ETSI GS MEC 028 V2.1.1 (2020-06)

Multi-access Edge Computing (MEC); WLAN Information API

Disclaimer

The present document has been produced and approved by the Multi-access Edge Computing (MEC) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/MEC-0028WlanAPI

Keywords
API, MEC, service, WLAN

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Multi-access Edge Computing (MEC).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document focuses on the WLAN Information MEC service. It describes the message flows and the required information. The present document also specifies the RESTful API with the data model.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS MEC 001: "Multi-access Edge Computing (MEC); Terminology".

[2] IETF RFC 2818: "HTTP Over TLS".

NOTE: Available at https://tools.ietf.org/html/rfc2818.

[3] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

NOTE 1: Available at https://tools.ietf.org/html/rfc5246.

NOTE 2: Obsoleted by IETF RFC 8446.

[4] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

NOTE: Available at https://tools.ietf.org/html/rfc6749.

[5] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

NOTE: Available at https://tools.ietf.org/html/rfc6750.

[6] IETF RFC 6225: "Dynamic Host Configuration Protocol Options for Coordinate-Based Location Configuration Information".

NOTE: Available at https://tools.ietf.org/html/rfc6225.

[7] IETF RFC 4776: "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information".

NOTE: Available at https://tools.ietf.org/html/rfc4776.

[8] IEEE 802.11-2016™: "IEEE Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks -- Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[9] Wi-Fi Agile Multiband Specification, Version 1.4.

NOTE: Available at https://www.wi-fi.org/file/wi-fi-agile-multiband-specification.

[10] ETSI GS MEC 009: "Multi-access Edge Computing (MEC); General principles for MEC Service APIs".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS MEC 011: "Multi-access Edge Computing (MEC); Edge Platform Application Enablement".

[i.2] OpenAPI™ Specification.

NOTE 1: Available at https://github.com/OAI/OpenAPI-Specification.

NOTE 2: OpenAPI Specification and OpenAPI Initiative and their respective logos, are trademarks of the Linux Foundation.

[i.3] Wi-Fi Alliance 2014: "Hot Spot 2.0 (Release 2) Technical Specification V1.0.0".

[i.4] ETSI GS MEC 002: "Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements".

[i.5] ETSI GS MEC 003: "Multi-access Edge Computing (MEC); Framework and Reference Architecture".

[i.6] ETSI GS MEC 012: "Multi-access Edge Computing (MEC); Radio Network Information API".

[i.7] ETSI GS MEC 029: "Multi-access Edge Computing (MEC); Fixed Access Information API".

[i.8] WiFi Alliance 2019: "Data Elements Specification v1.0".

[i.9] ISO 3166: "Codes for the representation of names of countries and their subdivisions".

[i.10] IEEE 802.11ax™: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 1: Enhancement for High Effficiency WLAN".

[i.11] IEEE P802.11ay™ D4.0: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 1: Enhancement for High Effficiency WLAN - Amendment 2: Enhanced throughput for operation in license-exempt bands above 45 GHz".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS MEC 001 [1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS MEC 001 [1] and the following apply:

3GPP	3rd Generation Partnership Project
AID	Association Identifier
AP	Access Point
API	Application Programming Interface
ASEL	Antenna Selection
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
DMG	Directional Multi-Gigabit

NOTE: As in Directional Multi-Gigabit WLAN.

EDMG	Enhanced Directional Multi-Gigabit

NOTE: As in Enhanced Directional Multi-Gigabit WLAN.

HE	High Efficiency

NOTE: As in High Efficiency WLAN.

HT	High Throughput

NOTE: As in High Throughput WLAN.

ID	Identifier
LMD	Load Measurement Duration
MAC	Medium Access Control
MCS	Modulation and Coding Scheme
MD	Measurement Duration
MIMO	Multiple-Input Multiple-Output
MPDU	MAC protocol Data Unit
NSS	Number of Spatial Streams
PHY	Physical layer
RSSI	Receive Signal Strength Indicator
SSID	Service Set Identifier
STA	Station
URI	Uniform Resource Identifier
VHT	Very High Throughput

NOTE: As in Very High Throughput WLAN.

WAI	WLAN Access Information
WAIS	WLAN Access Information Service
WLAN	Wireless Local Area Network

4 Overview

The present document specifies the WLAN Access Information (WAI) API to support the requirements defined for Multi-access Edge Computing in ETSI GS MEC 002 [i.4].

Clause 5 provides overview how WLAN Access Information Service (WAIS) may be used by the MEC applications and by the MEC platform. It describes the information flows used for WLAN Access Information Service.

The information that can be exchanged over the WAI API is described in clause 6 which provides detailed description on all information elements that are used for WLAN Access Information.

Clause 7 describes the actual WAI API providing detailed information how information elements are mapped into a RESTful API design.

5 Description of the service (informative)

5.1 WLAN Access Information Service introduction

Multi-access Edge Computing allows running the MEC applications at the edge of the network where the environment is characterized by low latency, proximity, high bandwidth and exposure to location and up-to-date information from the underlying access networks. The information on current conditions from the WLAN access is shared via WLAN Access Information Service.

WLAN Access Information Service (WAIS) is a service that provides WLAN access related information to service consumers within MEC System. The WLAN Access Information Service is available for authorized MEC applications and is discovered over the Mp1 reference point as specified in ETSI GS MEC 003 [i.5]. The granularity of the WLAN Access Information may be adjusted based on parameters such as information per station (STA), per Access Point (AP) or per Multiple Access Points (Multi-AP).

The WLAN Access Information may be used by the MEC applications and MEC platform to optimize the existing services and to provide new type of services that are based on up to date information from WLAN access possibly combined with the information such as Radio Network Information as specified in ETSI GS MEC 012 [i.6] or Fixed Access Network Information as specified in ETSI GS MEC 029 [i.7] from the other access technologies.

The present document defines the protocol, data model and interface in the form of RESTful Application Programming Interface (APIs) specifications. Information about the Access Points and client stations can be requested either by querying or by subscribing to notifications.

The procedures defined for queries are flexible and cater wide set of use cases from simple queries to queries requesting wide set of information on targets. This flexibility is enabled with concepts of attribute-based filtering and attribute selectors, as specified in ETSI GS MEC 009 [10], and those are described in more detail in clauses 6.18 and 6.19 of ETSI GS MEC 009 [10].

5.2 Sequence diagrams

5.2.1 Introduction

The service consumers communicate with WLAN Access Information Service over WAI API to get contextual information from the WLAN access network. Both the MEC application and MEC platform may be service consumers and both the MEC platform and MEC application may be providers of WLAN Access Information.

The WAI API supports both queries and subscriptions (pub/sub mechanism) over the RESTful API or over alternative transports such as message bus. Alternative transports are not specified in detail in the present document. When queries are used, the attribute-based filter expression can be used to limit the number of objects returned by query operation and attribute-selectors can be used to limit the number of attributes included in the response.

For RESTful architectural style, the present document defines the HTTP protocol bindings.

5.2.2 Sending a query for Access Point information

5.2.2.1 General query procedure

Figure 5.2.2.1-1 shows a scenario where the service consumer (e.g. a MEC application or a MEC platform) sends a query to receive information about Access Points (AP). The response may contain information on one or more access points. The number of queried objects and desired contents can be controlled with an attribute-based filter expression and attribute-selectors as defined in ETSI GS MEC 009 [10].

Figure 5.2.2.1-1: Flow of service consumer querying Access Point information

A service consumer requesting Access Point information, as illustrated in Figure 5.2.2.1-1, consists of the following steps:

1) Service consumer sends a GET request to the resource representing the Access Point(s) information. The request may contain attribute-filter to limit the number of Access Points whose information is received and attribute-selector to limit the number of attributes included in the response.

2) WAIS responds with "200 OK" with the message body containing the requested Access Point information.

5.2.2.2 Sending a query for a list of Access Points

A list of Access Points available in the system can be queried with the flow as in Figure 5.2.2.1-1 by using the attribute selector as follows:

GET …/queries/ap?fields=apId

5.2.2.3 Sending a query for WLAN capabilities

The WLAN Capabilities of Access Points can be queried with the flow of Figure 5.2.2.1-1 by using the attribute selector as follows:

GET …/queries/ap?fields=apId,wlanCap

The above query, if successful, would return the identifiers of Access Points available together with their WLAN Capabilities.

As an example, the WLAN Capabilities of the Access Point with an apId equal to "admiralsclub" can be queried using the attribute selector and filter attribute as follows:

GET …/queries/ap?filter=(eq,apId,admiralsclub)&fields=apId,wlanCap

5.2.2.4 Sending a query for BSS Load

The BSS Load of an Access Point can be queried with the flow of Figure 5.2.2.1-1 by using the attribute selector and filter attribute (in this instance the Access Point with apId equal to "admiralsclub") as follows:

GET …/queries/ap?filter=(eq,apId,admiralsclub)&fields=apId,bssLoad

More accurate information about BSS Load, for the same Access Point, can be obtained by adding the attribute "extBssLoad" in the list of requested fields as follows:

GET …/queries/ap?filter=(eq,apId,admiralsclub)&fields=apId,bssLoad,extBssLoad

5.2.2.5 Sending a query for WAN metrics

The WAN metrics of an Access Point can be queried with the flow of Figure 5.2.2.1-1 by using the attribute selector and filter attribute (in this instance the Access Point with apId equal to "admiralsclub") as follows:

GET …/queries/ap?filter=(eq,apId,admiralsclub)&fields=apId,wanMetrics

5.2.2.6 Sending a query for AP Location

The location of an Access Point can be queried with the flow of Figure 5.2.2.1-1 by using the attribute selector and filter attribute (in this instance the Access Point with apId equal to "admiralsclub") as follows:

GET …/queries/ap?filter=(eq,apId,admiralsclub)&fields=apId,apLocation

5.2.2.7 Sending a query for AP Neighbor report

The neighbour report of an Access Point can be queried with the flow of Figure 5.2.2.1-1 by using the attribute selector and filter attribute (in this instance the Access Point with apId equal to "admiralsclub") as follows:

GET …/queries/ap?filter=(eq,apId,admiralsclub)&fields=apId,apNeighbor

5.2.3 Sending a query for Station information

5.2.3.1 General query procedure

Figure 5.2.3.1-1 shows a scenario where the service consumer (e.g. a MEC application or a MEC platform) sends a request to receive information about client station(s). The response may contain information on one or more stations and the number of queried objects and desired contents can be controlled with attribute-based filtering and attribute-selectors as defined in ETSI GS MEC 009 [10].

