application, suitable for sending unsolicited commands to the AHD or to devices connected via the AHD.

This Recommendation is part of the ITU-T H.810 sub-series "ITU-T H.810 Interoperability design guidelines for personal health systems". See [ITU-T H.810] for more details.

0.1 Organization

This Recommendation is organized in the following manner.

Clauses 0 to 5: Introduction and terminology – These clauses provide an overview of how this Recommendation is structured.

Clause 6: Use cases – A descriptive scenario that motivates the class of problems that the APS is addressing.

Clause 7: Authenticated persistent session overview – A technical overview of the operation of the authenticated persistent session.

Clause 8: Authenticate persistent session management – This clause describes the interactions between the information exchange parties.

Clause 9: Behavioural model: MQTT – This clause is an overview of sequences of interactions under this CDC and summarizes typical iterations, constraints and exceptions.

Clause 10: Behavioural Model: SMS shoulder tap capability.

Annex A: The guidelines that document the normative elements for the authenticated persistent session are presented in a tabular format in this annex. The annex references other locations with normative content.

Annex B: root file for an authenticated persistent session.

Appendix I: APS details.

Appendix II: APB resource schema.

0.2 CDC guideline releases and versioning

See clause 0.2 of [ITU-T H.810] for release and versioning information.

0.3 What's new

To see what is new in this release of the design guidelines, refer to clause 0.3 of [ITU-T H.810].

Recommendation ITU-T H.812.4

Interoperability design guidelines for personal health systems: WAN interface: Authenticated persistent session device class

1 Scope

This Recommendation defines two certified device classes. Both certified device classes contain guidelines that document a secure mechanism by which a WAN application can initiate communications with an application residing within a transient piece of customer premises equipment known as an application hosting device (AHD). The two certified device classes are for the WAN application (APS-CDC-WAN) and for the AHD (APS-CDC-AHD).

The mechanism addresses: (1) the establishment and management of a persistent long term session between the WAN-Application and the AHD application, (2) the use of the MQTT protocol for message exchange and (3) the use of short message service (SMS) to re-establish IP level connectivity with transient AHDs that have a cellular interface.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T H.810] Recommendation ITU-T H.810 (2015), *Interoperability design guidelines for personal health systems*.

All other referenced documents can be found in clause 2 of [ITU-T H.810].

3 Definitions

This Recommendation uses terms defined in [ITU-T H.810].

4 Abbreviations and acronyms

This Recommendation uses abbreviations and acronyms defined in [ITU-T H.810].

5 Conventions

This Recommendation follows the conventions defined in [ITU-T H.810].

6 Authenticated persistent session use case

The authenticated persistent session provides a mechanism by which future Continua certified device classes can initiate communications from cloud based services to the AHD.

7 Authenticated persistent session (APS) overview

The Authenticated persistent session certified device class defines a long lived, persistent context for exchanging messages between a WAN application and an AHD application. The context is persistent in that it maintains an operational state across TCP connections, pausing when the underlying TCP connection is lost, and resuming when it is re-established. The session is long lived in that applications maintain the session for whatever time duration is required. Long lived persistent sessions support applications that send occasional messages requiring a timely response.

NOTE 1 – These guidelines define an Authenticated persistent session certified device class for an AHD application (APS-CDC-AHD) and for a WAN application (APS-CDC-WAN). The notation APS-CDC is used as a shorthand when it is not necessary to disambiguate between the actual WAN and AHD CDCs.

The APS-CDC is optimized for sending messages over networks where bandwidth, power and IP resources are limited. The optimization is obtained by eliminating AHD application based polling. The APS-CDC defines an optional wake up capability based on the short message service (SMS) for use when the AHD has cellular network connectivity. This capability allows the WAN application to wake up an AHD application that no longer has IP connectivity due to the cellular network reallocating inactive resources. Implementations that support SMS may be able to take advantage of this optional capability in order to minimize their network utilization.

The term *authenticated persistent session* (APS) describes the concept of the persistent session as defined in this document. A related term, *authenticated persistent binding* (APB) is used to describe the information resource exchanged during persistent session establishment. We qualify *persistent session* and *persistent binding* with *authenticated* to emphasize a relationship that the WAN application creates between the APB resource and an AHD application security credential in order to ensure proper authentication when the AHD application resumes a persistent session.

Figure 7-1 depicts the framework of the APS.

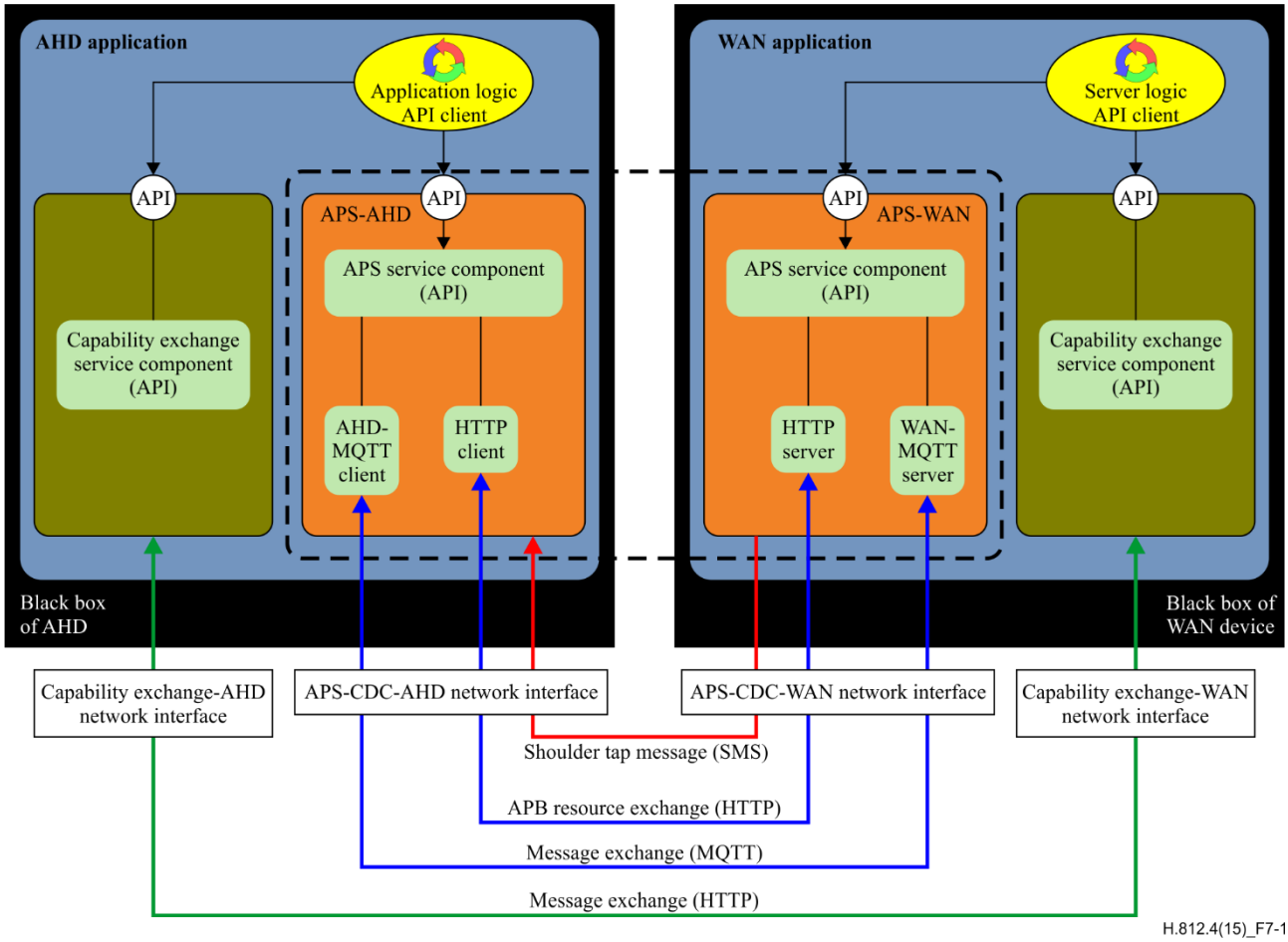

Figure 7-1 – APS Framework

An authenticated persistent session (APS) is a binding between two *APS service components*, one in the *WAN application* and one in *the AHD application*, which enables the *API clients* to behave as if there is an always connected pipe between them. In Figure 7-1 the *APS API service components* are the peer entities that implement these guidelines in order to deliver the persistent session service to their *API clients*. The *WAN application* using the APS *API client* component (see [ITU-T H.810]

Devices Components and Interfaces) can securely issue commands to the AHD application, across service disruptions, without needing to manage the connectivity or authenticity of the peer.

NOTE 2 – Figure 7-1 represents an architectural model and does not mandate a particular implementation.

NOTE 3 – The existence of an APS between two components does not mean that messages can be exchanged between the components at a given point in time. Message delivery is only possible when there is connectivity at the transport layer.

The APB resource that defines the APS is based on exchanged security credentials using a given source of authentication information. Any entity that provides the appropriate authentication information may gain access to the APS and continue the persistent session.

NOTE 4 – It is possible for an APS to move from one physical device to a different physical device as long as the AHD implementation presents the same credentials. Therefore a WAN application should not assume that an APS represents a connection to a particular AHD hardware platform; the APS is bound to a security credential such as an ITU-T X.509 certificate, an OAuth token or an SAML token.

There are three steps involved in creating and exchanging a message using an APS. Once the APS is in place only the final step is needed to send additional messages. The three steps, in order are:

– Capability exchange (see [ITU-T H.812.3]) – In this phase the AHD application obtains information from the WAN application using HTTP. The information identifies if the WAN application has support for APS-CDC-WAN. The information is contained in the root.xml file of the WAN application and includes the URL to use for APS establishment. See clause 8.1.

– APS establishment (see clauses 8.2.3 and 8.2.4 – The AHD application, using a secure HTTPS connection, creates the APB resource on the WAN application indicating its desire to establish a persistent session. During this phase the AHD application authenticates itself to the WAN application and is provided with APB resource information. When this phase completes the AHD has either established the APS and is ready to exchange messages with the WAN application, or has terminated the APS establishment process causing the APB resource to be removed. See clause 8.2.3.

– Message exchange using MQTT (see clause 9 – In this phase a TLS connection is established by the AHD application connecting it to the MQTT server exposed by the WAN application. This connection is used for the normal exchange of messages. In an APS the management information is contained in the APB resource, which is manipulated using RESTful operations over HTTPS. The data flow associated with the operation of the APS is carried in messages flowing over the MQTT connection. Once an APS has been created there is typically no additional management activity, so all activity is over MQTT.

7.1 Support for multiple CDCs

An AHD application in the future may contain multiple CDCs (or vendor-specific components) that make use of the APS. An example of this might be a CDC for remote AHD configuration. These CDCs will have message handlers to process the received messages. Each message that is transmitted from the WAN application is addressed to one of these message handlers via the topic name used in the MQTT PUBLISH command. It is the responsibility of the APS implementer to ensure that messages received by the AHD application are dispatched to the correct message handler.

NOTE 1 – The dispatcher does not use any information in the MQTT payload. The payload is opaque to the dispatcher.

Figure 7-2 gives an example of delivering the payload in an MQTT message to different message handlers. There are two message handlers in this example: 1) the APS management message handler which supports the ECHO message; 2) an undefined future CDCs or vendor-specific message handler. The MQTT message is received by the Network-IF component which forwards it to the dispatcher. The dispatcher extracts the MQTT header. The MQTT header contains the topic

name which identifies the message handler to which the payload needs to be delivered. The topic name is a string that uniquely identifies the CDC that is expected to process the message.

NOTE 2 – This description is illustrative and does not proscribe a particular method of implementation.

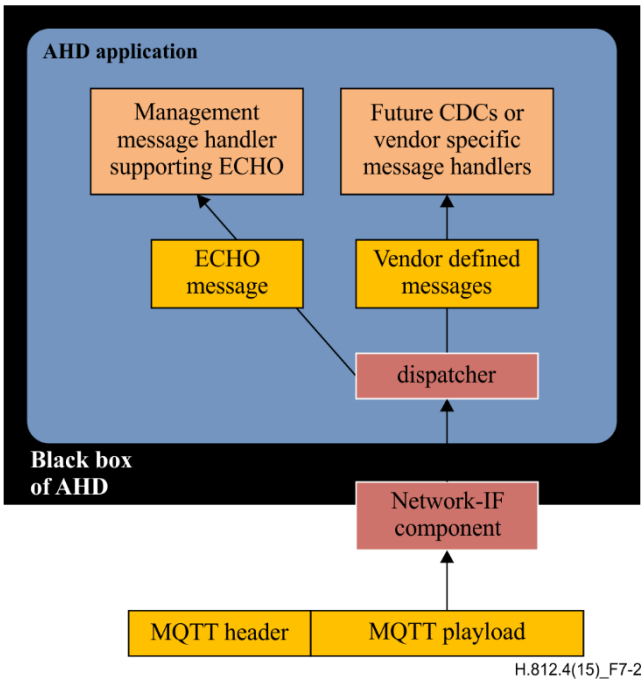

Figure 7-2 – Example of payload delivery to different message handlers

7.2 Topics used in MQTT

Continua compliant entities implementing the APS-CDC **shall** support the use of the MQTT protocol to publish and subscribe to messages. The MQTT protocol uses a topic-based addressing mechanism, and this standard specifies three kinds of topics to be used by an APS. They are shown in Table 7-1.