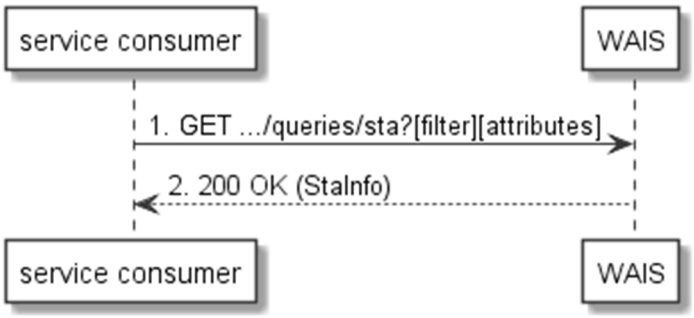

Figure 5.2.3.1-1: Flow of service consumer querying station Info

A service consumer requesting client station information, as illustrated in Figure 5.2.3.1-1, consists of the following steps:

1) Service consumer sends a GET request to the resource representing the station(s) information. The request may contain attribute-filters to limit the number of client stations whose information is received and attribute-selectors to limit the number of attributes included in the response.

2) WIS responds with "200 OK" with the message body containing the requested WLAN station information.

5.2.3.2 Sending a query for a list of stations

A list of stations available in the system can be queried with the flow as in Figure 5.2.3.1-1 by using the attribute selector as follows:

GET …/queries/sta?fields=staId

The above query, if successful, would return the identities of all the stations that are known to be associated in the system. Information about the Access Points that the stations are associated to can be queried as follows:

GET …/queries/sta?fields=staId,apAssociated

Further, to get the stations associated to a particular Access Point, the following query can be used including the attribute selector and filter attribute (in this instance the stations associated to Access Point with apAssociated equal to "mec123"):

GET …/queries/sta?filter=(eq,apAssociated,mec123)&fields=staId,apAssociated

5.2.3.3 Sending a query for channel used by station(s)

The channel used by stations can be queried with the flow of Figure 5.2.3.1-1 by using the attribute selector as follows:

GET …/queries/sta?fields=staId,channel

5.2.3.4 Sending a query for RSSI of station(s)

The RSSI value of stations can be queried with the flow of Figure 5.2.3.1-1 by using the attribute selector as follows:

GET …/queries/sta?fields=staId,rssi

The results can be narrowed down to stations under specific Access Point by adding filter attribute (in this instance the Access Point with apId equal to "mec123") to the query as follows:

GET …/queries/sta?filter=(eq,apAssociated,mec123)&fields=staId,rssi

5.2.3.5 Sending a query for station data rates

The physical layer data rate of stations can be queried with the flow of Figure 5.2.3.1-1 by using the attribute selector as follows:

GET …/queries/sta?fields=staId,staDataRate

As there may be great number of stations in the system, it may be practical to limit the query to consider either stations under specific Access Point or certain specific station by including the attribute filter:

GET …/queries/sta?filter=(eq,apAssociated,mec404)&fields=staId,staDataRate

GET …/queries/sta?filter=(eq,staId,C8:D0:66:08:B6:0F)&fields=staId,staDataRate

5.2.3.6 Sending a query for station statistics

The statistics of stations can be queried with the flow of Figure 5.2.3.1-1 by using the attribute selector as follows:

GET …/queries/sta?fields=staId,staStatistics

As there may be great number of stations in the system, it may be practical to limit the query to consider either stations under specific Access Point or certain specific station by including the attribute filter:

GET …/queries/sta?filter=(eq,apAssociated,mec404)&fields=staId,staStatistics

GET …/queries/sta?filter=(eq,staId,C8:D0:66:08:B6:0F)&fields=staId,staStatistics

5.2.4 REST based subscribe-notify model

5.2.4.1 Subscribing to WLAN event notifications

To receive notifications on selected WLAN events, the service consumer creates a subscription to certain specific event that is available at WAIS. Figure 5.2.4.1-1 shows a scenario where the service consumer uses REST based procedures to create a subscription for WLAN event notifications.

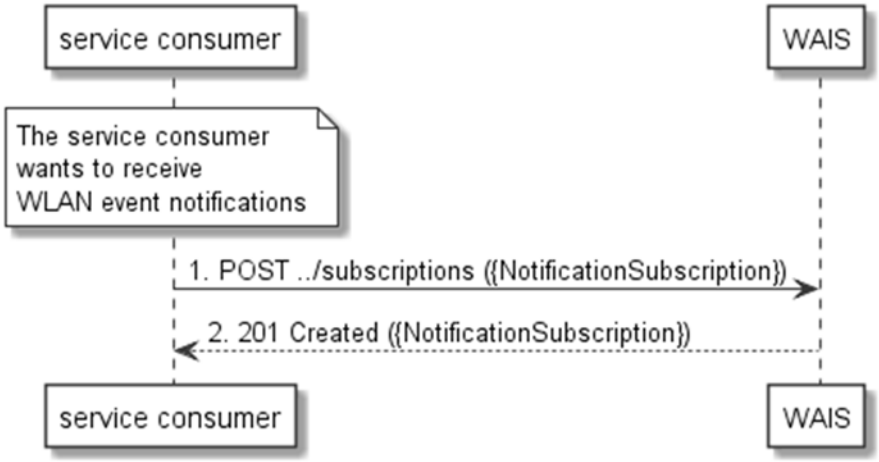

Figure 5.2.4.1-1: Flow of subscribing to WLAN event notifications

Subscribing to the WLAN event notifications, as illustrated in Figure 5.2.4.1-1, consists of the following steps.

When the service consumer wants to receive notifications about the WLAN events, it creates a subscription to the WLAN event notifications:

1) The service consumer sends a POST request with the message body containing the {NotificationSubscription} data structure The variable {NotificationSubscription} is replaced with the data type specified for different WLAN event subscriptions as specified in clauses 6.3.2 and 6.3.3, and it defines the subscribed event, the filtering criteria and the address where the service consumer wishes to receive the WLAN event notifications.

2) WIS sends "201 Created" response with the message body containing the data structure specific to that WLAN event subscription. The data structure contains the address of the resource created and the subscribed WLAN event type.

5.2.4.2 Receiving notification on expiry of WLAN event subscription

WAIS may define an expiry time for the WLAN event subscription. In case expiry time is used, the time will be included in the {NotificationSubscription} data structure that is included in the response message to the subscription. Prior the expiry, WAIS will also send a notification to the service consumer that owns the subscription.

Figure 5.2.4.2-1 shows a scenario where the service consumer receives a subscription expiry notification for the existing subscription.

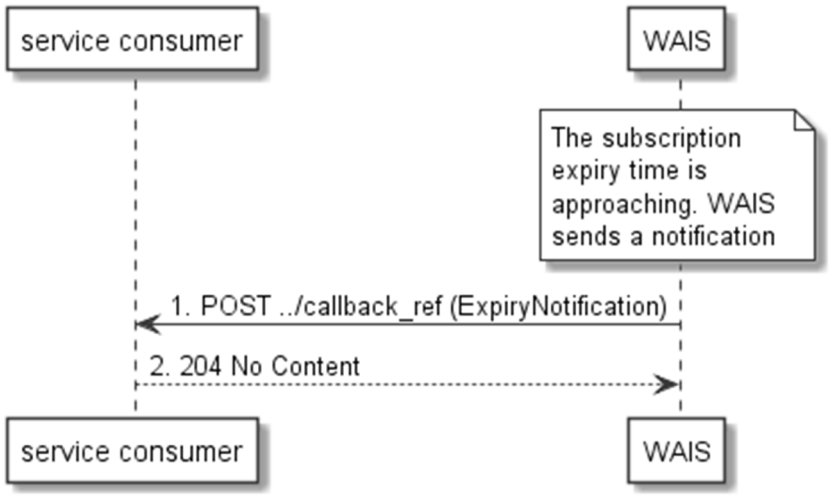

Figure 5.2.4.2-1: Flow of WIS sending a notification on expiry of the subscription

Sending a notification on expiry of the subscription, as illustrated in Figure 5.2.4.2-1 consists of the following steps. If WAIS has defined an expiry time for the subscription, WAIS will send a notification prior the expiry:

1) WAIS sends a POST request to the callback reference address included by the service consumer in the subscription request. The POST request contains a data structure ExpiryNotification.

2) Service consumer sends a "204 No Content" response.

5.2.4.3 Updating subscription for WLAN event notifications

Figure 5.2.4.3-1 shows a scenario where the service consumer needs to update an existing subscription for a WLAN event notification. The subscription update is triggered e.g. by the need to change the existing subscription, or due to the expiry of the subscription.

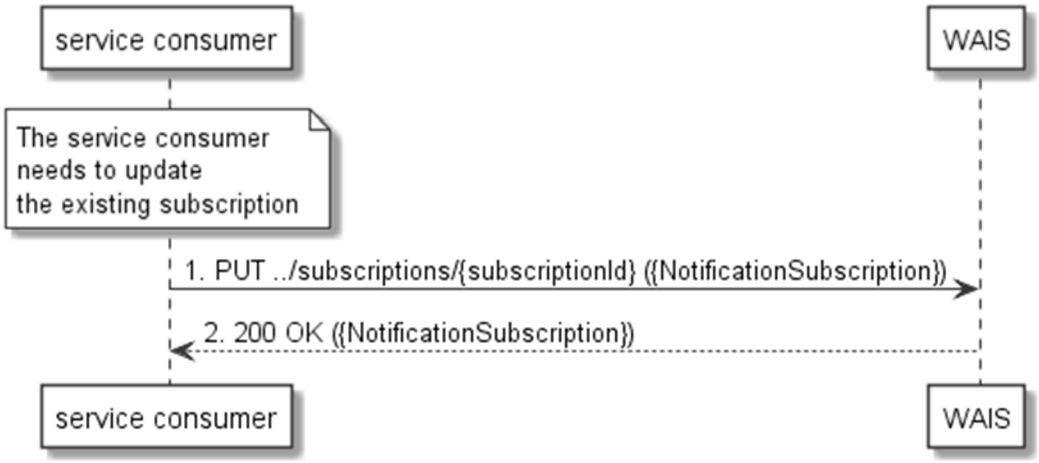

Figure 5.2.4.3-1: Flow of service consumer updating subscription for WLAN event notifications

Updating subscription for WLAN event notifications, as illustrated in Figure 5.2.4.3-1, consists of the following steps.