Table 7-1 – Topics used in MQTT

Name used in this document	Format of the topic string used in MQTT	Description
Message topics	`pcha/message/<WAN APBI>/<AHD APBI>/<mh>`	Topics used to transmit messages to the APS API client components in the AHD application.
Status topic	`pcha/status/<WAN APBI>/<AHD APBI>`	Topic used to track status of the APS
Response topics	`pcha/response/<WAN APBI>/<AHD APBI>/<mh>`	Topic used to receive responses from the AHD application

Each APS is identified by a pair of APB identifiers (APBIs) in the corresponding APB resource, and these APBIs **shall** be inserted in the topic strings in place of the characters <AHD APBI> and <WAN APBI>. See clause 8.2.2 for more details on the APBIs. The <mh> **shall** be replaced by an identifier specified by the CDC that is using the APS exchange mechanism. The identifier allows different CDC peers to exchange messages in the context of a single APS. An example of a message topic for an APS might appear as follows:

pcha/message/1/34521ee41da2eff/APS

The MQTT server **shall** control access to these topics using the following rules:

– A WAN application **shall** have write access to any message topics containing its WAN APBI.

– A WAN application **shall** have read access to the status and response topics containing its WAN APBI.

– An AHD **shall** have read access to any message topics containing its AHD APBI.

– An AHD **shall** have write access to any status topics containing its AHD APBI.

– An AHD **shall** have write access to any response topics containing its AHD APBI.

– Suitably authenticated management applications MAY have read access to any topic.

– All other access **shall** NOT be permitted.

In general the above requirements are stating that an APS-CDC shall only have access to topics defined for that APS-CDC. A similar relationship holds, in theory, between the WAN application and MQTT server, but how the WAN application and MQTT server actually interact is implementation dependent. In many implementations the WAN application is also the authenticated management application.

7.3 Shoulder tap

If the WAN application needs to send a message to the AHD application and the AHD application is no longer connected to the MQTT server, the WAN application can use one of the shoulder tap methods supported by the AHD application to alert it that a message is waiting. The AHD application, upon reception of the shoulder tap, reconnects to the MQTT server. The AHD is then able to receive messages from the WAN application. Currently the only defined shoulder tap method is Binary SMS messaging.

8 APS management

An authenticated persistent session (APS) is a long term association between two mutually authenticated peer entities, one associated with the WAN application and the other with the AHD application. Authentication is performed using TLS in conjunction with OAUTH as outlined in Annex B of [ITU-T H.812].

The WAN application, after it has successfully authenticated the AHD application allocates a resource called the authenticated persistent binding (APB). The APB contains a set of attributes that both define the APS and provide the basis for its management. It is the responsibility of the WAN application to ensure that for a given OAUTH bearer token: (1) the same APB **shall** be returned on repeated requests for the APS resource, and that (2) if a different OAUTH bearer token is provided a different APS resource (or an error) **shall** be returned.

The APB resource is an XML document with a set of elements as defined in Tables 8-4 and 8-5. The management of APB resources is covered in this clause.

The WAN application implementing the APS-CDC uses hData to present to the AHD application three items relating to APSes in the root.xml file. The first item is a *profile*. The profile is an entry that indicates that the WAN application supports the APS-CDC. The second item, *resourceType*, describes the content of the APB resource and contains a reference to an XML schema that can be used to validate it. The third item, *section*, is an entry that indicates to the AHD application where to POST its contribution to the APB resource when first establishing the APS.

The initial content of the APB resource is jointly established by the AHD and WAN applications. The AHD application provides an APB resource structured in accordance with the XML schema identified in the *resourceType* element of the root.xml file. The AHD application provides values for a subset of the APB elements as identified in Table 8-1. The WAN application when it receives the APB resource from the AHD application fills in the remaining elements as defined in Table 8-2.

During the establishment of an APS, a pair of identifiers is allocated by the WAN application. These identifiers are part of the APB resource. One identifier in the pair is associated with the AHD application (AHD APBI) and the other identifier is associated with the WAN application (WAN APBI). The WAN APBI together with the AHD APBI identify the APB instance and **shall** be unique across all the APS being managed by the WAN application.

8.1 APB resources

The APS-CDC-WAN defines a management interface that uses HTTPS and hData. These mechanisms prescribe a RESTful and secure access mechanism to information defining the APS, which is contained in the APB resource. The starting point for the hData layout of this interface is the root.xml file. For a WAN application implementing the APS-CDC-WAN the root.xml file **shall** contain the entries as specified in Figure 8-1, Figure 8-2 and Figure 8-3.

```
<profile>
 <!-- Specified value -->
 <id>APS-CDC-WAN</id>
 <reference>
  http:// handle.itu.int/11.1002/3000/hData/APS/2015/01/H.812.4.pdf
 </reference>
</profile>
```

Figure 8-1 – Profile element indicating capability

The entry in Figure 8-1 indicates to the AHD application that the WAN application supports the APS message transfer infrastructure (APS-CDC-WAN). This entry **Shall** appear exactly as shown in Figure 8-1.

```
<resourceType>
 <resourceTypeID>APB</resourceTypeID>
 <!-- location of reference that describes the APS standard -->
 <reference>
  http://handle.itu.int/11.1002/3000/hData/APS/2015/01/H.812.4.pdf
 </reference>
 <representation>
  <mediaType>application/xml</mediaType>
  <!-- Schema for the APB resource xml -->
  <validator>
   http://handle.itu.int/11.1002/3000/hData/APS/2015/01/APBConfigResource.xsd
  </validator>
 </representation>
<resourceType>
```

Figure 8-2 – ResourceType element describing APB content

The entry in Figure 8-2 provides a description and the structure (such as a schema) of the APB. The entry **Shall** appear exactly as shown in Figure 8-2.

```
<section>
 <!-- chosen by the WAN application -->
 <path>path/to/post/folder</path>
 <profileID>APS-CDC-WAN</profileID>
 <!-- required in this specification; optional but recommended in hData; -->
 <resourcePrefix>true</resourcePrefix>
 <resourceTypeID>APB</resourceTypeID>
</section>
```

Figure 8-3 – Section element describing where to POST

The entry in Figure 8-3 identifies a URL to which the AHD application performs the initial POST in the APS establishment. The <profileID> element value **shall** be that of the <id> element value in the <profile> element and the <resourceTypeID> value **shall** be APB. The <resourcePrefix> element **shall** be present in this specification and it **shall** be set to true (it is optional in the hData specification). The <path> element **shall** be present but the URL value is determined by the application.

Table 8-1 and Table 8-2 describe the contents of the APB resource that characterize the APS.

The APB resource is expressed as anXMLdocument, an example of which follows. The example in Figure 8-4 shows an AHD application supporting MQTT and an SMS shoulder tap.

See Appendix II for the APB resource schema.

Table 8-1 – APBXMLelements provided by AHD application

Element	Usage
supportedMH	Mandatory – A space-separated list identifying the message handlers that are supported by the AHD application. All AHD applications that support APS message transfer Shall support the APS diagnostic handler as denoted below. – The three uppercase characters "APS" This value Shall be ignored by the AHD application whenever the APB resource is obtained from the WAN application. NOTE – If a vendor-specific message handler is used, the identifying string should have properties that minimize the potential for a collision with another uncoordinated vendor message handler.
exchangeMechanism	Mandatory – A space-separated list identifying the underlying technologies that are being used by the AHD application to support message exchanges. The AHD application Shall identify each technology that it supports in an ordered list with the first entry in the list being its preferred choice. The only currently supported exchange mechanism is MQTT. This value Shall be ignored by the AHD application whenever the APB resource is obtained from the WAN application.
shoulderTapMechanism	Mandatory – A space-separated list identifying the underlying technologies that the AHD application uses to accept a shoulder tap. The shoulder tap enables the WAN application to re-establish a TCP connection with the AHD application in the event that the resources used to maintain that connection have been removed. The AHD application identifies each technology that it supports in an ordered list with the first entry in the list being its preferred choice. The WAN application Shall select the first technology that it supports from the list. If the AHD application does not

Table 8-1 – APBXMLelements provided by AHD application

Element	Usage
	support a shoulder tap it Shall provide an empty list. SMS is currently the only defined mechanism for performing a shoulder tap. This value Shall be ignored by the AHD application whenever the APB resource is obtained from the WAN application.
SMS	Conditionally required – This element Shall be present if a shoulder tap mechanism of SMS is selected. The SMS element contains the information that the WAN application will use in order to perform the shoulder tap operation. The SMS element is the parent element for SMSHeaderDstPort, SMSApplicatonId and MSISDN. This value Shall be ignored by the AHD application whenever the APB resource is obtained from the WAN application.
MSISDN	Mandatory SMS Child – The MSISDN is the SMS number used to reach the AHD application (the AHD application's 'phone number'). It Shall be composed of the numeric digits [0-9] with an optional leading "+". The total string Shall be 15 characters of less. This value Shall be ignored by the AHD application whenever the APB resource is obtained from the WAN application.
SMSHeaderDstPort	Mandatory SMS Child – The SMSHeaderDstPort gives the value to be used as the 16-bit destination port in the SMS user data header (UDH information element identifier value of 0x05). See clause 9.3.1 for additional information. The information Shall be represented in this element as a decimal number. This value Shall be ignored by the AHD application whenever the APB resource is obtained from the WAN application.
SMSApplicationId	Optional SMS Child – The SMSApplicationID Shall be a sequence of Unicode characters. The length of this string, when encoded using UTF8, Shall not exceed 148 octets. This string Shall be sent in the payload of a shoulder tap. The purpose of the element is to provide an application identifier in the shoulder tap which can be used to route the shoulder tap message to the appropriate AHD application The exact semantics associated with how this routing takes place on a given AHD platform is not defined by these guidelines. If the APS is being formed by an application on a platform in which other applications may create APSes the value of SMSApplicationId may need to be managed. This value Shall be ignored by the AHD application whenever the APB resource is obtained from the WAN application.
APSState	See description of the element in Table 8-2

Table 8-2 – APBXMLelements provided by WAN application

Element	Usage
WANAPBI	Mandatory – The identifier for the WAN component of the authenticated persistent binding resource that was created. The WANAPBI Shall be represented as a string of size less than 2048 UTF-8 characters. The following characters Shall not be present in the string: "/", "#", "+", "*". The Unicode NULL character may not be used. This value Shall be ignored by the WAN application whenever the APB resource is obtained from the AHD application.
AHDAPBI	Mandatory – The identifier for the AHD application component of the authenticated persistent binding resource that was created. The AHDAPBI Shall be represented as a string of size less than 2048 UTF-8 characters. The following characters Shall not be present in the string: "/", "#", "+", "*". The Unicode NULL character may not be used. This value Shall be ignored by the WAN application whenever the APB resource is obtained from the AHD application.
APSExchangeURL	Mandatory – The URL to use when establishing the TLS session on which MQTT messages will be exchanged. The URI scheme Shall be mqtts. The AHD application may need to change the URI scheme to work with a given MQTT client. This value Shall be ignored by the WAN application whenever the APB resource is obtained from the AHD application.
APSState	Mandatory – The state of the APS. The WAN application Shall set this element to NEW in response to an AHD application POST operation if the APS does not exist. If the WAN application already has an existing APS in place with the AHD application, as determined by the authentication of the security credential, this value Shall be set to ENABLED. The AHD Shall set this value to TERMINATED to close and remove the persistent session with the WAN application. The WAN application Shall support a valid XPath representation of the APSState element of the APS when setting the value of APSState.
expirationTime	Mandatory – The maximum time period that may elapse after the last POST to the APB resource by the AHD application, or the last activity on the message channel in which the peer AHD application was known to be active. If this time period is exceeded the WAN application Should terminate the APS. However, if the APB resource is in the ENABLED state the WAN application Shall attempt to issue the ECHO management message before terminating the APS. The WAN application Should not terminate the APS if a response is received to the ECHO message. (Note that the WAN application may terminate an APS at any time though that action may not represent graceful behaviour.). This element Shall be expressed as an ISO8601 duration – for example a 12 hour expirationTime is represented as PT12H.
requiredResponseTime	Mandatory – The maximum delay in seconds that the WAN application can tolerate for a response to the ECHO message. This value provides the AHD application with information that it can use to determine how to best allocate APS resources. An AHD application Should Not establish an APS with a WAN application if it is unable or unwilling to meet, in normal operation, the requiredResponseTime for an ECHO message. This element Shall be expressed as an ISO8601 duration – for example a 10 second requiredResponseTime is represented as PT10S. This value Shall be ignored by the WAN application whenever the APB resource is obtained from the AHD application.

Table 8-2 – APBXMLelements provided by WAN application

Element	Usage
clientId	Conditionally required – This element Shall be present if an exchangeMechanism of MQTT is selected. The clientId Shall be used by the AHD application when it issues an MQTT CONNECT. The value of the clientId is generated by the WAN application. This value Shall be ignored by the WAN application whenever the APB resource is obtained from the AHD application.
AHDCredential	Conditionally required – This element Shall be present if an exchangeMechanism of MQTT is selected. The AHDCredential Shall be used by the AHD application as the password when it issues a MQTT CONNECT. This value Shall be ignored by the WAN application whenever the APB resource is obtained from the AHD application.

```
<?xml version="1.0" encoding="UTF-8"?>
 <aps:APB xmlns:aps="http://handle.itu.int/11.1002/3000/hData/APS"
     xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation = "
http://handle.itu.int/11.1002/3000/hData/APS/2015/01/APBConfigResource.xsd">

 <!-- These fields are filled in by the AHD -->
 <supportedMH>APS lampreynetworks.com/private</supportedMH>
 <exchangeMechanism>MQTT privateMessageProtocol</exchangeMechanism>
 <shoulderTapMechanism>SMS</shoulderTapMechanism>
 <SMS>
   <MSISDN>441111223344</MSISDN>
   <SMSHeaderDstPort>1234</SMSHeaderDstPort>
   <SMSApplicationId>4827351</SMSApplicationId>
 </SMS>

 <!-- These fields are filled in by the WAN application -->
 <WANAPBI>WANAPBI_1</WANAPBI>
 <AHDAPBI>5468233453aae3fd224</AHDAPBI>
 <APSExchangeURL>mqtts://example.org:1883</APSExchangeURL>

 <!-- State set by WAN application when first created -->

 <APSState>NEW</APSState>
 <expirationTime>PT50H</expirationTime> <!-- Time in hours -->
 <requiredResponseTime>PT30S</requiredResponseTime>  <!-- Time in seconds -->
 <clientId>RestAHD</clientId>
 <AHDCredential>AHDCredential55555</AHDCredential>
</aps:APB>
```

Figure 8-4 – Example of AHD application supporting MQTT and an SMS shoulder tap

8.2 APS behaviour

8.2.1 APS session state

An APS is in one of three states: NEW, ENABLED or TERMINATED. A WAN application **shall** only issue messages to an AHD application when the state of the APS is ENABLED. An APS is in the NEW state when it is first created during the APS establishment procedure. Once the AHD

application agrees to establish the APS the AHD application moves the APS into the ENABLED state where it remains until either the AHD application or WAN device terminates it. See Table 8-2 for additional information on the APSState element in the APB resource.

8.2.2 Authenticate persistent binding identifiers (APBI)

During the establishment of an APS between an AHD application and a WAN application, the WAN application allocates and maintains a pair of identifiers for the life of the APS. One identifier in the pair is associated with an APS instance on the AHD application (AHD APBI) and the other identifier is associated with the APS instance in the WAN application (WAN APBI). The pair of identifiers is used to bind the sending and receiving APS endpoints together. It is the responsibility of the WAN application to manage the allocation of both the WAN APBI and the AHD API so that every distinct APS that is created by the WAN application can be uniquely identified by the pair of APBIs alone. Furthermore, the WAN application must assure that this unique APB resource is only exchanged with an AHD application possessing the security credential (e.g. ITU-T X.509 certificate) that was used when the APS was first created. The AHD APBI must be unique across the full set of existing APSes maintained by the WAN application.

8.2.3 Authenticated persistent binding establishment

APS establishment refers to the process by which the AHD application and WAN application exchange information in order to enable and configure the APS. An APS must be established before messages can be exchanged. The AHD initiates APS establishment after it completes capability exchange with a WAN application and determines that the WAN application supports the APS CDC.

APS establishment requires that the AHD application authenticate itself to the WAN application (acting as an OAUTH Authorization server) using some method that results in the AHD obtaining an authorized OAUTH bearer token. A successfully authenticated TLS connection in which the AHD application possesses a valid OAUTH access token represents mutual authentication for the purposes of an APS.

When there has been mutual authentication the WAN application has the required security credentials it needs in order to identify and associate an APS with a given AHD application, in this and all subsequent transactions. How the WAN application uses the certificate to link the APS to an AHD application is up to the implementation.

Within this mutually authenticated context, the AHD application establishes the APS by performing an HTTP POST to the WAN application. The resource posted is anXMLdocument containing the APB resource but the AHD application fills in only those elements as specified in Table 8-1.

The element values provide the WAN application with the information it needs to configure and allocate the internal resources needed to support the APS. The reply to this POST contains a URL to a modified version of the APB resource containing the WAN provided elements of Table 8-2. The AHD application then retrieves the APB resource via an HTTP GET to the provided URL. The WAN application may refuse to establish an APS due to resource limitations.

8.2.4 Accepting an authenticated persistent binding

The AHD application examines the response of the GET. If the parameters are acceptable to the AHD application, it establishes a secured connection to the MQTT server and sets up the MQTT link performing the necessary subscription and publishing actions. Upon successful completion of these steps, the AHD application **shall** indicate that it accepts the APS by performing an HTTP PUT to the WAN application, using the URL provided in the POST response with APSState appended to it (URL/APSState). The value of the APSState element identified by the URL in the PUT operations **shall** be set to ENABLED. See clause I.4 for details. At this point the APS is enabled and the AHD application can receive messages. The WAN application **shall** only update

the APSState of its APB resource in this transaction. Should the AHD application provide an XPath that references something other than <APSState> the WAN application **shall** return an appropriate HTTP error. An AHD application may perform additional PUT operations to update the APSState of the APS as needed.

8.2.5 Authenticated persistent binding termination

An AHD application may terminate the APS at any time by setting the APSState value to TERMINATED (see Appendix I.5). The AHD application should then perform appropriate operations to release resources used in association with the APS, including clearing the MQTT server (see clause 9.1.1). The APBI is no longer valid after the AHD application terminates the APS. The WAN application may terminate the APS session if the AHD application has failed to renew the APS within the specified expirationTime interval, or due to a decision by the application logic. The WAN application does not remove the APS session due to a termination of a transport connection.

The WAN application removes information that associated the APS with the authentication key so that if the AHD application initiated another APS capability exchange with the same authentication credential, the WAN application would return NEW for the APSState element value in the APB resource. The WAN application can release resources associated with a terminated APS. Terminating an APS is an abortive process that may cause a currently in operation command to fail.

An APS can be terminated by administrative procedures.

8.2.6 APS-CDC diagnostic message

The APS-CDC provides the basic framework by which application oriented CDCs can initiate message exchange from the WAN application. These application oriented CDCs are expected to have well defined operations that are specific to the application's needs. These operations are out of scope for the APS-CDC

The APS-CDC does define a message structure in order to support managing the APS-CDC itself. Only one command is defined for supporting the APS-CDC, the ECHO command. In future releases, other commands may be added. All entities implementing the APS-CDC **shall** support the management message ECHO command.

8.2.6.1 Diagnostic message structure for the APS-CDC message exchange

8.2.6.1.1 Payload

The APS-CDC message exchange facility (MQTT) supports a diagnostic message format that defines a small set of commands that can be exchanged between APS-CDC peer entities. These commands are carried in the payload section of the diagnostic message. A diagnostic message Shall contain only one command. The content of the payload depends upon the command. The diagnostic message Shall be sent in Network Byte Order and has the layout in Table 8-3.

Table 8-3 – Fields of the APS-CDC diagnostic message

Field name	Description	Size in bits	Values
Operation Octet 0	Identifies the operation to be performed. The two MSB bits in the operation field are reserved and Shall be sent as 0 and ignored on reception. Responses to commands Shall be formed by performing a logical OR of the command with 0x40. Thus a command of 0x03 causes a value of 0x43 to be returned in the operation field.	8	0x00 – 0x3F: command 0x40 – 0x7F: response 0x80 – 0xFF: reserved
Handle Octet 1-4	A handle Shall be provided by the sender of the command and returned by the receiver. The handle is opaque to the receiver of the command. The sender Shall not reuse a handle that is associated with an outstanding command.	32	
Status Octet 5	The status field Shall be present in both command and response messages. In commands it Shall be set to 0x00 by the sender, and ignored by the receiver. If the status field is not 0x00 in a response message the sender Should not process the rest of the message.	8	The validity of fields after the status field may not be reliable when the status field is not 0x00.
Length Octet 6-7	The payload length Shall be present in all diagnostic messages. The length field Shall be given in octets and represents the number of octets in the message payload from the first octet after the length field through the last octet of the message payload.	16	Since the payload field includes the 21 octets used to represent time the minimum value of length is 21.
Payload	The payload Shall start with a fixed length subfield of 21 octets. This subfield holds the current value of time as being reported by the sender or responder to the command. The payload May contain additional octets of echo data. The sender of the ECHO command Shall ensure that the length field properly identifies the number of octets of ECHO data. The time subfield Shall be encoded as a string of UTF-8 characters and formatted in accordance with [ITU-T H.812.1] clause D.1.5, Timestamping and time synchronization. Since the timestamp is reported in a fixed length field the fractions of a	Depends upon the command. Specified in the length field	If a receiver is able to detect a mismatch between the number of octets of data in the message and the length of the payload is should return an appropriate error code

Table 8-3 – Fields of the APS-CDC diagnostic message

Field name	Description	Size in bits	Values
	second component is NULL padded for each level of accuracy not reported in the timestamp.		
NOTE – The term payload can be confusing since it is used in several contexts in this document. The diagnostic message itself is the payload of an MQTT message. The payload here refers to the set of bytes that are associated with a given command instruction. For example, the payload of an ECHO command diagnostic message is a timestamp followed by an arbitrary string of bytes that is returned by the recipient.			

8.2.6.1.2 Supported diagnostic message commands

All diagnostic messages defined by these design guidelines have associated responses. The responding entity Shall form a reply to a command by structuring the fields as documented in Table 8-3. The commands supported are identified below:

ECHO

(Operation Field value of 0x01 for command and 0x41 for response)

The ECHO command enables the WAN application to determine if the AHD application is able to receive and respond to diagnostic messages and allows the WAN application to obtain the AHD application's sense of time.

The entity sending the ECHO command Shall provide a payload in which the first 21 bytes contain the time of the sender as defined above in Table 8-3. The remaining bytes, if any, may be set to any value of interest to the sender. The length field is set to the length of the ECHO payload.

The responder to the ECHO command Shall set the operation field to 0x81.

The ECHO response Shall contain the handle provided by the WAN application from the corresponding ECHO command, the status field, the length field and the payload received from the ECHO command with the time field replaced by the time of the ECHO responder using the same format as defined for the sender. The ECHO response Should be sent in an expeditious manner. The responder to the ECHO message Shall examine the length field to determine if the sent value exceeds the implementation defined limit. If it does, it Shall set the status code appropriately, and return the local time and the maximum number of additional bytes supported by the implementation. The payload length field Shall reflect the number of bytes in the returned payload. If the implementation can support the number of bytes sent in the ECHO command it Shall return the sent payload. All implementations Shall support ECHO payloads that are less than or equal to 256 bytes.

8.2.6.1.3 Status field

The status field is composed of a bit indicating valid time and a status code. The most significant bit in the status field is the time synchronized bit. It Shall be set to indicate that valid NTP synchronized time, or equivalent, is being reported in the time field of the payload, and Shall be cleared otherwise.

The following status codes values are defined for the ECHO response

– 0x0000 – Success – No error was detected in processing the command

– 0x0001 – Unknown Failure – The requested command was not successfully performed. The length field may be set to a positive value. When the length field is a positive value the payload contains a message of length bytes that may provide additional insight as to the error encountered.

– 0x0002 – Command not supported. The responding entity Shall return this value whenever the value in the operation field (byte 0) of a received diagnostic message is not supported.

– 0x0003 – Length of command exceeds maximum supported value

– 0x0004 – Error in field values

9 Behavioural model: MQTT

MQTT [OASIS MQTT] is a required capability for applications that support the APS-CDC. This clause describes the usage of MQTT in supporting the transmission of messages in the context of an APS.