When the service consumer needs to modify an existing subscription for WLAN event notifications, it can update the corresponding subscription as follows:

1) Service consumer updates the subscription resource by sending a PUT request to the resource containing all the subscriptions with the modified data structure specific to that WLAN event subscription.

2) WAIS returns "200 OK" with the message body containing the accepted data structure specific to that WLAN event subscription.

5.2.4.4 Unsubscribing from WLAN event notifications

When the service consumer does not want to receive notifications anymore after subscribing to WLAN events, the service consumer unsubscribes from the WLAN event notifications. Figure 5.2.4.4-1 shows a scenario where the service consumer uses REST based procedures to delete the subscription for WLAN event notifications.

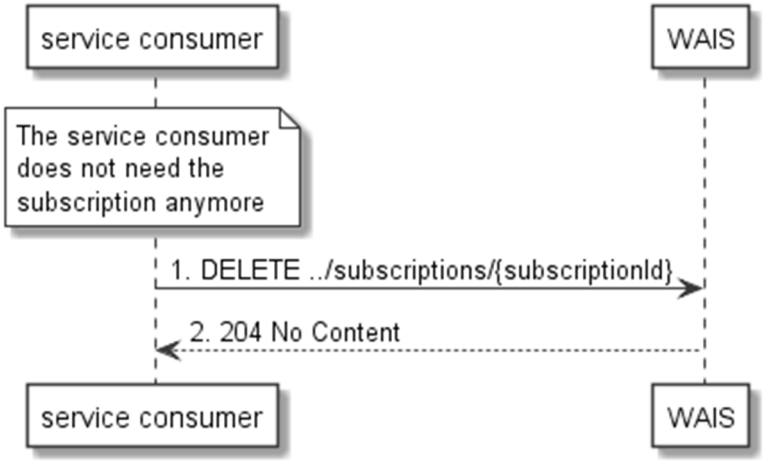

Figure 5.2.4.4-1: Flow of unsubscribing from the WLAN event notifications

Unsubscribing from the WLAN event notifications, as illustrated in Figure 5.2.4.4-1, consists of the following steps:

When the service consumer does not want to receive the notifications anymore, it can unsubscribe from the WLAN notification events by deleting the subscription:

1) Service consumer sends a DELETE request to the resource representing the WLAN event subscription that was created.

2) WIS sends "204 No content" response.

5.2.5 Receiving WLAN event notifications about station data rates

Figure 5.2.5-1 presents the scenario where the WAIS sends WLAN event notifications about WLAN station data rates, as defined in IEEE 802.11-2016 [8], to the service consumer.

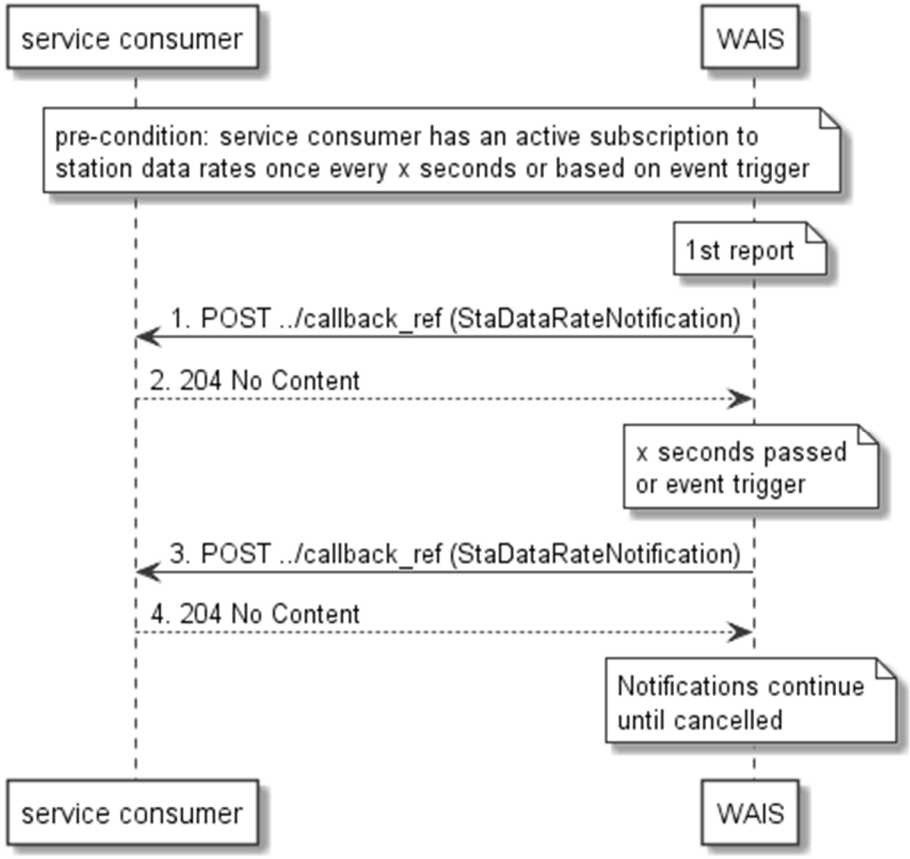

Figure 5.2.5-1: Flow of receiving WLAN event notifications on station data rates

Receiving WLAN event notifications on station data rates, as illustrated in Figure 5.2.5-1, consists of the following steps:

1) WAIS sends a POST request with the message body containing the StaDataRatesNotification data structure to the callback reference address included by the service consumer in the station data rates event subscription.

2) Service consumer sends a "204 No Content" response to the WAIS.

5.2.6 Receiving WLAN event notifications about associated stations

Figure 5.2.6-1 presents the scenario where the WAIS sends WLAN event notifications about WLAN stations that are associated with a particular access point, as defined in IEEE 802.11-2016 [8], whose information is requested.

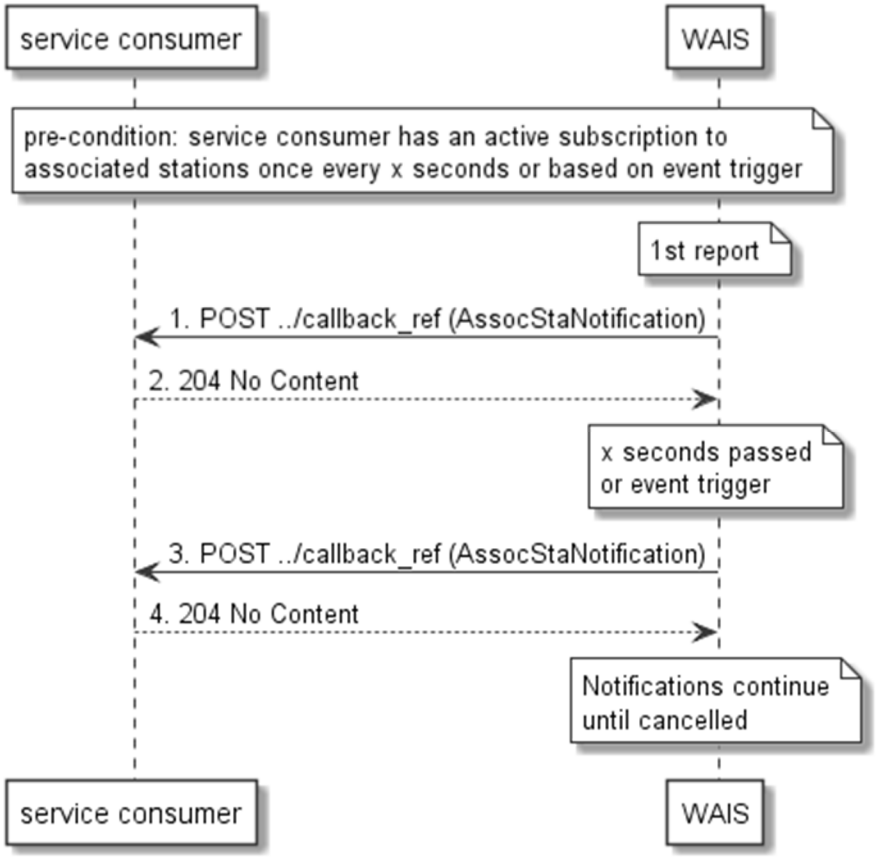

Figure 5.2.6-1: Flow of receiving WLAN event notifications on associated stations

Receiving WLAN event notifications on stations associated with the access points, as illustrated in Figure 5.2.6-1, consists of the following steps:

1) WAIS sends a POST request with the message body containing the AssocStaNotification data structure to the callback reference address included by the service consumer in the WLAN event subscription.

2) Service consumer sends a "204 No Content" response to the WAIS.

5.2.7 Measurement Configuration

5.2.7.1 Creating a Measurement configuration

To configure specific characteristics of the Beacon Request or STA statistics measurements, the service consumer (e.g. a MEC application or a MEC platform) creates a new measurement configuration by providing (by a POST) the configuration and receiving an identifier of the configuration to be used in the measurement request. Figure 5.2.7.1-1 shows a scenario where the service consumer uses REST based procedures to create a new measurement configuration.

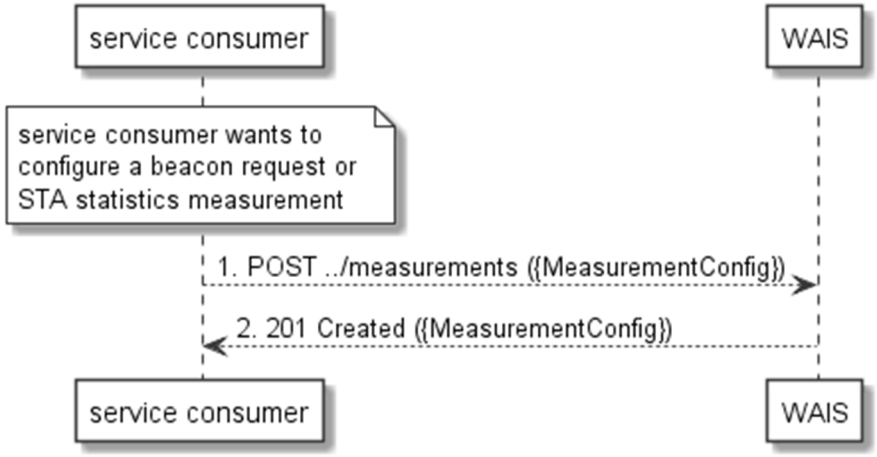

Figure 5.2.7.1-1: Flow of service consumer creating a measurement configuration

A service consumer requesting a certain measurement through the Beacon Request of STA statistics, consists of the following steps:

1) Service consumer configures measurement by creating a new measurement configuration MeasurementConfig, which includes measurementId, by sending a POST request to WIS.