9.1 Overview of operation

The WAN application for APSes implements an MQTT server. The hostname or IP address and TCP port number of the server is provided in the APB resource. The exchange of messages between the AHD application and the WAN application uses an MQTT server that is associated with the WAN application, using the topics defined in clause 7.2. The following figure provides an overview of the exchanges between the AHD application and the WAN application. The topic strings, as shown in the figure, are dependent on the AHD APBI, the WAN APBI, and the message handlers used by different CDCs as described in the following clause.

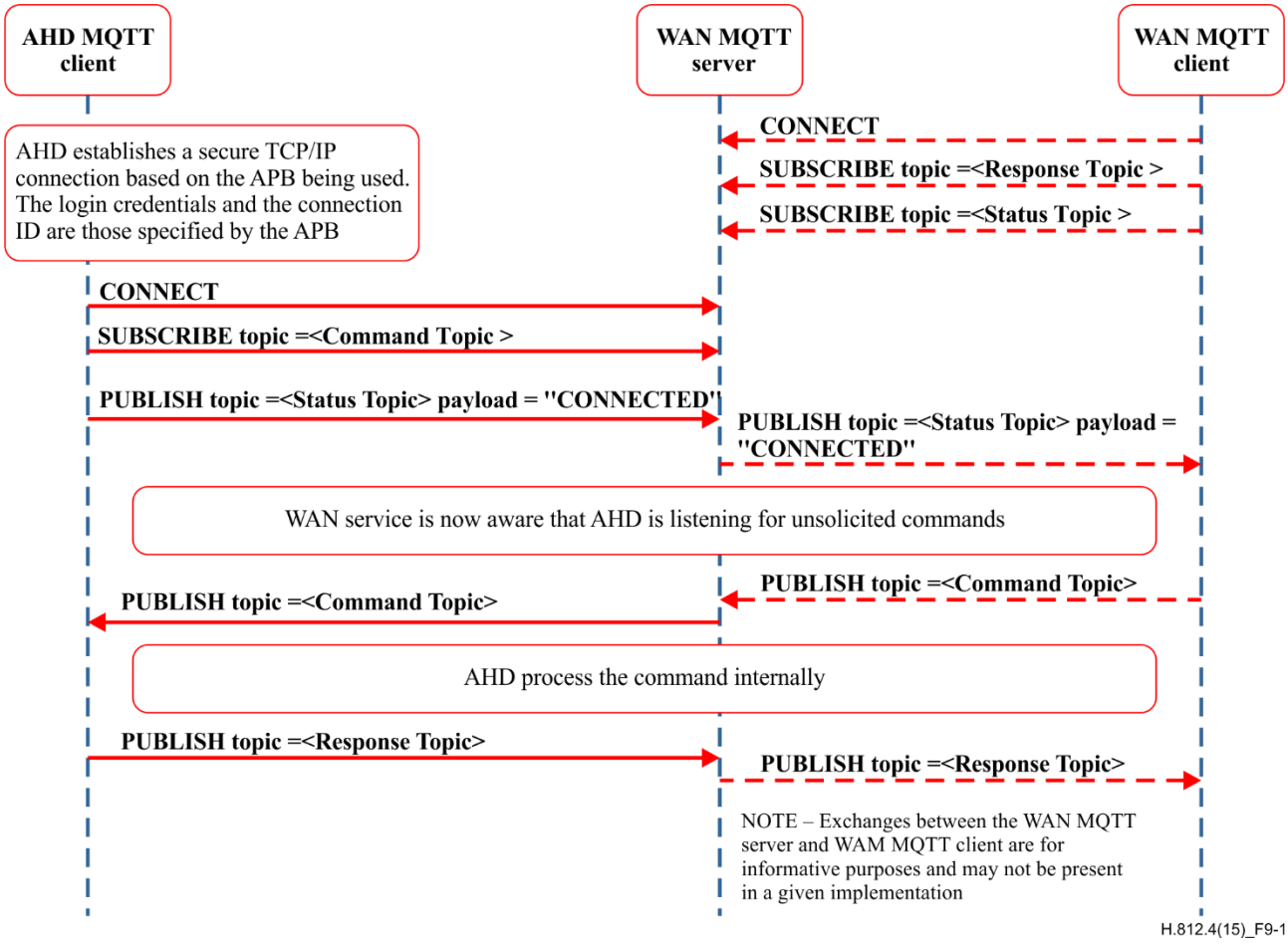

Figure 9-1 – AHD application and WAN application MQTT client interactions

In clause 8.2, interactions are described from the point of view, respectively, of the AHD application and the WAN application. It is important to note that how the WAN application communicates with its MQTT server is up to the application. The only normative components of the APS interface are the exchanges between the AHD application and the WAN and MQTT services.

9.1.1 Graceful APS termination

When possible, an AHD application should terminate an APS gracefully.

To terminate an APS gracefully the following steps **shall** be taken by the AHD application:

– Establish a connection with the WAN application that owns the APB resource defining the APS that is to be terminated.

– Perform a PUT operation of an APB resource with the <APSState> element set to TERMINATED to disable further use of the APS by the WAN application.

– CLOSE any active connection used by the APS to exchange messages over MQTT.

– Perform an MQTT CONNECT with the clean session flag set to true (clears the AHD's subscriptions on the MQTT server), the state of the retained Will flag to cleared, and the Will topic and Will message absent (prevents the allocation of any resources to send a status message when the connection to the AHD application is lost).

– Publish a zero length message to the status topic with the retain flag set to true to release the status resource.

– Disconnect from the MQTT server.

9.2 Interaction of the WAN application with the AHD application

The WAN application interacts with the AHD application via its associated MQTT server component. The precise way in which the WAN application interfaces with its MQTT server is not specified in these guidelines.

The WAN application, if it has determined that a message is to be sent using the APS, sends this message by issuing a PUBLISH packet to the appropriate message topic. The MQTT server uses a QoS level of 2 when issuing the PUBLISH packet.

If the WAN application has a message to send and the status topic indicates that the AHD application is not connected, it may attempt to bring the connection back up (if the AHD application supports shoulder tapping) by sending the out of band shoulder tap.

(Informative Note) The WAN application may subscribe to any APS response topics of interest. It may also subscribe to status topics, should it wish to track the online/offline status of its APSes. To listen for status updates from all APSes it can subscribe to the following wildcarded topic expression:

```
pcha/status/<WAN APBI>/#
```

9.3 State of the AHD's connection to the WAN MQTT server

Figure 9-1 documents the states that the status topic can be in, and the events that cause transitions between states.

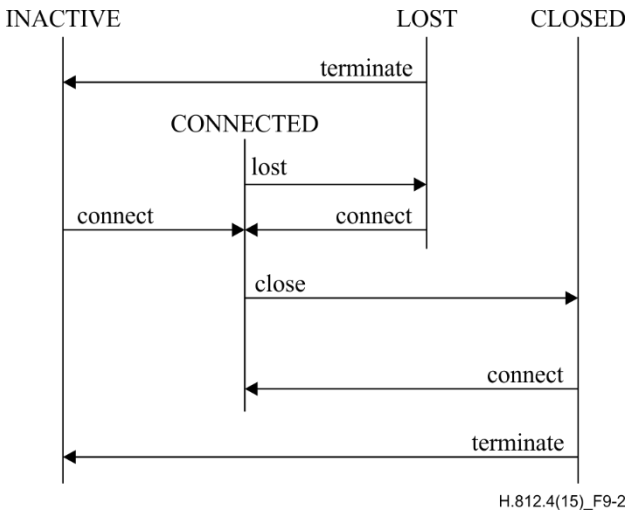

Figure 9-2 – State diagram for the status topic

The following normative table documents the states and state transitions of the status topic. The status topic is used by the WAN application to track the status of the AHD application's connectivity to the APS.

Table 9-1 – State table for the status topic

State	Event	Next state	Description
INACTIVE	connect	CONNECTED	The AHD application has established an MQTT session by logging in with a new client ID and a clean session flag set to false. The AHD application publishes a message to the status topic with a payload content of CONNECTED.
CONNECTED	lost	LOST	The WAN (MQTT) service has detected a TCP disconnection or a timeout event due to the absence of MQTT ping messages. The WAN (MQTT) service will publish a Will message to the status topic containing a payload of LOST.
CONNECTED	close	CLOSED	The AHD application closes the MQTT connection (sends an MQTT DISCONNECT control packet) but does not terminate the MQTT session. The AHD application publishes a message to status topic with a payload of CLOSED prior to disconnecting.
LOST	connect	CONNECTED	The AHD application has reconnected to an MQTT session by logging in with its existing client ID and a clean session flag set to false. The AHD application publishes a message to status topic with a payload content of CONNECTED.
LOST	terminate	INACTIVE	The AHD application has decided to terminate the APS by logging in with its existing client id and setting the clean session flag to true. It signals this condition by publishing a zero length message to the status topic. It then logs out by sending an MQTT DISCONNECT control packet.
CLOSED	connect	CONNECTED	The AHD application has reconnected to an MQTT session by logging in with its existing client ID and a clean session flag set to false. The AHD application publishes a message to status topic with a payload

Table 9-1 – State table for the status topic

State	Event	Next state	Description
			content of CONNECTED.
CLOSED	terminate	INACTIVE	The AHD application has decided to terminate the APS by logging in with its existing client id and setting the clean session flag to true. It signals this condition by publishing a zero length message to the status topic. It then logs out by sending an MQTT DISCONNECT control packet.

9.3.1 Interaction of an AHD application with the MQTT server

The AHD application establishes the APS session by performing an HTTP POST to the WAN application in the context of a secure connection providing some security credential. Once the AHD application has received this information, it interacts with the WAN application by creating a TLS connection with the MQTT server component associated with the WAN application.

Once it has established a TLS connection, the AHD application sends an MQTT CONNECT control packet to the MQTT server on that connection. The AHD application waits for a response from the MQTT server. If it receives a data packet that is not an MQTT connection acknowledgement, then the AHD application closes the TCP/IP connection.

The AHD application sets the following fields in its MQTT connect message (normal connection).

Table 9-2 – Information contained in the AHD application's MQTT connect message

Information element	Value set by the AHD	Comments
Flags	0xEC	– User name and password are present – Retained Will message requested (with QoS 2) – Clean Session not requested
Keep Alive	Chosen by the AHD implementation	If no activity has taken place during a given keep alive time period the AHD application should send an MQTT PING to keep the connection open. It may set a value of 0 to indicate that it doesn't commit to send any PING messages
Client Identifier	A string provided by the WAN application in the APB resource.	The MQTT server uses the client identifier to identify the MQTT session. When operating in the context of a particular APS the AHD application must always use the string specified by the WAN application in the APB resource
Will Topic	The AHD's *status* topic	Topic used to track the status of the connection
Will Message	The string "LOST"	Payload of MQTT message that is to be generated (internal to the WAN application) indicating that the AHD has gone offline unexpectedly.
User Name	The AHD APBI provided by the WAN application in the APB resource	Used to authorize AHD application access to topics.

Table 9-2 – Information contained in the AHD application's MQTT connect message

Information element	Value set by the AHD	Comments
Password	The AHDCredential provided by the WAN application in the APB resource	Used to authenticate the AHD application

The Will flag, Will Retain flag and Will message ensure that the WAN application is informed when communications with the AHD are unexpectedly disrupted. This notification process is internal to the implementation of the WAN application, but is controlled by these parameters. The AHD application is required to set them to the values specified above.

The MQTT Keep Alive value determines how quickly the MQTT server will detect the loss of connectivity to the AHD application. It also commits the AHD application to periodically send an MQTT PING packet if there has been no other activity.

When it has a received a positive connection acknowledgement from the MQTT server, the AHD application then proceeds to send MQTT SUBSCRIBE requests to its command topics. These command topics are qualified by the CDC message handler as shown in clause 7.2. The AHD application **shall** subscribe on behalf of all the message handlers it has advertised in the APB resource. It sets the information in the MQTT SUBSCRIBE request indicated in Table 9-3.

Table 9-3 – Information contained in MQTT SUBSCRIBE message

Information element	Value	Comments
Topic	The *command* topic name	A set of topics from which the AHD application wishes to receive PUBLISH messages
Requested QoS	2	This allows the WAN application to define the QoS level based on the value of QoS selected in the PUBLISH control packet

When it has a received a positive SUBSCRIBE acknowledgement from the MQTT server, the AHD application sends a PUBLISH control packet to update the *status* topic to show that it has come online. The publish status is sent with QoS 2. The message parameters are shown in Table 9-4.

Table 9-4 – Information contained in the AHD's publish status message

Information element	Value	Comments
Retain Flag	True	Message is to be retained by the MQTT server so that later subscribers can be informed of the AHD application's current connection status
Topic	The *status* topic name	Topic that is tracking the connection state of the APS
QoS	2	
Payload	The string "CONNECTED" Or "CLOSED"	Status information to be sent to the WAN application indicating that the AHD application associated with the APS is online Or Status information to be sent to the WAN application indicating that the AHD application is disconnecting from the MQTT server but maintaining the APS enabled

There is a second type of publish status message defined in this standard. This message is used only when the AHD application is in the process of terminating the APS. The publish status message in this case has the retain flag set to true and an empty payload. The purpose of this message is to clear resources associated with the APS on the MQTT server.

After the AHD application has completed the SUBSCRIBE operation it is ready to receive messages from the WAN application.

At this point the AHD application enables the APS performing an HTTP PUT operation to the URL provided by the WAN application during APS establishment. The HTTP PUT contains the APB resource with the <APSState> element value set to ENABLED. No message can be received before the AHD application enables the APS.

When the AHD application has processed a message, it responds by sending an MQTT PUBLISH control packet indicated in Table 9-5.

Table 9-5 – Information contained in the AHD application's MQTT publish response message

Information element	Value	Comments
Retain Flag	False	Message does not need to be retained once it has been delivered to the WAN application
Topic	The *response* topic name	See Table 7-1.
QoS	2	The response Shall be delivered exactly once
Payload	Dependent on entity using the APS service	Response to be sent to the WAN application

If the AHD application detects loss of its MQTT connection, or loss of the underlying TCP/IP connection then it may attempt to reconnect immediately, following the process described at the beginning of this clause. If it is able to tell that the disconnection happened because of a total loss of network connectivity, then it should defer a reconnection attempt until the network is restored.

The AHD application may elect to disconnect the MQTT connection while still maintaining the APS. In this case, the AHD application should publish a status update message, but with a payload of CLOSED rather than CONNECTED, prior to sending the MQTT DISCONNECT message. It may reconnect at a future time of its choosing.

If the AHD application supports a shoulder tap mechanism it must attempt to reconnect when it receives a shoulder tap.

Upon reconnection, the AHD application should be prepared to handle incoming messages immediately, since some messages might have been queued up for it during the time when it was disconnected.

10 Behavioural model: SMS shoulder tap capability

These guidelines define a capability that facilitates operation of the APS with networks that remove IP infrastructure for inactive connections. This capability is based on the short message service (SMS) as defined in [b-GSM/UMTS][b-CDMA 2000]. Future versions of these guidelines may provide different mechanisms to implement this capability as cellular network providers deploy additional services.

10.1 Shoulder tap overview

When there is no data exchanged between a WAN application and an AHD application, both wireless network resources and AHD energy consumption can be reduced by tearing down the wireless data connection, resulting in a loss of IP connectivity. A wireless data connection can also

be lost due to coverage issues, or lack of energy (available battery capacity) on an AHD. The loss of IP connectivity does not terminate the APS and when IP connectivity is re-established, the software entities bound by the APS can once again use the IP network to exchange information.

This clause defines an out-of-band mechanism called a shoulder tap (ST), which the WAN application can use to accelerate the re-establishment of IP connectivity. The mechanism can be used with any AHD application that has a cellular interface supporting SMS.

Figure 10-1 presents a high level overview of the sequence of events in a shoulder tap.

The first step of the ST process is an exchange of information between the AHD application and the WAN application. This takes place during APS establishment. At some subsequent point in time, the network connection between the AHD application and the WAN application is discontinued causing the underlying exchange mechanism to mark the connection as being lost. When an application activity using the APS-CDC requires the WAN application to send a message, the WAN application recognizes the fact that the IP connectivity to the AHD application has been lost. At this point it transmits a shoulder tap message to the AHD application using an out-of-band capability such as SMS to wake up the AHD. Receipt of the shoulder tap message informs the AHD application that the WAN application wishes to exchange a message with it. The AHD application then re-establishes IP data connectivity and resumes message exchange with the WAN application in the context of the APS.

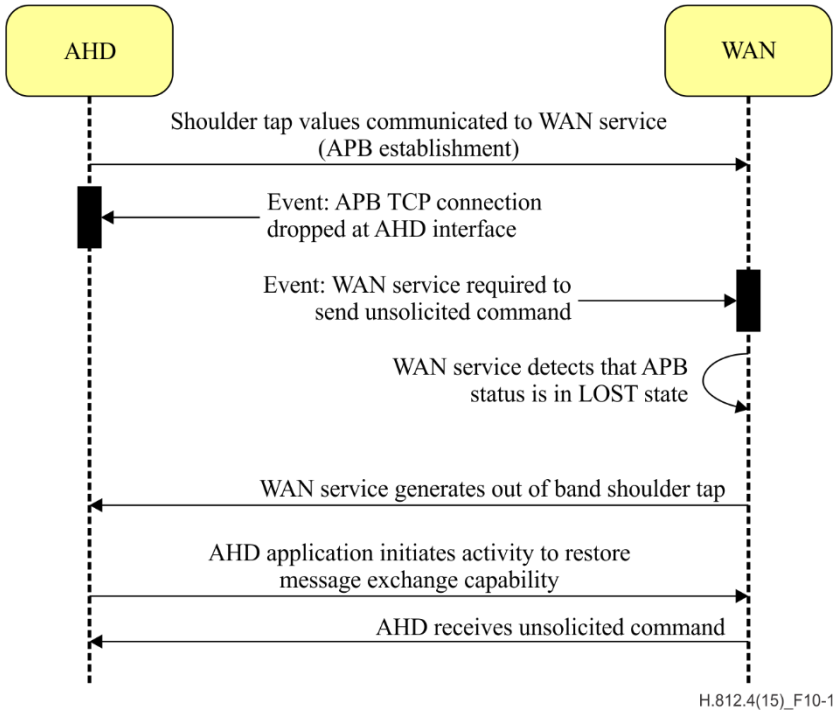

Figure 10-1 – Shoulder tap overview

10.2 Scope

The availability of an out-of-band shoulder tap mechanism is a function of the capabilities of the networks that the AHD application and the WAN application are associated with, the capability of the WAN application to initiate the shoulder tap, and the capability of the AHD application to receive and process the shoulder tap. This implies that all entities including the WAN application, the network, and the AHD application, must be able to operate in accordance with these guidelines to implement shoulder tap functionality. However, these guidelines only document the interface behaviour between the AHD application and the WAN application as seen at AHD's interface to the network. It is the responsibility of the system integrator to ensure that the required network

infrastructure is in place to enable the WAN application to meet the interface requirements defined here.

10.3 Shoulder tap invocation determination

It is possible that an active data connection is currently available to the AHD application so that a shoulder tap does not need to be invoked by the WAN application. This can be determined by looking at the status of the connection state in the underlying message exchange facility. When using MQTT the connection state is maintained in the status topic. The shoulder tap should not be performed if the status topic already indicates that the connection is operational (CONNECTED state).

10.4 AHD SMS information

When an AHD application uses SMS shoulder tapping the AHD application communicates the following information to the WAN application during APS establishment:

– The supported types of shoulder tapping, which must include SMS.

– The address (MSISDN) to which the SMS message is to be sent.

– The port number used in the SMS user data header (UDH) to identify the UDH defined end point (port) that will receive the SMS message.

– An AHD application specified identifier that is returned to the AHD in the SMS payload.

The WAN application uses the AHD provided information to generate the SMS message as defined in this clause. In the event that a third party SMS provider is used to generate or deliver the SMS message to the AHD, the third party SMS provider is considered to be part of the WAN application and proper behaviour at the AHD interface is determined by the structure of the SMS message delivered to the AHD by the third party provider.

10.5 SMS message structure

The WAN application creates an SMS message as defined herein and sends the message toward the AHD. The following bullet points describe the SMS message as it is delivered to the AHD.

– The message is a binary SMS message.

– The message is delivered to the MSISDN provided by the AHD application.

– The SMS message contains a User data header and the TP-UDHI (Transfer layer protocol data header indicator) bit is set.

– The layout of the SMS payload is given in Figure 10-2.

– The SMSHeaderDstPort is encoded into the UDH.

NOTE – The corresponding source port associated with information element 0x04 in the UDH is not used by the AHD application.

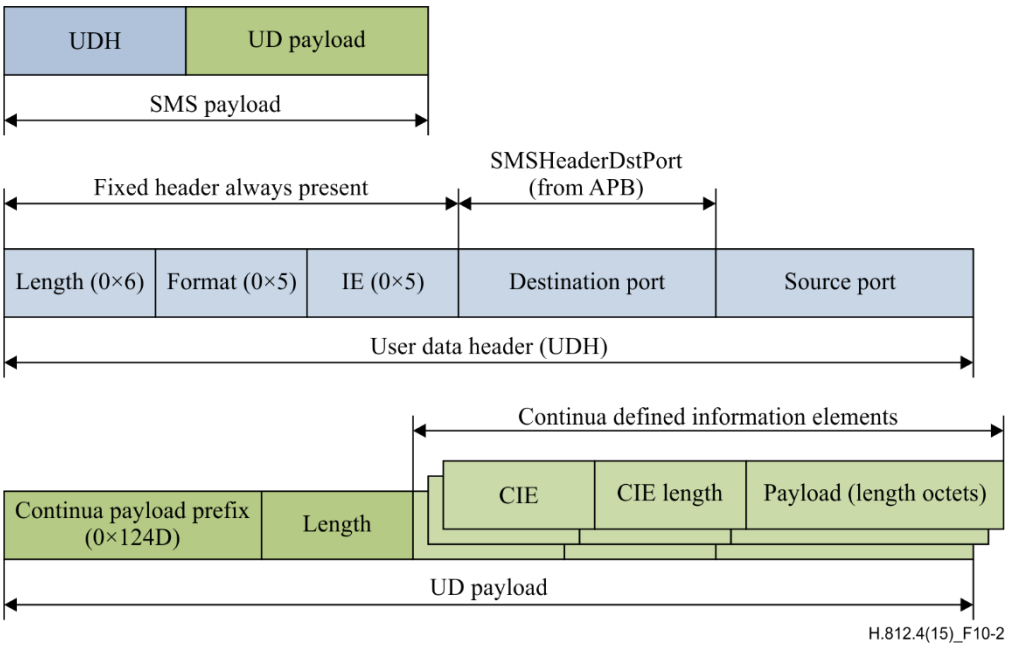

Figure 10-2 – Payload of binary SMS message

The UDH is six octets long with the information in the header formatted in hexadecimal (0x05). The header contains one information element (value 0x05 – Application port addressing scheme, 16 bit addressing).

The payload contains a Continua defined prefix value of 0x124D and a repeating sequence of Continua information elements (CIE) as defined in Table 10-2.

Table 10-1 – Structure of payload

Field	Length
Continua Prefix '0001001001001101'b =0x124D	2 octets
Length of Shoulder tap payload excluding first three octets	1 octet
Type of Information-element "A"	1 octet
Length of Information-element "A"	1 octet
Value of Information-element "A"	0 to "n" octets
(repeated for other information elements as needed)	

Table 10-2 – Continua information elements

CIE Type	Length	Requirement	MEANING
00	1-148	optional	Shoulder tap application identifier – This value is communicated to the WAN application in the APB element <SMSApplicationId>. In the SMS message it is encoded using UTF-8.
01	1	optional	Shoulder tap semantic – This value indicates the action that the AHD application should take upon reception of the shoulder tap. Currently defined values are: 0x01: Re-establish transport level connectivity – The WAN application wishes to send a message to the AHD application and is waiting for the transport level connectivity to be re-established.

10.6 AHD application requirements

When the AHD application is running on an OS platform that processes the arriving SMS message, that platform will need to provide an interface to the AHD application that allows the AHD application to be notified when the binary SMS message arrives. The mechanisms used to notify the AHD application are not specified by these guidelines.

10.7 Semantic Behaviour of the AHD application relative to ST reception

Upon receipt of a shoulder tap with Reason 'Re-establish connection to message exchange server', the AHD application **shall** re-establish its TCP connection to the WAN MQTT server and submit a CONNECT message. This procedure may need re-establishment of the connection to the packet-switched network.

Annex A

Normative guidelines for the APS-CDC

(This annex forms an integral part of this Recommendation.)

These tables list the guideline specifications for Continua certification of an AHD application and WAN application that support authenticated persistent sessions.

A.1 Guidelines for the APS components in capabilities exchange

A WAN application that supports an authenticated persistent session (APS-CDC-WAN) **Shall** provide a root.xml file in accordance with Table A-1. An AHD application that supports an authenticated persistent session (APS-CDC-AHD) is also required to support Table A-1.