2) WIS responds with a "201 Created", with the message body including the accepted MeasurementConfig structure.

3) Service consumer includes the measurementId in the attributes of the query to get specific information such as the staStatistics of the StaInfo resource data type or the apNeighbor of the ApInfo resource data type.

5.2.7.2 Updating a Measurement Configuration

Figure 5.2.7.2-1 shows a scenario where the service consumer needs to update an existing Measurement Configuration. The update is triggered e.g. by the need to change the existing measurement to a different channel or station.

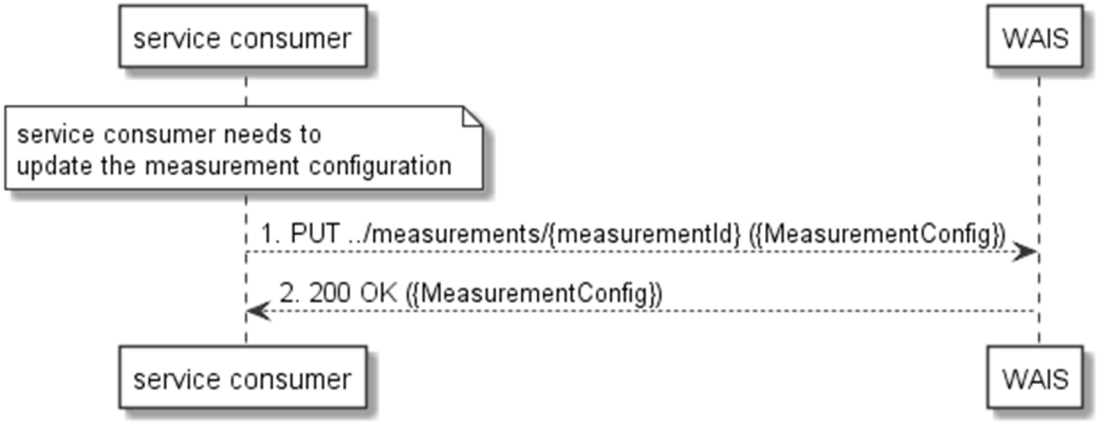

Figure 5.2.7.2-1: Flow of service consumer updating a measurement configuration

Updating subscription for WLAN event notifications, as illustrated in Figure 5.2.7.2-1, consists of the following steps.

When the service consumer needs to modify an existing measurement for WLAN, it can update the corresponding measurement as follows:

1) Service consumer updates the measurement configuration by sending a PUT request to the resource (i.e. MeasurementConfig) containing all the measurement configurations with the modified data structure specific to that WLAN measurement configuration.

2) WIS returns "200 OK" with the message body containing the accepted data structure (i.e. MeasurementConfig) specific to that WLAN measurement configuration.

5.2.7.3 Deleting a Measurement Configuration

When the service consumer does not want to use a measurement configuration anymore, the service consumer DELETES the Measurement Configuration. Figure 5.2.7.3-1 shows a scenario where the service consumer uses REST based procedures to delete the Measurement Configuration.

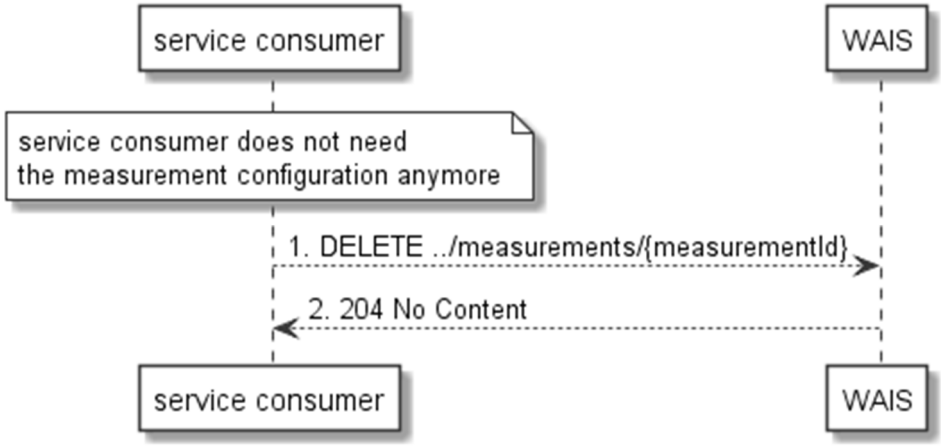

Figure 5.2.7.3-1: Flow of deletion of a Measurement Configuration

Deletion of a Measurement Configuration, as illustrated in Figure 5.2.7.3-1, consists of the following steps:

When the service consumer does not want to use the measurement configuration anymore, it can delete it:

1) Service consumer sends a DELETE request to the resource representing the WLAN measurement configuration that was created.

2) WIS sends "204 No content" response.

5.2.7.4 Example of using a Measurement Configuration

Once configured, a measurementId can be used as an attribute to any query for measurement, such as ApInfo or StaInfo. In the following diagram, the flow that can be used for StaInfo is shown.

Figure 5.2.7.4-1: Use of measurementId as a query attribute to StaInfo

6 Data Model

6.1 General

The following clauses provide the description of the data model.

6.2 Resource data types

6.2.1 Introduction

This clause defines data structures that shall be used in resource representations.

6.2.2 Type: ApInfo

This type represents the information on Access Points available from the WLAN Access Information Service.

The attributes of the ApInfo shall follow the notations provided in Table 6.2.2-1.

Table 6.2.2-1 Attributes for ApInfo

Attribute name	Data type	Cardinality	Description
timeStamp	TimeStamp	0..1	Time stamp.
apId	ApIdentity	1	Identifier(s) to uniquely specify the Access Point whose information is exposed within this data type.
channel	Uint32	0..1	Channel configured for the Access Point.
wlanCap	WlanCapabilities	0..1	WLAN capabilities of Access Point.
wanMetrics	WanMetrics	0..1	WAN Metrics element provides information about the WAN link connecting an IEEE 802.11 Access Node and the Internet. Transmission characteristics such as the speed of the WAN connection to the Internet are included in Hotspot 2.0 Technical Specification v1.0.0 [i.3].
bssLoad	BssLoad	0..1	BSS Load attribute contains information on the current STA population and traffic levels in the BSS as defined in IEEE 802.11-2016 [8].
extBssLoad	ExtBssLoad	0..1	Extended BSS Load attribute contains more detailed information on the current STA population and traffic levels in the BSS as per ETSI GS MEC 002 [i.4].
apLocation	ApLocation	0..1	The location on the Access Point.
apNeighbor	NeighborReport	0..1	Information about neighbor Access Points.

6.2.3 Type: StaInfo

This type represents the information on wireless stations available from the WLAN Access Information Service.

The attributes of the StaInfo shall follow the notations provided in Table 6.2.3-1.

Table 6.2.3-1 Attributes for StaInfo

Attribute name	Data type	Cardinality	Description
timeStamp	TimeStamp	0..1	Time stamp.
staId	StaIdentity	1	0 to N identifiers to uniquely specify the station whose information is exposed within this data type.
channel	Uint32	0..1	Channel currently used by the station.
apAssociated	ApAssociated	0..1	Information about the Access Point that this Client Station is associated to.
rssi	Rssi	0..1	Receive Signal Strength Indicator.
staDataRate	StaDataRate	0..1	Station Data Rate as defined in IEEE 802.11-2016 [8].
staStatistics	StaStatistics	0..1	Statistics as defined in IEEE 802.11-2016 [8] for the client station collected over measurement duration.
beaconReport	BeaconReport	0..1	Beacon Report as defined in Wi-Fi Agile Multiband Specification [9].

6.2.4 Type: MeasurementConfig

This type represents the different measurements configuration available from the WLAN Access Information Service.

The attributes of the MeasurementConfig shall follow the notations provided in Table 6.2.4-1.

Table 6.2.4-1: Attributes for MeasurementConfig

Attribute name	Data type	Cardinality	Description
measurementId	String	1	Identifier of this measurement configuration.
measurementDuration	Integer	1	Duration of the measurement, shall be lower than Maximum Measurement Duration in TU as defined in section 11.11.4 of IEEE 802.11 [8].
randomnInterval	Integer	1	Random interval to be used for starting the measurement. In units of TU as specifed in section 11.11.3 of IEEE 802.11 [8].
channelLoad	ChannelLoadConfig	0..1	Configuration related to the Channel Load.
beaconRequest	BeaconRequestConfig	0..1	Configuration related to Beacon Request.
staStatistics	StaStatisticsConfig	0..1	Configuration related to the statistics provided by STAs.
NOTE: This element enables the configuration of the channelLoad, beaconRequest and staStatistics in a single resource data type, although only one of each measurement. Multiple measurement configurations of each kind are not allowed.			

6.3 Subscription data types

6.3.1 Introduction

This clause defines data structures for subscriptions.

6.3.2 Type: AssocStaSubscription

This type represents a subscription to get updates on client stations that are associated to an Access Point.

Table 6.3.2-1: Attributes of the AssocStaSubscription

Attribute name	Data type	Cardinality	Description
subscriptionType	String	1	Shall be set to "AssocStaSubscription".
callbackReference	URI	1	URI selected by the service consumer to receive notifications on the subscribed WLAN information. This shall be included both in the request and in response.
_links	Structure (inlined)	0..1	Hyperlink related to the resource. This shall be only included in the HTTP responses and in HTTP PUT requests.
>self	LinkType	1	Self referring URI. The URI shall be unique within the WLAN information API as it acts as an ID for the subscription.
apId	ApIdentity	1	Identifier(s) to uniquely specify the target Access Point for the subscription
expiryDeadline	TimeStamp	0..1	The expiration time of the subscription determined by the WLAN Access Information Service.

6.3.3 Type: StaDataRateSubscription

This type represents a subscription to get updates on the Data Rate of targeted client station(s).

Table 6.3.3-1: Attributes of the StaDataRateSubscription

Attribute name	Data type	Cardinality	Description
subscriptionType	String	1	Shall be set to "StaDataRateSubscription".
callbackReference	URI	1	URI selected by the service consumer to receive notifications on the subscribed WLAN Access Information Service. This shall be included both in the request and in response.
_links	Structure (inlined)	0..1	Hyperlink related to the resource. This shall be only included in the HTTP responses and in HTTP PUT requests.
>self	LinkType	1	Self referring URI. The URI shall be unique within the WLAN Access Information API as it acts as an ID for the subscription.
staId	StaIdentity	1..N	Identifier(s) to uniquely specify the target client station(s) for the subscription
expiryDeadline	TimeStamp	0..1	The expiration time of the subscription determined by the WLAN Access Information Service.

6.4 Notifications data types

6.4.1 Introduction

This clause defines data structures that define notifications.

6.4.2 Type: AssocStaNotification

This type represents a notification from WLAN Access Information Service with regards to client stations associated to the targeted Access Point.

The attributes of the AssocStaNotification shall follow the indications provided in Table 6.4.2-1.

Table 6.4.2-1: Attributes of the AssocStaNotification

Attribute name	Data type	Cardinality	Description
notificationType	String	1	Shall be set to "AssocStaNotification".
timeStamp	TimeStamp	0..1	Time stamp.
apId	ApIdentity	1	Identifier(s) to uniquely specify the Access Point to which the client stations are associated.
staId	StaIdentity	0..N	Identifier(s) to uniquely specify the client station(s) associated.

6.4.3 Type: StaDataRateNotification

This type represents a notification from WLAN Information service with regards to Data Rates of the subscribed client stations.

The attributes of the StaDataRateNotification shall follow the indications provided in Table 6.4.3-1.

Table 6.4.3-1: Attributes of the StaDataRateNotification

Attribute name	Data type	Cardinality	Description
notificationType	String	1	Shall be set to "StaDataRateNotification".
timeStamp	TimeStamp	0..1	Time stamp.
staDataRate	StaDataRate	0..N	Data rates of a client station.

6.5 Referenced structured data types

6.5.1 Introduction

This clause defines data structures that are referenced from data structures defined in the previous clauses, but are neither resource representations nor bound to any pub/sub mechanism.

6.5.2 Type: TimeStamp

This type represents a time stamp.

Table 6.5.2-1: Attributes of the TimeStamp

Attribute name	Data type	Cardinality	Description
seconds	Uint32	1	The seconds part of the time. Time is defined as Unix-time since January 1, 1970, 00:00:00 UTC.
nanoSeconds	Uint32	1	The nanoseconds part of the time. Time is defined as Unix-time since January 1, 1970, 00:00:00 UTC.

6.5.3 Type: ApIdentity

This type represents identifiers determining a specific Access Point.

Table 6.5.3-1: Attributes of the ApIdentity

Attribute name	Data type	Cardinality	Description
macId	String	1	Unique Identifier assigned to an Access Point (as network interface controller) for communications at the data link layer of a network segment.
ssid	String	0..N	Service Set Identifier to identify logical networks including Basic Service Set and Extended Service Set.
ipAddress	String	0..N	IPv4 or IPv6 address allocated for the Access Point.

6.5.4 Type: WlanCapabilities

This type represents the WLAN capabilities of the Access Point.

Table 6.5.4-1: Attributes of the WlanCapabilities

Attribute name	Data type	Cardinality	Description
ht	HtCapabilities	0..1	Information about Access Point HT capabilities as defined in IEEE 802.11-2016 [8].
vht	VhtCapabilities	0..1	Information about Access Point VHT capabilities as defined in IEEE 802.11-2016 [8].
he	HeCapabilities	0..1	Information about Access Point HE capabilities as defined in FFS.
dmg	DmgCapabilities	0..1	Information about Access Point DMG capabilities as defined in IEEE 802.11-2016 [8].
edmg	EdmgCapabilities	0..1	Information about Access Point EDMG capabilities as defined in draft IEEE P802.11/D4.0 [i.11].

6.5.5 Type: AssociatedStations

This type represents the stations that are associated with the Access Point.

Table 6.5.5-1: Attributes of the AssociatedStations

Attribute name	Data type	Cardinality	Description
macId	string	1	Unique identifier assigned to a station (as network interface controller) for communications at the data link layer of a network segment.
assocId	string	0..1	Unique number which identifies a particular association between an Access Point and a station.
ipAddress	string	0..N	IPv4 or IPv6 address allocated for the station associated with the Access Point.

6.5.6 Type: WanMetrics

This type represents the metrics related to the backhaul characteristics of an Access Point as defined for WAN metrics in Hotspot 2.0 Technical Specification v1.0.0 [i.3].

Table 6.5.6-1: Attributes of the WanMetrics

Attribute name	Data type	Cardinality	Description
wanInfo	Uint8	1	Info about WAN link status, link symmetricity and capacity currently used.
downlinkSpeed	Uint32	1	4-octet positive integer whose value is an estimate of the WAN Backhaul link current downlink speed in kilobits per second.
uplinkSpeed	UInt32	1	4-octet positive integer whose value is an estimate of the WAN Backhaul link's current uplink speed in kilobits per second.
downlinkLoad	UInt8	1	1-octet positive integer representing the current percentage loading of the downlink WAN connection, scaled linearly with 255 representing 100 %, as measured over an interval the duration of which is reported in Load Measurement Duration. In cases where the downlink load is unknown to the AP, the value is set to zero.
uplinkLoad	Uint8	1	1-octet positive integer representing the current percentage loading of the uplink WAN connection, scaled linearly with 255 representing 100 %, as measured over an interval, the duration of which is reported in Load Measurement Duration. In cases where the uplink load is unknown to the AP, the value is set to zero.
lmd	Uint16	1	The LMD (Load Measurement Duration) field is a 2-octet positive integer representing the duration over which the Downlink Load and Uplink Load have been measured, in tenths of a second. When the actual load measurement duration is greater than the maximum value, the maximum value will be reported. The value of the LMD field is set to 0 when neither the uplink nor downlink load can be computed. When the uplink and downlink loads are computed over different intervals, the maximum interval is reported.

6.5.7 Type: BssLoad

This type represents the load of a BSS as defined in IEEE 802.11-2016 [8].

Table 6.5.7-1: Attributes of the BssLoad

Attribute name	Data type	Cardinality	Description
staCount	UInt16	1	An unsigned integer that indicates the total number of STAs currently associated with this BSS.
channelUtilization	UInt8	1	The percentage of time, linearly scaled with 255 representing 100 %, that the AP sensed the medium was busy, as indicated by either the physical or virtual Carrier Sense (CS) mechanism.
availAdmCap	Uint16	1	Available Admission Capacity that specifies the remaining amount of medium time available via explicit admission control, in units of 32 μs/s.

6.5.8 Type: ExtBssLoad

This type represents the Extended BSS Load information as defined in IEEE 802.11-2016 [8].

Table 6.5.8-1: Attributes of the ExtBssLoad

Attribute name	Data type	Cardinality	Description
muMimoStaCount	UInt16	1	Indicates the total number of STAs currently associated with this BSS that have a 1 in the MU Beamformee Capable field of their VHT Capabilities element.
spatStreamUnderUtil	UInt8	1	The percentage of time, linearly scaled with 255 representing 100 %, that the AP has underutilized spatial domain resources for given busy time of the medium.
obsSec20MhzUtil	Uint8	1	Observable loading on each of the secondary 20 MHz channel.
obsSec40MhzUtil	Uint8	1	Observable loading on each of the secondary 40 MHz channel.
obsSec80MhzUtil	Uint8	1	Observable loading on each of the secondary 80 MHz channel.

6.5.9 Type: ApLocation

This type represents the location information of the Access Point as defined in IEEE 802.11-2016 [8].

Table 6.5.9-1: Attributes of the ApLocation

Attribute name	Data type	Cardinality	Description
geolocation	GeoLocation	0..1	Geospatial Location of the AP as defined in IEEE 802.11-2016 [8].
civicLocation	CivicLocation	0..1	Civic Location of the AP as described in IETF RFC 4776 [7].

6.5.10 Type: NeighborReport

This type represents the information about neighbor Access Points as defined in IEEE 802.11-2016 [8].

Table 6.5.10-1: Attributes of the NeighborReport

Attribute name	Data type	Cardinality	Description
bssid	String	1	BSS Id of the Access Point that is being reported.
bssidInfo	UInt32	1	Additional information related to Access Point that is being reported such as AP reachability, security, key scope, Mobility Domain, HT/VHT capability and Fine Time Measurements.
operatingClass	Uint8	1	The channel set of the AP indicated by this BSSID.
channel	Uint8	1	The channel currently used by this Access Point.
phyType	Uint8	1	PHY type of the AP indicated by this BSSID. It is an integer value coded according to the value of the dot11PHYType.
optionalSubelements	not specified	0..N	Optional subelements as described in IEEE 802.11-2016 [8].

6.5.11 Type: StaIdentity

This type represents identifiers determining a specific client station.

Table 6.5.11-1: Attributes of the StaIdentity

Attribute name	Data type	Cardinality	Description
macId	String	1	Unique identifier assigned to station (as network interface controller) for communications at the data link layer of a network segment.
ssid	String	0..N	Service Set Identifier to identify logical networks.
aid	String	0..1	Number which identifies a particular association between a station and an Access Point
ipAddress	String	0..N	IPv4 or IPv6 address allocated for the station.

6.5.12 Type: ApAssociated

This type represents information for the Access Point that the client station is associated to.

Table 6.5.12-1: Attributes of the ApAssociated

Attribute name	Data type	Cardinality	Description
macId	string	1	Unique identifier assigned to the Access Point (as network interface controller) for communications at the data link layer of a network segment.
ssid	String	0..N	Service Set Identifier to identify logical networks.
assocId	string	0..1	Unique number which identifies a particular association between the station and Access Point.
ipAddress	string	0..N	IPv4 or IPv6 address allocated for the Access Point.

6.5.13 Type: StaStatistics

This type represents information statistics of the client station as defined in IEEE 802.11-2016 [8].

Table 6.5.13-1: Attributes of the StaStatistics

Attribute name	Data type	Cardinality	Description
md	UInt16	1	Measurement Duration.
groupIdentity	UInt8	1	Indicates the requested statistics group describing the Statistics Group Data according to table 9-114 of IEEE 802.11-2016 [8].
statisticsGroupData	not specified	1	Statistics Group Data as defined in Annex C of IEEE 802.11-2016 [8].
optionalSubelements	not specified	0..N	Optional subelements as described in IEEE 802.11-2016 [8].

6.5.14 Type: HtCapabilities

This type represents information on HT capabilities of an Access Point as defined in IEEE 802.11-2016 [8].