Table A-1 – APS elements of capabilities exchange

Name	Description	Comments
APS-CDC-WAN_Root_Support	A WAN application **Shall** indicate that it supports the APS-CDC-WAN by providing a profile with the value of the id element set to APS-CDC-WAN in the root.xml file.	See Figure 8-1.
APS-CDC-AHD_Root_Support	An AHD application that POSTs a root.xml file to a WAN application during capability exchange **Shall** provide a profile with the id element set to APS-CDC-AHD in the root.xml file.	See Figure 8-1. Note that APS-CDC-WAN is replaced by APS-CDC-AHD.
APS-CDC-WAN_Description_Information	A WAN application **Shall** describe the content of the APB resource using a <resourceType> entry in the root.xml in accordance with Figure 8-2.	This entry in the root.xml describes the content of the APB resource as well as referencing a validator for the formatting of the APB resource.
APS-CDC-WAN POST_Location	A WAN application **Shall** provide a URL where the AHD application is to perform the initial POST to establish an APS in a <section> entry in the root.xml in accordance with Figure 8-3.	
APS-CDC-WAN_Resource_Prefix	The <resourcePrefix> child element of the <section> entry **Shall** be present and the value **Shall** be set to true.	The resource prefix is required to be present and true in this specification though it is optional in the hDATA specification.
APS-CDC-WAN_Profile_ID	The <profileID> value of the <section> described in Figure 8-3 and the <id> value of the <profile> described in Figure 8-1 **Shall** be set to APS-CDC.	The profileID element value of the section identifies the profile to which it is associated.

A.2 Guidelines for AHDAPS management (APS-CDC-AHD)

An AHD application that supports the Authenticated persistent session certified device class **Shall** operate in accordance with Table A.2.

Table A.2 – APS management AHD

Name	Description	Comments
APS-CDC-AHD_Initiate_ APS_Establishment	If an AHD application indicates support for an APS during capability exchange then it **Shall** initiate APB establishment by POSTing its APB resource.	These guidelines do not define the exact time by which the APS is to be established. However, management services of the APS-CDC should be made available to the WAN in a timely manner.
_APS-CDC-AHD_POST_ Location	An AHD application establishing an APS session **Shall** POST the APB resource to the URL specified in the <path> child element of the <section> defined in Figure 8-3.	The AHD application obtains the URL for the POST in a <section> element of the root.xml. Since there may be many sections in the root.xml, the <profileID> element value identifies the correct <section>.
APS-CDC-AHD_APB_ POST_XML	An AHD application establishing an APS session **Shall** POST the APB resource as anXMLdocument.	The APS is described by an APB resource which is expressed as anXMLdocument.
APS-CDC-AHD_APB_ Schema	An AHD application establishing an APS session **Shall** always transmit APB resources in accordance with the APB resource schema of Appendix II.	
APS-CDC-AHD_APB_FILL	An AHD application establishing an APS session **Shall** fill in elements of the APB resource in accordance with Table 8-1.	
APS-CDC-AHD_Supported_ MH_List	The entries in the <supportedMH> element **Shall** be a space separated list.	The list may contain proprietary entries.
APS-CDC-AHD_APS_MH	An AHD application APSes **Shall** include the string "APS" as one of the list entries in the supportedMH element of the APB resource.	This implies that all AHD applications will respond to APS-CDC defined management messages from the WAN application.
APS-CDC-AHD_Supported_ MX_List	The entries in <exchangeMechanism> **Shall** be a space separated list ordered from the most desired to the least desired with the first element being the most desired by the AHD.	This guideline specifies the format of the listing in the element value.
APS-CDC-AHD_MQTT_ MX	The AHD application **Shall** specify "MQTT" in its list of supported exchange mechanisms.	Continua compliant AHD applications implementing the APS-CDC must support MQTT.
APS-CDC-AHD_Supported_ ST_list	The entries in <shoulderTapMechanism> **Shall** be a space separated list ordered from the most desired to the least desired with	This guideline specifies the format of the listing in the element value.

Table A.2 – APS management AHD

Name	Description	Comments
	the first element being the most desired by the AHD.	
APS-CDC-AHD_ST_BASE	The AHD application **Shall** provide an empty list for shoulderTapMechanism if it does not support a shoulder tap mechanism.	
APS-CDC-AHD_ST_SMS	If the AHD application supports SMS as a shoulder tap mechanism then the AHD application **Shall** include the <SMS> element in the APB resource.	
APS-CDC-AHD_SMS_ MSISDN	If the AHD application supports SMS as a shoulder tap mechanism then the AHD application **Shall** include the number to reach the AHD application in the <MSISDN> child element of the <SMS> element in the APB resource.	
APS-CDC-AHD_SMS_ Destination_Port	If the AHD application supports SMS as a shoulder tap mechanism the AHD application **Shall** include the port associated with the AHD application in the <SMSHeaderDstPort> child element of the <SMS> element in the APB resource.	The source port and the source number do not need to be specified in the APB since the AHD application never sends an SMS message to the WAN application.
APS-CDC-AHD_SMS_ APP_ID	If the AHD application supports SMS as a shoulder tap mechanism the AHD application **may** include the <SMSApplicationId> child element of the <SMS> element in the APB resource.	This message contains an identifier that the AHD application can use to identify the received SMS message as being for itself.
APS-CDC-AHD_SMS_ APP_ID_Limit	The AHD application **Shall** not provide a string that when encoded inUTF-8 will exceed 148 octets for <SMSApplicationId>	
APS-CDC-AHD_SMS_ APB_GET	An AHD application **Shall** obtain the completed APB resource by invoking an HTTP GET using the URL provided by the WAN application in response to the AHD application's successful POST request.	The AHD application gets a URL in the POST return. This URL identifies the location of the APB resource which the AHD application can obtain using an HTTP GET.
APS-CDC-AHD_Ignore_ XML	An AHD application **Shall** ignore any XML elements it does not understand in the APB.	Supports migration to future versions of the APB
APS-CDC-AHD_Process_ WAN_Elements	On receipt of an APB resource from the WAN application the AHD application **Shall** only process the elements defined in Table 8-2.	The AHD application is defined to provide values for particular elements in the APB. If a WAN application incorrectly updates the values for these elements the

Table A.2 – APS management AHD

Name	Description	Comments
		AHD should ignore them.
APS-CDC-AHD_APS_ ENABLE	The AHD application **Shall** invoke an HTTP PUT of the APB/APSState resource with the value set to ENABLED to indicate it is ready to accept messages.	
APS-CDC-AHD_APS_ Termination	An AHD application **Shall** indicate that the APS is terminated by invoking an HTTP PUT on the current APB resource with the <APSState> element value set to TERMINATED.	This action is the first step taken in APS termination.
APS-CDC-AHD_immutable	An APB resource obtained from a WAN application **Shall not** be modified except for the <APSState> element.	The AHD cannot modify fields of the APB resource and communicate those back to the WAN application.

A.3 Guidelines for the AHD application interactions with the MQTT server

Table A.3 covers the interaction of the AHD application with respect to MQTT exchanges. An AHD application implementing the APS-CDC-AHD **shall** operate in accordance with Table A.3.

Table A.3 – AHD-MQTT exchanges

Name	Description	Comments
APS-CDC-AHD_Message_ Exchange	An AHD application Shall support the use of MQTT as a method of message exchange.	Future versions of these guidelines may support other methods of message exchange.
APS-CDC-AHD_MQTT_ conformance	An AHD application Shall be compliant with the requirement for a client as specified in [MQTT].	
APS-CDC-AHD_MQTT_ Connect_URL	An AHD application's MQTT client Shall use the information identified in the <APS_ExchangeURL> element of the APB resource in order to establish the transport connection to the MQTT server.	The WAN application indicates to the AHD application the URL that allows it to connect to the MQTT server in the <APS_ExchangeURL> element value. See Table 8-2.
APS-CDC-AHD_MQTT APS_Connect_Setup	The MQTT client component of the AHD application Shall issue the MQTT CONNECT control packet in accordance with Table 9-2.	The APS requires specific MQTT settings to be used in a CONNECT control packet.
APS-CDC-AHD_MQTT Connect_User _Name	An AHD application Shall use the value of the <AHDAPBI> element provided by the WAN application in the APB resource as the user name in the MQTT connect message.	See Table 8-2

Table A.3 – AHD-MQTT exchanges

Name	Description	Comments
APS-CDC-AHD_MQTT_ Connect _Password	An AHD application Shall use the value of the <AHDCredential> element provided by the WAN application in the APB resource as the password in the MQTT connect message.	See Table 8-2
APS-CDC-AHD_MQTT_ Client_Identifier	An AHD application Shall use the value of the <clientId> element provided by the WAN application in the APB resource as the client identifier in the MQTT connect message.	See Table 8-2
APS-CDC-AHD_MQTT_ Connect_Will_Topic	An AHD application Shall set the Will Topic of the connect message to the status topic for this APS as defined in Table 7-1.	The setting tells the MQTT server to publish the Will message on the status topic when the connection to the AHD application is lost.
APS-CDC-AHD_MQTT APS_Connect_Will_ Message	An AHD application Shall set the Will message of the connect message to "LOST".	A LOST message will be sent to the WAN application if connection to the AHD application is lost.
APS-CDC-AHD_MQTT_ Normal_Connect_Flags	An AHD application Shall set the flags field of the connect control packet to indicate that the user name and password are present, that a clean session is NOT requested, and that a retained WILL message is requested. See Figure 9-2.	The MQTT connection is to require a user name and password login, a retained WILL message, with no clean session. The latter indicates that any messages for the AHD application will be received once the connection is complete and the AHD application has completed its subscription to the command topic.
APS-CDC-AHD_AHD_ Command_Subscribe	An AHD application Shall subscribe to the message topics as defined in Table 7-1.	
APS-CDC-AHD_Subscribe_ QoS	An AHD application Shall set the QoS of the message topic subscription requests to 2 in accordance with Table 9-3.	
APS-CDC-AHD_AHD Subscribe_All_Supported_ mh	An AHD application Shall subscribe to all message topics for Message Handlers that it has indicated support for in its <supportedMH> element value.	Since the AHD application does not know which CDCs are supported by the WAN application, it needs to subscribe to all of them.
APS-CDC-AHD_Publish_ Status_Topic	An AHD application Shall publish on the status topic for this APS as defined in Table 7-1.	
APS-CDC-AHD_Status Publish_Retain	An AHD application Shall issue a PUBLISH control packet in	In the case where the AHD is retaining the APS in the enabled

Table A.3 – AHD-MQTT exchanges

Name	Description	Comments
	accordance with Table 9-4 when writing values to the status topic.	state, publishing is done with the retain flag true.
APS-CDC-AHD_Clear_ Queue	An AHD application Shall set the retain flag of the PUBLISH control packet to true when setting the payload to a zero-length message.	In the case where the AHD is terminating the APS, publishing is done with the retain flag true since the publishing is to clear any outstanding status messages. See clause 9.1.1.
APS-CDC-AHD_Status_ Publish_QoS	An AHD application Shall set the QoS level of the PUBLISH control packet on the status topic message to 2.	A QoS of 2 applies to all PUBLISH control packets.
APS-CDC-AHD_Status_ Publish_Payload _Values	An AHD application Shall set the Payload of the PUBLISH control packet on the status topic to one of either "CONNECTED" or "CLOSED" or be of zero-length.	In these guidelines the status message payload published by the AHD application may take on one of the following values "CONNECTED" "CLOSED" or of zero length, the last of which is used only in the case of clearing MQTT when the APS is terminated by the AHD application.
APS-CDC-AHD_Response_ Publish_Topic	An AHD application Shall PUBLISH on the response topic in accordance with Table 9-4.	The response topic is specified in Table 7-1. The proper substitutions must be made.
APS-CDC-AHD_Response_ Publish _Retain	An AHD application Shall set the retain flag to false when publishing on a response topic	The message does not need to be retained since it has been delivered to the WAN application. The MQTT server is internal to the WAN application.
APS-CDC-AHD_Response_ Publish_QoS	An AHD application Shall set the QoS level of the PUBLISH control packet on a response topic message to 2.	A QoS of 2 applies to all PUBLISH control packets.
APS-CDC-AHD_ECHO _ Support	An AHD application Shall support the APS-CDC-WAN diagnostic message ECHO command as described in clause 8.2.6	
APS-CDC-AHD_Status_ Behavior	An AHD application Shall manage the status topic in accordance with Table 9-5.	See also Figure 9-2. Additional guidelines related to the status topic are in this table.
APS-CDC-AHD_Status_ Publish _Clear_MQTT	An AHD application Shall set the status topic to INACTIVE when it successfully connects to the MQTT server under the conditions of setting the clean session flag to true with a payload of zero-length and a retain flag set to true.	This guideline defines the publish action of the AHD after connecting to MQTT server to clear it of resources. This status update is part of a sequence of events that take place when the AHD has terminated the APS.
APS-CDC-AHD_Graceful_	An AHD application Shall terminate	This guideline intends to validate

Table A.3 – AHD-MQTT exchanges

Name	Description	Comments
APS_Termination_Procedure	an APS following the procedure in clause 9.1.1.	that the graceful APS termination procedure follows all the steps in clause 9.1.1 in order; terminate the APS on the APS management connection, put the MQTT server into the LOST or CLOSED state if not already in the LOST or CLOSED state, connect using the clear-connect configuration, publish using the clear-status configuration, and close the MQTT connection.

A.4 Guidelines for WAN application APS management

The WAN application configures several elements of the APB resource for the APS. It is also responsible for assuring that a given APS is associated with a given security credential where the security credential identifies the AHD that is authenticated to use the APS. A WAN application implementing the APS-CDC-WAN **Shall** operate in accordance with Table A.4.

Table A.4 – APS management requirements for the WAN application

Name	Description	Comments
APS-CDC-WAN_ Enforce_Authorized_ APB_Access	A WAN application **Shall** assure that the APB resource created to represent a given APS can only be accessed by an entity possessing the security credential that was used to establish the APS.	This guideline requires that the WAN application assure that any reconnection made by the AHD application for APS management is only able to operate within the APS authorized for the AHD application.
APS-CDC-WAN_ Enforce_Topic_ Space_Access	A WAN application **Shall** enforce access control to the topic space as defined in clause 7.2.	
APS-CDC-WAN_ XPath	A WAN application Shall support references to the <APSState> element defined in the APB when this reference is expressed in accordance with [XPath 2.0].	
APS-CDC-WAN_ MQTT_Support	A WAN application **Shall** support the use of MQTT as a mechanism for APS message exchange.	How the WAN application interacts with the MQTT server is implementation dependent but the interface exposed to the AHD application is that specified by the MQTT standard.
APS-CDC-WAN_ APS_Management_ Support	A WAN application supporting the APS-CDC **shall** support the APS management messages defined in clause 8.2.6.1.1.	

Table A.4 – APS management requirements for the WAN application

Name	Description	Comments
APS-CDC-WAN_ APB_POST_ RESPONSE_APB_ CREATED	If a WAN application creates an APS with the AHD application it **Shall** set the return code to 201.	
APS-CDC-WAN_ APB_POST_ RESPONSE_APB_ NOT_CREATED	If a WAN application does not create or update an APB on a client request to do so, it **Shall** return an appropriate status code in either the 400 group or 500 group.	
APS-CDC-WAN_ Process_WAN_ Elements	On receipt of an APB resource from the AHD application the WAN application **Shall** only process the elements defined in Table 8-1.	
APS-CDC-WAN_ Ignore_XML	A WAN application **Shall** ignore any XML elements it does not understand in the APB.	Supports migration to future versions of the APB
APS-CDC-WAN_No_ Modify	A WAN application **Shall** not modify any elements in Table 8-1 when presenting or processing the elements of the APB.	
APS-CDC-WAN_ APB_Schema	A WAN application establishing an APS session **Shall** always transmit APB resources in accordance with the APB resource schema of Appendix II.	
APS-CDC-WAN_ Unique_AHDAPBI	A WAN application **Shall** create an <AHDAPBI> element value that is unique across all APSes that are known to be valid for the WAN application.	At any given time, if the WAN application has N APSes, the <AHDAPBI> value of each one of the N associated APB resources must be unique. This requirement does not exclude the reuse of a value from an APS that was terminated.
APS-CDC-WAN_ AHDAPBI _ Constraints	The WAN application **Shall** restrict the <AHDAPBI> element's value according to the AHDAPBI entry in Table 8-2.	
APS-CDC-WAN_ WANAPBI _ Constraints	The WAN application **Shall** restrict the <WANAPBI> element's value according to the WANAPBI entry in Table 8-2.	
APS-CDC-WAN_ Unique_ClientId	A WAN application **Shall** create a <clientId> value that is unique across all APSes currently in service.	Recall that this value serves as the MQTT AHD client identifier.
APS-CDC-WAN_ ClientId_Contraints	A WAN application **Shall** restrict the <clientId> value according to the clientId entry in Table 8-2.	The current MQTT specification restricts the length of the string to be 23 UTF-8 characters.

Table A.4 – APS management requirements for the WAN application

Name	Description	Comments
APS-CDC-WAN_ NEW_APSState	The WAN application **Shall** set the <APSState> value to NEW if the AHD application does an HTTP POST and there exists no APS for the given security credential.	When the WAN application handles a POST from the AHD application and no APS currently exists for that security credential, the WAN application will need to complete the APB resource POSTed by the AHD and in that case the state is set to NEW.
APS-CDC-WAN_ ExpirationTime	A WAN application **Shall** provide an expiration time in the <expirationTime> element value which represents the time duration for which the WAN application will tolerate inactivity.	This value represents the length of time the WAN application will accept no activity from the AHD application within the APS before testing the AHD application to see if it is still engaged. After this time if the WAN application receives no timely response to an APS "ECHO" management message after a shoulder tap wake up OR the AHD application does not respond to the shoulder tap wake up, the WAN application may terminate the APS.
APS-CDC-WAN_ ResponseTime	A WAN application **Shall** provide a required response time to an APS "ECHO" management message in the <requiredResponseTime> element value which represents the duration in time for which it is prepared to wait for a response to the ECHO.	This value represents how long an AHD application has to respond to a UC "ECHO" message before the WAN application considers the AHD application out of service at which time the WAN application may terminate the APS.
APS-SUPPORT-TERMINATE	A WAN application **Shall** support the termination of an APS as defined in clause 8.2.5.	
APS-CDC-WAN_ MQTT_URL	A WAN application **Shall** provide the URL to the WAN MQTT end point in the <APSExchangeURL> element value.	

Table A.4 – APS management requirements for the WAN application

Name	Description	Comments
APS-CDC-WAN_ APB_EXISTS	If the AHD application invokes an HTTP POST and an APS already exists for the security credential the WAN application **Shall** ignore the contents of the POST and return the URL to the existing APB.	An AHD application that performs a POST to recover an APB using a security credential associated with an existing APB will get the already existing APB resource. The value of the APSState element in this case is set to ENABLED. It is advisable to check the state of APSState to ensure the expected value is returned. *Note that when and APB already exists on the WAN device, it will ignore all information the AHD includes in the APB POST. Therefore, when the AHD receives and APB with APSState set to ENABLED, it should check that all AHD related details in the APB are still correct. If the AHD related details are not correct anymore the AHD will first need to terminate this existing APB and subsequently create a new APB with updated information.*
APS-CDC-WAN_ APB_URL	A WAN application **Shall** respond to a HTTP POST that successfully created an APB resource with a URL that points to the APB resource.	
APS-CDC-WAN_ Provide_APB	A WAN application **Shall** provide the completed APB resource when the AHD application performs a GET using the POST URL. The POST URL is the URL returned by the WAN application in response to the AHD applications POST operation.	When the AHD application does an HTTP GET for the APB resource, the WAN application delivers the APB resource that the AHD application has been authenticated to operate with.
APS-CDC-WAN_ NO_APB_GET	If an AHD does an HTTP GET for the APB resource but the WAN application finds no APB resource that is authorized for use by this AHD application, the WAN application **Shall** respond with code 404 resource not found.	This case could happen, for example, when a trusted AHD has neglected to do a POST but still has the correct URL to point to the resource.
APS-CDC-WAN_ APSState_Update	A WAN application **Shall** update the <APSState> element value of the APB resource to the <APSState> element value sent by the AHD application in an HTTP PUT transaction if the value is either ENABLED or TERMINATED, otherwise it **Shall** return the status code 403.	

Table A.4 – APS management requirements for the WAN application

Name	Description	Comments
APS-CDC-WAN_ APSState_Only	A WAN application **Shall** ignore all values in the APB resource except the <APSState> element value sent by the AHD application in an HTTP PUT transaction.	
APS-CDC-WAN_ NO_APB_PUT	If an AHD application does an HTTP PUT of an APB resource but the WAN application finds no existing APB resource authenticated for use by the AHD application, the WAN application **Shall** respond with code 404 resource not found.	
APS-CDC-WAN_ WAIT_FOR_ ENABLE	A WAN application **Shall** refrain from sending messages to an AHD application until the <APSState> is set to ENABLED.	Though the AHD application is technically able to receive messages as soon as it has connected and subscribed to the message topic, no message are sent until the APS state has been set to enabled. Only the AHD application can set the state. The AHD application does not set the state to enabled until it is ready to handle messages.
APS-CDC-WAN_ APB_Remove_On_ Terminate	A WAN application **Shall** terminate the APS associated with the APB when the AHD sets the <APSState> to TERMINATED. The WAN application **Shall** ensure that a MQTT connection based on the terminated APB resource will fail.	
APS-CDC-WAN_ ExpirationTime	A WAN application **Shall** operate in accordance to Table 8-2 relative to inactivity exceeding <expirationTime>	See Table 8-2, <expirationTime>

A.5 Guidelines for the AHD application SMS shoulder tap

An AHD application implementing the APS-CDC-AHD **shall** operate in accordance with Table A.5.

Table A.5 – SMS shoulder tap AHD

Name	Description	Comments
APS-CDC-AHD_ST_Missing_ID	If the AHD application supports a shoulder tap using SMS, and it provides an SMSApplicationId then it **Shall** ignore all messages that do not contain the application identifier it set in the APB resource.	The identifier is a number the AHD application created in order to identify the SMS message as being for itself.
APS-CDC-AHD_ST_Reestablish	If the AHD application supports shoulder tap using SMS, then it **Shall** attempt to re-establish TCP connectivity with the WAN application when an SMS message containing the CEI of 01 (Re-establish transport level connectivity) is received.	This guideline assumes the message is addressed to the address and port specified in the APB resource.

A.6 Guidelines for the WAN application SMS shoulder tap

A WAN application implementing the APS-CDC-WAN Shall operate in accordance with Table A-6.

Table A-6 – SMS shoulder tap WAN

Name	Description	Comments
APS-CDC-WAN_ST_Send_Contents	If the WAN application supports shoulder tap using SMS, then when generating the shoulder tap message it **Shall**: a) use the MSISDN and SMSHeaderDstPort elements within the APB resource, and b) include the shoulder tap payload.	
APS-CDC-WAN_ST_Format	A WAN application **Shall** format the shoulder tap payload as specified in clause 10.5.	This guideline specifies details such as the presence of the Continua header and TLV messages.
APS-CDC-WAN_ST_Include_APP_ID	A WAN application **Shall** include the <SMSApplicationId> element value of the APB resource in the payload of the SMS in accordance with clause 10.5.	This value is a means for the AHD application to identify the SMS message as being for itself.

Annex B

XML schema for the APB resource

(This annex forms an integral part of this Recommendation.)