Table 6.5.14-1: Attributes of the HtCapabilities

Attribute name	Data type	Cardinality	Description
htCapabilityInfo	UInt16	1	HT Capability Information as defined in IEEE 802.11-2016 [8].
ampduParameters	UInt8	1	A-MPDU parameters as defined in IEEE 802.11-2016 [8].
supportedMcsSet	Uint128	1	Supported MCS set as defined in IEEE 802.11-2016 [8].
htExtendedCap	UInt16	1	Extended HT Capabilities as defined in IEEE 802.11-2016 [8].
txBeamFormCap	UInt32	1	Transmit Beamforming Capabilities as defined in IEEE 802.11-2016 [8].
aselCap	UInt8	1	ASEL capabilities as defined in IEEE 802.11-2016 [8].

6.5.15 Type: VhtCapabilities

This type represents information on VHT Capabilities of an Access Point as defined in IEEE 802.11-2016 [8].

Table 6.5.15-1: Attributes of the HtCapabilities

Attribute name	Data type	Cardinality	Description
vhtCapInfo	UInt32	1	VHT capabilities Info as defined in IEEE 802.11-2016 [8].
vhtMcsNss	UInt64	1	Supported VHT-MCS and NSS Set as defined in IEEE 802.11-2016 [8].

6.5.16 Type: HeCapabilities

This type represents information on HE Capabilities of an Access Point as defined in draft IEEE P802.11ax/D4.3 [i.10].

Table 6.5.16-1: Attributes of the HtCapabilities

Attribute name	Data type	Cardinality	Description
heMacCapInfo	Uint8	1	MAC capabilities of an Access Point.
hePhyCapinfo	Uint8	1	PHY capabilities of an Access Point.
supportedHeMcsNssSet	Uint8	1	Supported MCS and NSS Set.
ppeThresholds	not defined	0..1	PPE Threshold determines the nominal packet padding value for a HE PPDU.

6.5.17 Type: DmgCapabilities

This type represents information on DMG Capabilities of an Access Point as defined in draft IEEE P802.11ay/D4.0 [i.11].

Table 6.5.17-1: Attributes of the DmgCapabilities

Attribute name	Data type	Cardinality	Description
dmgStaCapInfo	Uint64	1	DMG station capabilities information as defined in draft IEEE P802.11/D4.0 [i.11]
dmgApOrPcpCapInfo	Uint16	1	DMG AP or PCP capabilities information as defined in draft IEEE P802.11/D4.0 [i.11]
dmgStaBeamTrackTime Limit	Uint16	1	DMG station beam tracking time limit as defined in draft IEEE P802.11/D4.0 [i.11]
ExtScMcsCap	Uint8	1	Extended SC MCS capabilities as defined in draft IEEE P802.11/D4.0 [i.11]
maxNrBasicAmsduSubfr ames	Uint8	1	Number of basic A-MSDU subframes in A-MSDU as defined in draft IEEE P802.11/D4.0 [i.11]
maxNrShortAmsduSubfr ames	Uint8	1	Number of short A-MSDU subframes in A-MSDU as defined in draft IEEE P802.11/D4.0 [i.11]
tddCap	Uint16	1	TDD capabilities as defined in draft IEEE P802.11/D4.0 [i.11]
sarCap	Uint8	1	SAR capabilities as defined in draft IEEE P802.11/D4.0 [i.11]

6.5.18 Type: EdmgCapabilities

This type represents information on EDMG Capabilities of an Access Point as defined in draft IEEE P802.11ay/D4.0 [i.11].

Table 6.5.18-1: Attributes of the EdmgCapabilities

Attribute name	Data type	Cardinality	Description
ampduParameters	Uint8	1	A-MPDU parameters as defined in draft IEEE P802.11/D4.0 [i.11]
trnParameters	Uint16	1	Training parameters as defined in draft IEEE P802.11/D4.0 [i.11]
supportedMcs	Uint32	1	Supported MCS as defined in draft IEEE P802.11/D4.0 [i.11]
reserved	Uint8	0..1	

6.5.19 Type: GeoLocation

This type represents information Geospatial Location of an Access Point as defined in IEEE 802.11-2016 [8] and in IETF RFC 6225 [6].

Table 6.5.19-1: Attributes of the GeoLocation

Attribute name	Data type	Cardinality	Description
latUncertainty	Uint8	1	The uncertainty for Latitude information as defined in IETF RFC 6225 [6]
lat	Uint64	1	The latitude value of location as defined in IETF RFC 6225 [6]
longUncertainty	Uint8	1	The uncertainty for Longitude information as defined in IETF RFC 6225 [6]
long	Uint64	1	The longitude value of location as defined in IETF RFC 6225 [6]
altitudeType	Uint8	0..1	The type description for altitude information e.g. floors or meters as defined in IETF RFC 6225 [6]
altitudeUncertainty	Uint8	0..1	The uncertainty for altitude information as defined in IETF RFC 6225 [6]
altitude	Uint32	0..1	The altitude value of location as defined in IETF RFC 6225 [6]
datum	Uint8	1	The datum value to express how coordinates are organized and related to real world as defined in IETF RFC 6225 [6]

6.5.20 Type: CivicLocation

This type represents information on Civic Location of an Access Point as defined in IETF RFC 4776 [7].

Table 6.5.20-1: Attributes of the CivicLocation

Attribute name	Data type	Cardinality	Description
country	String	1	The two-letter ISO 3166 [i.9] country code in capital ASCII letters, e.g. DE or US, as per ISO 3166 [i.9]
ca0	String	0..1	Language
ca1	String	0..1	National subdivisions (state, canton, region,province, prefecture)
ca2	String	0..1	County, parish, gun (JP), district (IN)
ca3	String	0..1	City, township, shi (JP)
ca4	String	0..1	City division, borough, city district, ward, chou (JP)
ca5	String	0..1	Neighborhood, block
ca6	String	0..1	Group of streets below the neighborhood level
ca16	String	0..1	Leading street direction
ca17	String	0..1	Trailing street suffix
ca18	String	0..1	Street suffix or type
ca19	String	0..1	House number
ca20	String	0..1	House number suffix
ca21	String	0..1	Landmark of vanity address
ca22	String	0..1	Additional location information
ca23	String	0..1	Name (residence and office occupant)
ca24	String	0..1	Postal/zip code
ca25	String	0..1	Building (structure)
ca26	String	0..1	Unit (apartment/suite)
ca27	String	0..1	Floor
ca28	String	0..1	Room
ca29	String	0..1	Type of place
ca30	String	0..1	Postal community name
ca31	String	0..1	Post office box
ca32	String	0..1	Additional code
ca33	String	0..1	Seat (desk.cubicle, workstation)
ca34	String	0..1	Primary road name
ca35	String	0..1	Road section
ca36	String	0..1	Branch road name
ca37	String	0..1	Sub-branch road name
ca38	String	0..1	Street name pre-modifier
ca39	String	0..1	Street name post-modifier
ca128	String	0..1	Script

6.5.21 Type: Rssi

This type represents information on the Received Signal Strength Indicator (RSSI) of a client station as defined in IEEE 802.11-2016 [8].

Table 6.5.21-1: Attributes of the Rssi

Attribute name	Data type	Cardinality	Description
rssi	Uint8	1	The Received Signal Strength Indicator from a station

6.5.22 Type: StaDataRate

This type represents the data rates of a client station as defined in Data Elements Specification v1.0 [i.8].

Table 6.5.22-1: Attributes of the StaDataRate

Attribute name	Data type	Cardinality	Description
staId	StaIdentity	0..1	Identifier(s) to uniquely specify the client station(s) associated.
staLastDataDownlinkRate		0..1	The data transmit rate in kbps that was most recently used for transmission of data PPDUs from the access point to the station.
staLastDataUplinkRate		0..1	The data transmit rate in Kbps that was most recently used for transmission of data PPDUs from the associated station to the access point.

6.5.23 Type: LinkType

This type represents a type of link.

Table 6.5.23-1: Attributes of the LinkType

Attribute name	Data type	Cardinality	Description
href	String	1	URI referring to a resource

6.5.24 Type: ChannelLoadConfig

This configuration applies to BssLoad measurement as described in clause 6.5.7 in the present document.

Table 6.5.24-1: Attributes of the ChannelLoadConfig

Attribute name	Data type	Cardinality	Description
apId	ApIdentity	1	Identifier(s) to uniquely specify the target Access Point
cChannelId	Integer	1	Channel number which load is reported
channelLoad	Integer	1	Channel load as per IEEE 802.11-2012 [8], section 11.11.9.3

6.5.25 Type: BeaconRequestConfig

Table 6.5.25-1: Attributes of the BeaconRequestConfig

Attribute name	Data type	Cardinality	Description
staId	StaIdentity	1	Identifier to uniquely specify the station whose information is exposed within this data type.
channelId	Integer	1	Channel number to scan. A Channel Number of 0 indicates a request to make iterative measurements for all supported channels in the Operating Class where the measurement is permitted on the channel and the channel is valid for the current regulatory domain. A Channel Number of 255 indicates a request to make iterative measurements for all supported channels in the current Operating Class listed in the latest AP Channel Report received from the serving AP.
measurementMode	Integer	1	0 for passive. 1 for active. 2 for beacon table.
bssId	String	1..N	The BSSID field indicates the BSSID of the BSS(s) for which a beacon report is requested. When requesting beacon reports for all BSSs on the channel, the BSSID field contains the wildcard BSSID.
ssId	String	1..N	(Optional) The SSID subelement indicates the ESS(s) or IBSS(s) for which a beacon report is requested.
reportingCondition	Integer	1	As in table T9-89 of IEEE 802.11-2012 [8].

6.5.26 Type: StaStatisticsConfig

Table 6.5.26-1: Attributes of the StaStatisticsConfig

Attribute name	Data type	Cardinality	Description
staId	StaIdentity	1	Identifier to uniquely specify the station whose information is exposed within this data type.
groupIdentity	Integer	1	As per table T 9-114 of IEEE 802.11-2012 [8].
triggeredReport	Bool	1	Yes, use triggered report.
triggerTimeout	Integer	1	The Trigger Timeout field contains a value in units of 100 TUs during which a measuring STA does not generate further triggered STA Statistics Reports after a trigger condition has been met.
triggerCondition	16bits bitmap	1	As per Figure 9-161 of IEEE 802.11. This bitmap defines what are the metrics returned by the STA Statistics Report.

6.5.27 Type: BeaconReport

Table 6.5.27-1: Attributes of the BeaconReport

Attribute name	Data type	Cardinality	Description
staId	StaIdentity	1	Identifier to uniquely specify the station whose information is exposed within this data type.
measurementId	String	1	Measurement ID of the Measurement configuration applied to this Beacon Report.
channelId	Integer	1	Channel number where the beacon was received.
bssId	String	1..N	The BSSID field indicates the BSSID of the BSS(s) for which a beacon report has been received.
ssId	String	1..N	(Optional) The SSID subelement indicates the ESS(s) or IBSS(s) for which a beacon report is received.
reportingCondition	Integer	1	As in table T9-89 of IEEE 802.11-2012 [8].

6.6 Referenced simple data types and enumerations

Referenced simple data types and enumerations are not used in the present document.

7 API definition

7.1 Introduction

This clause defines the resources and operations of the WLAN Access Information API (WAI API).

7.2 Global definitions and resource structure

All resource URLs of this API shall have the following root:

{apiRoot}/{apiName}/{apiVersion}/

The "apiRoot" is discovered using the service registry. The "apiName" shall be set to "wai" and "apiVersion" shall be set to "v1" for the present document. It includes the scheme ("http" or "https"), host and optional port, and an optional prefix string. The API shall support HTTP over TLS (also known as HTTPS defined in IETF RFC 2818 [2]). TLS version 1.2 as defined by IETF RFC 5246 [3] shall be supported. HTTP without TLS is not recommended. All resource URIs in the clauses below are defined relative to the above root URI.

The content format of JSON shall be supported.

The JSON format is signalled by the content type "application/json".

This API shall require the use of the OAuth 2.0 client credentials grant type according to IETF RFC 6749 [4] with bearer tokens according to IETF RFC 6750 [5]. See clause 7.16 of ETSI GS MEC 009 [10] for more information. The token endpoint can be discovered as part of the service availability query procedure defined in ETSI GS MEC 011 [i.1]. How the client credentials are provisioned into the MEC application is out of scope of the present document.

This API supports additional application-related error information to be provided in the HTTP response when an error occurs. See clause 7.15 of ETSI GS MEC 009 [10] for more information.

Figure 7.2-1 illustrates the resource URI structure of this API.

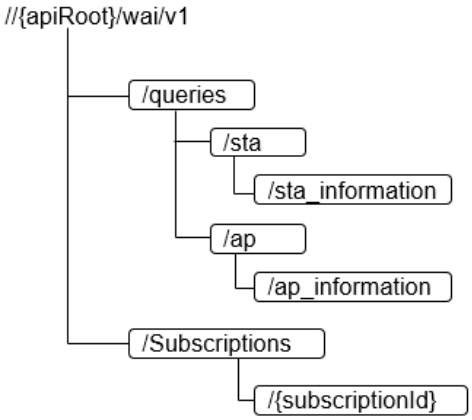

Figure 7.2-1: Resource URI structure of the WLAN Access Information API

Table 7.2-1 provides an overview of the resources defined by the present specification for the WAI API, and the applicable HTTP methods.

Table 7.2-1: Resources and methods overview

Resource name	Resource URI	HTTP method	Meaning
Access Point information	/queries/ap/ap_information	GET	Retrieve current status of Access Point information
Station information	/queries/sta/sta_information	GET	Retrieve current status of Station information
All subscriptions for a subscriber	/subscriptions	GET	Retrieve a list of active subscriptions for this subscriber
		POST	Create a new subscription
Existing subscription	/subscriptions/{subscriptionId}	GET	Retrieve information on current specific subscription
		PUT	Modify existing subscription by sending a new data structure
		DELETE	Cancel the existing subscription
Notification callback	Client provided callback reference	POST	Send a notification

7.3 Resource: ap_information

7.3.1 Description

This resource is queried to retrieve information on WLAN access points.

7.3.2 Resource definition

Resource URI: **{apiRoot}/wai/v1/queries/ap/ap_information**

This resource shall support the resource URI variables defined in Table 7.3.2-1.

Table 7.3.2-1: Resource URI Variables for resource "ap_information"

Name	Definition
apiRoot	See clause 7.2

7.3.3 Resource Methods

7.3.3.1 GET

The GET method is used to query information about the WLAN Access Points.

This method shall support the URI query parameters, request and response data structures, and response codes, as specified in Tables 7.3.3.1-1 and 7.3.3.1-2.

Table 7.3.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	Cardinality	Remarks
filter		0..1	Attribute-based filtering expression according to clause 6.19 of ETSI GS MEC 009 [10]. The WLAN Access Information API shall support receiving this parameter as part of the URI query string. All attribute names that appear in the ap_information and in data types referenced from it shall be supported by the WLAN Access Information API in the filter expression.
all_fields		0..1	Include all complex attributes in the response. See clause 6.18 of ETSI GS MEC 009 [10] for details. The WLAN Access Information API shall support this parameter.
fields		0..1	Complex attributes to be included into the response. See clause 6.18 of ETSI GS MEC 009 [10] for details. The WLAN Access Information API shall support this parameter.
exclude_fields		0..1	Complex attributes to be excluded from the response. See clause 6.18 of ETSI GS MEC 009 [10] for details. The WLAN Access Information API shall support this parameter.
exclude_default		0..1	Indicates to exclude the following complex attributes from the response. See clause 6.18 of ETSI GS MEC 009 [10] for details. The WLAN Access Information API shall support this parameter. The following attributes shall be excluded from the ap_information structure in the response body if this parameter is provided, or none of the parameters "all_fields", "fields", "exclude_fields", "exclude_default" are provided: • Not applicable.

Table 7.3.3.1-2: Data structures supported by the GET request/response on this resource

Request body	Data type	Cardinality	Remarks	
	n/a			
Response body	**Data type**	**Cardinality**	**Response Codes**	**Remarks**
	ApInfo	0..N	200 OK	Shall be returned when information about zero or more Access Points has been queried successfully. The response body shall contain in an array the representations of zero or more Access Points, as defined in clause 6.2.2. If the "filter" URI parameter or one of the "all_fields", "fields" (if supported), "exclude_fields" (if supported) or "exclude_default" URI parameters was supplied in the request, the data in the response body shall have been transformed according to the rules specified in clauses 6.19 and 6.18 of ETSI GS MEC 009 [10], respectively.
	ProblemDetails	1	400 Bad Request	Shall be returned upon the following error: Invalid attribute-based filtering expression. The response body shall contain a ProblemDetails structure, in which the "detail" attribute should convey more information about the error.
	ProblemDetails	1	400 Bad Request	Shall be returned upon the following error: Invalid attribute selector. The response body shall contain a ProblemDetails structure, in which the "detail" attribute should convey more information about the error.
	ProblemDetails	1	400 Bad Request	Shall be returned upon the following error: Response too big.
	ProblemDetails	See annex E of [10]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in annex E of ETSI GS MEC 009 [10] may be returned.

7.3.3.2 PUT

Not applicable.

7.3.3.3 PATCH

Not applicable.

7.3.3.4 POST

Not applicable.

7.3.3.5 DELETE

Not applicable.

7.4 Resource: sta_information

7.4.1 Description

This resource is queried to retrieve information on WLAN stations.

7.4.2 Resource definition

Resource URI: **{apiRoot}/wai/v1/queries/sta/sta_information**

This resource shall support the resource URI variables defined in Table 7.4.2-1.

Table 7.4.2-1: Resource URI Variables for resource "sta_information"

Name	Definition
apiRoot	See clause 7.2

7.4.3 Resource Methods

7.4.3.1 GET

The GET method is used to query information about the WLAN stations.

This method shall support the URI query parameters, request and response data structures, and response codes, as specified in Tables 7.4.3.1-1 and 7.4.3.1-2.

Table 7.4.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	Cardinality	Remarks
filter		0..1	Attribute-based filtering expression according to clause 6.19 of ETSI GS MEC 009 [10]. The WLAN Access Information API shall support receiving this parameter as part of the URI query string. All attribute names that appear in the ap_information and in data types referenced from it shall be supported by the WLAN Access Information API in the filter expression.
all_fields		0..1	Include all complex attributes in the response. See clause 6.18 of ETSI GS MEC 009 [10] for details. The WLAN Access Information API shall support this parameter.
fields		0..1	Complex attributes to be included into the response. See clause 6.18 of ETSI GS MEC 009 [10] for details. The WLAN Access Information API shall support this parameter.
exclude_fields		0..1	Complex attributes to be excluded from the response. See clause 6.18 of ETSI GS MEC 009 [10] for details. The WLAN Access Information API shall support this parameter.
exclude_default		0..1	Indicates to exclude the following complex attributes from the response. See clause 6.18 of ETSI GS MEC 009 [10] for details. The WLAN Access Information API shall support this parameter. The following attributes shall be excluded from the ap_information structure in the response body if this parameter is provided, or none of the parameters "all_fields", "fields", "exclude_fields", "exclude_default" are provided: • Not applicable.

Table 7.4.3.1-2: Data structures supported by the GET request/response on this resource

Request body	Data type	Cardinality	Remarks	
	n/a			
Response body	**Data type**	**Cardinality**	**Response Codes**	**Remarks**
	StaInfo	0..N	200 OK	Shall be returned when information about zero or more WLAN stations has been queried successfully. The response body shall contain in an array the representations of zero or more WLAN stations, as defined in clause 6.2.2. If the "filter" URI parameter or one of the "all_fields", "fields" (if supported), "exclude_fields" (if supported) or "exclude_default" URI parameters was supplied in the request, the data in the response body shall have been transformed according to the rules specified in clauses 6.19 and 6.18 of ETSI GS MEC 009 [10], respectively.
	ProblemDetails	1	400 Bad Request	Shall be returned upon the following error: Invalid attribute-based filtering expression. The response body shall contain a ProblemDetails structure, in which the "detail" attribute should convey more information about the error.
	ProblemDetails	1	400 Bad Request	Shall be returned upon the following error: Invalid attribute selector. The response body shall contain a ProblemDetails structure, in which the "detail" attribute should convey more information about the error.
	ProblemDetails	1	400 Bad Request	Shall be returned upon the following error: Response too big.
	ProblemDetails	See annex E of [10]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in annex E of ETSI GS MEC 009 [10] may be returned.

7.3.3.2 PUT

Not applicable.

7.3.3.3 PATCH

Not applicable.

7.3.3.4 POST

Not applicable.

7.3.3.5 DELETE

Not applicable.