The XML structure as seen by the AHD application performing the GET of the APB is as follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
    targetNamespace="http://handle.itu.int/11.1002/3000/hData/APS"
        xmlns:tns="http://handle.itu.int/11.1002/3000/hData/APS"
elementFormDefault="unqualified">
 <complexType name="APBType">
  <sequence>
   <element name="supportedMH">
    <simpleType>
     <list itemType="string" />
    </simpleType>
   </element>
   <element name="exchangeMechanism">
    <simpleType>
     <list itemType="string" />
    </simpleType>
   </element>
   <element name="shoulderTapMechanism">
    <simpleType>
     <list itemType="string" />
    </simpleType>
   </element>
   <element name="SMS" type="tns:SMSType" minOccurs="0"/>
   <group ref = "tns:WANServerFields" minOccurs="0"/>
   <any namespace="##other" minOccurs="0" maxOccurs="unbounded"
processContents="lax" />
  </sequence>
 </complexType>
 <element name="APB" type="tns:APBType"></element>
 <complexType name="SMSType">
  <sequence>
   <element name="MSISDN">
    <simpleType>
     <restriction base="string">
      <maxLength value="15"></maxLength>
      <pattern value="\d+"></pattern>
     </restriction>
    </simpleType>
   </element>
   <element name="SMSHeaderDstPort" type = "unsignedShort"/>
   <element name="SMSApplicationId" minOccurs="0">
    <simpleType>
     <restriction base="string">
      <maxLength value="128"/>
     </restriction>
    </simpleType>
   </element>
  </sequence>
 </complexType>
 <simpleType name="APBI">
  <restriction base="string">
   <maxLength value="2047"></maxLength>
   <pattern value="[^/#+*]+"></pattern>
  </restriction>
```

```
 </simpleType>
 <group name="WANServerFields">
  <sequence>
   <element name="WANAPBI" type="tns:APBI" />
   <element name="AHDAPBI" type="tns:APBI" />
   <element name="APSExchangeURL" type="anyURI" />
   <element name="APSState">
    <simpleType>
     <restriction base="string">
      <enumeration value="NEW"></enumeration>
      <enumeration value="ENABLED"></enumeration>
      <enumeration value="TERMINATED"></enumeration>
     </restriction>
    </simpleType>
   </element>
   <element name="expirationTime" type="duration"/>
   <element name="requiredResponseTime" type="duration" />
   <element name="clientId" type="string" minOccurs="0"/>
   <element name="AHDCredential" type="string" minOccurs="0"/>
  </sequence>
 </group>
</schema>
```

Appendix I

APS details

(This appendix does not form an integral part of this Recommendation.)

I.1 APS information in the root.xml

An AHD obtains information regarding the capabilities supported by a WAN application through examining the WAN application's hData defined resource layout. This information is obtained through the root.xml file that is made available by the WAN application using the capability exchange facility documented in [ITU-T H.812.3].

A WAN application that supports the APS includes three entries related to the APS in its *root.xml*. The first entry indicates to the AHD application that the APS capability is supported. This entry is provided in a profile element and appears as shown in Figure 8-1.

A second entry provides both a reference to and a validator (such as anXMLschema) for the APB descriptor (such as anXMLschema). This entry is provided in a resourceType element and appears as shown in Figure 8-2.

The third entry provides the URL the AHD application is to use when it wishes to establish an APS with the WAN application. This URL is where the AHD application POSTs a description of its APS related capabilities. This entry is provided in a section element and appears as shown in Table 8-3.

NOTE – The Continua device classes (CDCs) documented in the root.xml are not the message handlers supported by the AHD application. These are found in the APB resource. The WAN application does not expose which protocols will use the APS service.

I.2 APS Authentication: Resource owner password credentials approach

There are several techniques for associating an APS with a security credential. The following description illustrates the use of the resource owner password credentials as a method of obtaining access to the APB resource associated with the APS. For additional details see Annex B of [ITU-T H.812].

Once the AHD application determines that the WAN application supports creating an APS through capability exchange, the AHD application can initiate the process of APS establishment. The first step in this process is for the AHD application to validate the WAN application through establishing a TLS connection with the WAN application. The AHD application may be aware of several different URLs associated with the WAN application. In this case we assume that the AHD application and WAN application have exchanged information relative to an authentication service. The login service accepts a username/password (resource owner credentials) from the AHD application and if these match it returns an OAUTH access token of type bearer. With this access token in hand the AHD application is able to perform HTTPS operations to obtain the APB resource associated with the authenticated persistent session service advertised in the root.xml file.

I.3 APS Establishment: AHD application POST with partial APB

Once the connection has been established the AHD application does a POST to the URL provided in the *root.xml* of the WAN application. The POST contains anXMLdocument describing the AHD application's APS capabilities (Table 8-1) as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
  <aps:APB xmlns:aps="http://handle.itu.int/11.1002/3000/hData/APS"
xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation =
"http://handle.itu.int/11.1002/3000/hData/APS/2015/01/APBConfigResource.xsd">
  <!-- These fields are filled in by the AHD -->
  <supportedMH>APS lampreynetworks.com/private</supportedMH>
  <exchangeMechanism>MQTT privateMessageProtocol</exchangeMechanism>
  <shoulderTapMechanism>SMS</shoulderTapMechanism>
  <SMS>
    <MSISDN>441111223344</MSISDN>
    <SMSHeaderDstPort>1234</SMSHeaderDstPort>
    <SMSApplicationId>4827351</SMSApplicationId>
  </SMS>
</aps:APB>
```

Figure I.1 – Example APB posted by AHD application

The WAN application can examine the space separated list of supported message handlers in the <supportedMH> element to see if the AHD application supports services that the WAN application can issue messages to. The WAN application can also inspect the space separated list of exchange mechanisms and the space separated list of shoulder tap mechanisms. If the WAN application supports a transfer mechanism advertised by the AHD application, the WAN application will be able to establish an APS. In this case the WAN application responds with an appropriate HTTP code such as 201 CREATED and provides a URL to the authenticated persistent binding (APB) resource. If the AHD application does not support any CDCs or transfer mechanisms that the WAN application supports, the WAN application responds with an HTTP error code such as 501 (Not Implemented).

I.3.1 APS establishment: AHD GET for completed APB

The AHD application can then issue a GET request for the APB resource. The AHD application must properly format the resource path according to the <resourcePrefix> entry in the *root.xml*. The WAN application creates the APB resource for the APS. The APB resource created is associated with the authentication credentials of the AHD application. The WAN application fills in the remaining elements of theXML document describing the APB resource in accordance with Table 8-2.

The resulting APB, as would be obtained by the AHD using the GET operation, is outlined in Figure I.2.

```
<?xml version="1.0" encoding="UTF-8"?>
<aps:APB xmlns:aps="http://handle.itu.int/11.1002/3000/hData/APS"
     xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation =
"http://handle.itu.int/11.1002/3000/hData/APS/2015/01/APBConfigResource.xsd">


 <!-- These fields are filled in by the AHD -->
 <supportedMH>APS lampreynetworks.com/private</supportedMH>
 <exchangeMechanism>MQTT privateMessageProtocol</exchangeMechanism>
 <shoulderTapMechanism>SMS</shoulderTapMechanism>
 <SMS>
  <MSISDN>441111223344</MSISDN>
  <SMSHeaderDstPort>1234</SMSHeaderDstPort>
  <SMSApplicationId>4827351</SMSApplicationId>
 </SMS>

 <!-- chosen by the WAN application; may be the same for every APS -->
 <WANAPBI>WANAPBI</WANAPBI>
 <!-- chosen by the WAN application; must be unique in all APSes on the WAN
application
    It is used as the 'user name' for MQTT -->
 <AHDAPBI>AHDAPBI</AHDAPBI>
 <!-- The address to the MQTT server -->
 <APSExchangeURL>address to the MQTT server</APSExchangeURL>
 <!-- The APS state which is NEW when first created -->
 <APSState>NEW</APSState>
 <!-- Chosen by the WAN application; The length of time the AHD may be silent
    before the WAN application may try and shut it down (after probing) -->
 <expirationTime>expirationTime</expirationTime>
 <!-- Chosen by the WAN application; The length of time that the AHD has to
    respond to an ECHO -->
 <requiredResponseTime>requiredResponseTime</requiredResponseTime>
 <!-- chosen by the WAN application and serves as the client identifier for the
MQTT server -->
 <clientId>clientId</clientId>
 <!-- chosen by the WAN application and serves as the 'password' for the MQTT
server
    For example the thumbprint of the AHD certificate -->
 <AHDCredential>AHDCredential</AHDCredential>
</aps:APB>
```

NOTE – This example includes a private message handler (lampreynetworks.com/private) as well as the required APS message handler.

Figure I.2 – APB created by WAN application

The WAN application may want to configure the MQTT software component at this time. This standard does not specify how the WAN application interacts with the MQTT server. The AHD application will publish on the response and status topics. How the WAN application obtains this information is out of the scope of this Recommendation.

I.3.2 APS establishment: AHD setup with MQTT server

Once the AHD application receives the APB resource, it needs to establish a secured connection with the MQTT server. The address of the MQTT server is provided in the APB resource.

The MQTT CONNECT command flags are used in a manner to indicate that a username and password are present, that the Will message will be retained, and that the session is not to be cleaned (this means that undelivered messages will be persisted across teardowns of the TCP connection) as defined in Table 9-2. These settings allow a previously published message on a topic

to be received once the AHD application subscribes to that topic. The user name and password are the AHDAPBI and AHDCredential, respectively, provided in the APB resource. The MQTT protocol requires that the AHD application provide a client identifier. The client identifier is provided in the clientID element of the APB resource. The AHD application also specifies a keep alive time which states how long it may remain inactive before issuing an MQTT PING. Specifying a 0 indicates that the AHD application will not send PING packets. The AHD application also sets the WILL message flag. This parameter indicates what the MQTT server will do when the connection to the AHD application is lost. The AHD application sets the WILL parameters to use the status topic with a payload "LOST". Thus when the connection to the AHD application is lost, the MQTT server will publish a message to the status topic with the payload "LOST".

I.3.3 MQTT: AHD application subscribes to commands

Once connected, the AHD application subscribes to the message topic for each CDC it is interested in receiving messages from. A single message topic is specified as follows:

```
pcha/message/WANAPBI/AHDAPBI/mh
```

where the WANAPBI and AHDAPBI are provided in the APB resource and the 'mh' parameter is the CDC that is to receive the message. An example message topic may appear as follows:

```
pcha/message/WANAPBI/6d296e99-e5dc-43d0-b455-7c1f3eb35d83/APS
```

I.3.4 MQTT: AHD application publishes "CONNECTED"

When all the subscriptions are completed the AHD application publishes a message on the status topic

```
pcha/status/WANAPBI/6d296e99-e5dc-43d0-b455-7c1f3eb35d83
```

with the payload "CONNECTED". At this time, the AHD application is technically able to receive commands from the WAN application. However, there is an additional requirement that the WAN application refrain from sending any messages until the AHD application enables the APS.

I.4 APS Establishment: AHD application enables APS

Enabling the APS requires that the AHD application perform a PUT operation to the URL provided in the POST response (response_URL) appended with the XPath representation of the APSState element. (e.g. created_APS_resource_URL/APSState). The mime type is set to application/text and the http body contains the text ENABLED.

The WAN application responds with success (200 OK) if it is able to change the APSState.

I.5 Operation

At this point, the AHD application can receive messages for all message strings it has subscribed handlers to receive messages for. The AHD application is able to identify which CDC the message payload is for by examining the 'mh' component of the message topic. After handling the message, the AHD application responds by publishing a response-topic message with the payload returned from the CDC (if any).

The AHD application is allowed to disconnect from the MQTT server maintaining the APS session; the APS session is still enabled but the AHD application will not be able to receive messages. The WAN application will discover that the connection is in the "CLOSED" state by the reception of a CLOSED message on the status topic. The AHD application can re-establish the connection at any time by re-invoking the MQTT connect sequence. The AHD application will publish "CONNECTED" on the status topic when it successfully establishes the MQTT client connection.

However, the more likely situation for the AHD application reconnecting is that the WAN application wakes up the AHD application using one of the mutually supported shoulder-tap mechanisms because the WAN application needs to send a message.

If there has been no activity for the APB resource for <expirationTime>, the AHD application may receive an ECHO ('APS') management message from the WAN application. The AHD application informs the WAN application that it is still alive and connected by publishing on the response topic the response to the "ECHO" command. The WAN application expects to be notified of this response within the <requiredResponseTime> specified in the APB resource. If the AHD application is not connected at the time the WAN application may choose to use the shoulder-tap process in order to re-establish transport level connectivity.

At any time the AHD application can terminate an APS by performing a PUT operation in the same manner as when it enabled the APS but in this case setting the <APSState> element value of the APB resource to TERMINATED. The AHD application terminates the APS by clearing the MQTT server of any outstanding commands and UNSUBSCRIBES to associated response and status topics. Both sides may terminate the APS for administrative (out of band) reasons.

Once terminated, the WAN application removes information that associated the APB resource with the AHD application's authentication credential so that if the AHD application initiated another APS establishment procedure with the same authentication credential, the WAN application would return NEW for the APSState element value.

Appendix II

Example WAN root.xml file

(This appendix does not form an integral part of this Recommendation.)

The following XML code is an example of a WAN root.xml file.

```
<profile>
 <!-- Specified value -->
 <id>APS-CDC-WAN</id>
 <reference>
  http://handle.itu.int/11.1002/3000/hData/APS/2015/01/H.812.4.pdf
 </reference>
</profile>

<resourceType>
 <resourceTypeId>APB</resourceTypeId>
 <!-- location of reference that describes the APS standard -->
 <reference>
  http://handle.itu.int/11.1002/3000/hData/APS/2015/01/H.812.4.pdf
 </reference>
 <representation>
  <mediaType>application/xml</mediaType>
  <!-- Schema for the APB resource xml -->
  <validator>
   http://handle.itu.int/11.1002/3000/hData/APS/2015/01/APBConfigResource.xsd
  </validator>
 </representation>
<resourceType>

<section>
 <path>APB/</path>
 <profileId>APS-CDC-WAN</profileId>
 <!-- required in this specification; optional but recommended in hData; -->
 <resourcePrefix>true</resourcePrefix>
 <resourceTypeId>APB</resourceTypeId>
</section>
```

Bibliography

See [ITU-T H.810] for a list of non-normative references and publications that contain further background information.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016