7.5 Resource: subscriptions

7.5.1 Description

This resource contains various resources related to subscriptions for notifications.

7.5.2 Resource definition

Resource URI: **{apiRoot}/wai/v1/subscriptions/**

This resource shall support the resource URI variables defined in Table 7.5.2-1.

Table 7.5.2-1: Resource URI variables for resource "subscriptions"

Name	Definition
apiRoot	See clause 7.2

7.5.3 Resource methods

7.5.3.1 GET

The GET method is used to request information about the subscriptions for this requestor. Upon success, the response contains entity body with the list of links to the subscriptions that are present for the requestor.

This method shall support the URI query parameters, request and response data structures, and response codes, as specified in Tables 7.5.3.1-1 and 7.5.3.1-2.

Table 7.5.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	Cardinality	Remarks
subscription_type	String	0..1	Query parameter to filter on a specific subscription type. Permitted values: • assoc_sta Associated Stations • sta_data_rate Station data rate

Table 7.5.3.1-2: Data structures supported by the GET request/response on this resource

Request body	**Data type**	**Cardinality**	**Remarks**	
	n/a			
Response body	**Data type**	**Cardinality**	**Response Codes**	**Remarks**
	SubscriptionLinkList	1	200 OK	Upon success, a response body containing the list of links to requestor's subscriptions is returned.
	ProblemDetails	0..1	400 Bad Request	It is used to indicate that incorrect parameters were passed to the request. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	401 Unauthorized	It is used when the client did not submit credentials. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	1	403 Forbidden	The operation is not allowed given the current status of the resource. More information shall be provided in the "detail" attribute of the "ProblemDetails" structure.
	ProblemDetails	0..1	404 Not Found	It is used when a client provided a URI that cannot be mapped to a valid resource URI. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.

	Data type	Cardinality	Response Codes	Remarks
Response body	ProblemDetails	0..1	406 Not Acceptable	It is used to indicate that the server cannot provide the any of the content formats supported by the client. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	429 Too Many Requests	It is used when a rate limiter has triggered. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.

7.5.3.2 PUT

Not applicable.

7.5.3.3 PATCH

Not applicable.

7.5.3.4 POST

The POST method is used to create a new subscription to WLAN notifications. Upon success, the response contains entity body describing the created subscription.

This method shall support the request and response data structures, and response codes, as specified in Table 7.5.3.4-1.

Table 7.5.3.4-1: Data structures supported by the POST request/response on this resource

	Data type	Cardinality	Response Codes	Remarks
Request body	{NotificationSubscription}	1		The entity body in the request contains data type of the specific WLAN event subscription that is to be created, where the data type options are listed below and defined in clauses 6.3.2 through 6.3.3: • AssocStaSubscription. • StaDataRateSubscription.
Response body	{NotificationSubscription}	1	201 Created	Indicates successful resource creation, where the resource URI shall be returned in the HTTP Location header field. In the returned NotificationSubscription structure, the created subscription is described using the appropriate data type from the list below and as defined in clauses 6.3.2 through 6.3.3: • AssocStaSubscription. • StaDataRateSubscription.
	ProblemDetails	0..1	400 Bad Request	It is used to indicate that incorrect parameters were passed to the request. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	401 Unauthorized	It is used when the client did not submit credentials. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.

	Data type	Cardinality	Response Codes	Remarks
Response body	ProblemDetails	1	403 Forbidden	The operation is not allowed given the current status of the resource. More information shall be provided in the "detail" attribute of the "ProblemDetails" structure.
	ProblemDetails	0..1	404 Not Found	It is used when a client provided a URI that cannot be mapped to a valid resource URI. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	406 Not Acceptable	It is used to indicate that the server cannot provide the any of the content formats supported by the client. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	415 Unsupported Media Type	It is used to indicate that the server or the client does not support the content type of the entity body. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	422 Unprocessable Entity	It is used to indicate that the server understands the content type of the request entity and that the syntax of the request entity is correct but that the server is unable to process the contained instructions. This error condition can occur if an JSON request body is syntactically correct but semantically incorrect, for example if the target area for the request is considered too large. This error condition can also occur if the capabilities required by the request are not supported. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	429 Too Many Requests	It is used when a rate limiter has triggered. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.

7.5.3.5 DELETE

Not applicable.

7.6 Resource: existing subscription

7.6.1 Description

This resource represents a subscription that the client has created to receive WLAN event notifications.

7.6.2 Resource definition

Resource URI: **{apiRoot}/wai/v1/subscriptions/{subscriptionId}**

This resource shall support the resource URI variables defined in Table 7.6.2-1.

Table 7.6.2-1: Resource URI variables for resource "existing subscription"

Name	Definition
apiRoot	See clause 7.2.
subscriptionId	Refers to created subscription, where the WLAN Access Information API allocates a unique resource name for this subscription. The resource name can be also used to identify the resource.

7.6.3 Resource methods

7.6.3.1 GET

The GET method is used to retrieve information about this subscription. Upon success, the response contains entity body with the data type describing the subscription.

This method shall support the URI query parameters, request and response data structures, and response codes, as specified in Tables 7.6.3.1-1 and 7.6.3.1-2.

Table 7.6.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	Cardinality	Remarks
n/a			

Table 7.6.3.1-2: Data structures supported by the GET request/response on this resource

Request body	Data type	Cardinality	Remarks	
	n/a			
Response body	**Data type**	**Cardinality**	**Response Codes**	**Remarks**
	{NotificationSubscription}	1	200 OK	Upon success, a response body containing data type describing the specific WLAN event subscription is returned. The allowed data types for subscriptions are defined in clauses 6.3.2 through 6.3.3 and are as follows: • AssocStaSubscription. • StaDataRateSubscription.
	ProblemDetails	0..1	400 Bad Request	It is used to indicate that incorrect parameters were passed to the request. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	401 Unauthorized	It is used when the client did not submit credentials. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	1	403 Forbidden	The operation is not allowed given the current status of the resource. More information shall be provided in the "detail" attribute of the "ProblemDetails" structure.
	ProblemDetails	0..1	404 Not Found	It is used when a client provided a URI that cannot be mapped to a valid resource URI. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.

	Data type	Cardinality	Response Codes	Remarks
Response body	ProblemDetails	0..1	406 Not Acceptable	It is used to indicate that the server cannot provide the any of the content formats supported by the client. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	429 Too Many Requests	It is used when a rate limiter has triggered. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.

7.6.3.2 PUT

The PUT method is used to update the existing subscription. PUT method in this case has "replace" semantics. Upon successful operation, the target resource is updated with new Data Type received within the message body of the PUT request.

This method shall support the URI query parameters, request and response data structures, and response codes, as specified in Tables 7.6.3.2-1 and 7.6.3.2-2.

Table 7.6.3.2-1: URI query parameters supported by the PUT method on this resource

Name	Data type	Cardinality	Remarks
n/a			

Table 7.6.3.2-2: Data structures supported by the PUT request/response on this resource

	Data type	Cardinality	Response Codes	Remarks
Request body	{NotificationSubscription}	1		New NotificationSubscription is included as entity body of the request. The allowed data types for subscriptions are defined in clauses 6.3.2 through 6.3.3 and are as follows: • AssocStaSubscription. • StaDataRateSubscription.
Response body	{NotificationSubscription}	1	200 OK	Upon success, a response body containing data type describing the updated subscription is returned. The allowed data types for subscriptions are defined in clauses 6.3.2 through 6.3.3 and are as follows: • AssocStaSubscription. • StaDataRateSubscription.
	ProblemDetails	0..1	400 Bad Request	It is used to indicate that incorrect parameters were passed to the request. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	401 Unauthorized	It is used when the client did not submit credentials. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	1	403 Forbidden	The operation is not allowed given the current status of the resource.

				More information shall be provided in the "detail" attribute of the "ProblemDetails" structure.
Response body	**Data type**	**Cardinality**	**Response Codes**	**Remarks**
	ProblemDetails	0..1	404 Not Found	It is used when a client provided a URI that cannot be mapped to a valid resource URI. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	406 Not Acceptable	It is used to indicate that the server cannot provide the any of the content formats supported by the client. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	412 Precondition Failed	It is used when a condition has failed during conditional requests, e.g. when using ETags to avoid write conflicts when using PUT. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	422 Unprocessable Entity	It is used to indicate that the server understands the content type of the request entity and that the syntax of the request entity is correct but that the server is unable to process the contained instructions. This error condition can occur if an JSON request body is syntactically correct but semantically incorrect, for example if the target area for the request is considered too large. This error condition can also occur if the capabilities required by the request are not supported. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	429 Too Many Requests	It is used when a rate limiter has triggered. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.

7.6.3.3 PATCH

Not applicable.

7.6.3.4 POST

Not applicable.

7.6.3.5 DELETE

The DELETE method is used to cancel the existing subscription. Cancellation can be made by deleting the resource that represents existing subscription.

This method shall support the URI query parameters, request and response data structures, and response codes, as specified in Tables 7.6.3.5-1 and 7.6.3.5-2.

Table 7.6.3.5-1: URI query parameters supported by the DELETE method on this resource

Name	Data type	Cardinality	Remarks
n/a			

Table 7.6.3.5-2: Data structures supported by the DELETE request/response on this resource

Request body	Data type	Cardinality	Remarks	
	n/a			
Response body	**Data type**	**Cardinality**	**Response Codes**	**Remarks**
	n/a		204 No Content	Upon success, a response 204 No Content without any response body is returned.
	ProblemDetails	0..1	401 Unauthorized	It is used when the client did not submit credentials. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	1	403 Forbidden	The operation is not allowed given the current status of the resource. More information shall be provided in the "detail" attribute of the "ProblemDetails" structure.
	ProblemDetails	0..1	404 Not Found	It is used when a client provided a URI that cannot be mapped to a valid resource URI. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.
	ProblemDetails	0..1	429 Too Many Requests	It is used when a rate limiter has triggered. In the returned ProblemDetails structure, the "detail" attribute should convey more information about the error.

Annex A (informative): Complementary material for API utilization

To complement the definitions for each method and resource defined in the interface clauses of the present document, ETSI MEC ISG is providing for the WLAN Access Information (WAI) API a supplementary description file compliant to the OpenAPI Specification [i.2].

In case of discrepancies between the supplementary description file and the related data structure definitions in the present document, the data structure definitions take precedence.

The supplementary files, relating to the present document, are located at https://forge.etsi.org/rep/mec/gs028-wai-api.

History

Document history		
V2.1.1	June 2020	Publication