Standardized Connectivity Management Objects
WLAN Parameters

For use with OMA Device Management

Approved Version 1.0 – 24 Oct 2008

Open Mobile Alliance

OMA-DDS-DM_ConnMO_WLAN-V1_0-20081024-A

Contents

Figures

Tables

1. Scope

1.1 Connectivity Object – WLAN Bearer

This document defines a Wireless LAN (WLAN) bearer specific parameters used together with the standardized connectivity management object [CONNMO] in order to have a complete standardized Network Access Point definition for WLAN connectivity settings in the OMA DM management tree.

While this WLAN object is optional for any OMA DM implementation, their widespread use will simplify the management of WLAN connectivity parameters in devices.

The object is defined using the OMA DM Device Description Framework [DMTND]. The object has standardized points of extension to permit implementation-specific parameters to accompany the standardized parameters. This added flexibility is intended to encourage the use of the standardized object while not unnecessarily restricting individual vendor innovations.

2. References

2.1 Normative References

[CONNMO] *Standardized Connectivity Management Objects, Version 1.0,* Open Mobile Alliance™, OMA-DDS-DM_ConnMO-V1_0-D, URL:http://www.openmobilealliance.org

[DMTND] *Device Management Tree and Description, Version 1.2*, Open Mobile Alliance™, OMA-TS-DM-DMTND-V1_2, URL:http://www.openmobilealliance.org

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

2.2 Normative Authorities of References

Various parameters specified in the management objects defined in this document rely on an authority outside the scope of this specification to supply the set of acceptable values and value formats. In such references to external authority, only the directly cited material is referenced, not the entire external specification. The following authorities of reference are cited in this document:

[802.1X] IEEE Std 802.1X-2004. IEEE, 2004, URL: http://www.ieee.org/

[EAPMO] *Standardized Connectivity Management Objects, EAP Parameters, Version 1.0,* Open Mobile Alliance™, OMA-DDS-DM_ConnMO_EAP-V1_0-D, URL:http://www.openmobilealliance.org

[RFC791] *RFC 791, Internet Protocol*, DARPA, 1981, URL:http://www.ietf.org/rfc/rfc791.txt

[RFC2617] *RFC 2617, HTTP Authentication: Basic and Digest Access Authentication,* URL; http://www.ietf.org/rfc/rfc2617.txt

[RFC3513] *RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture*, The Internet Society, 2003, URL:http://www.ietf.org/rfc/rfc3513.txt

[RFC4632] *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan,* The Internet Society, August 2006,

[WLAN] IEEE P802.11-2007. IEEE, 2007, URL: http://www.ieee.org/

[WPA] Wi-Fi Protected Access (WPA) Version 3.1. Wi-Fi Alliance, August 2004, URL: http://www.wi-fi.org/

2.3 Informative References

None

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

See the DM Tree and Description [DMTND] document for definitions of terms related to the management tree.

3.3 Abbreviations

BSSID	Base station SSID
CA Certificate	Client Authenticate Certificate
EAP	Extensible Authentication Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
NAPAUTHINFO	Network Access Point Authentication Information
NAPDEF	Network Access Point Definition
OMA	Open Mobile Alliance
SSID	Service Set Identifier
UMA	Unlicensed Mobile Access
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WISP	Wireless Internet Service Provider
WPA	Wi-Fi Protected Area

4. Introduction

Usually, over time, network protocols grow and are replaced as the market cycle plays out. Connectivity Management Object [CONNMO] is structured in such a way as to be resilient to the addition of new bearer and proxy types without requiring wholesale replacement of the object definitions. In this way, the common structure survives into future versions of the management objects thus easing the burden of transition from old bearer types to new.

This document specifies WLAN bearer specific part of the general Network Access Point management object allowing vendor specific extensions. This specification is suitable for configuring wireless LAN connectivity using the 802.11 standards [WLAN] (e.g. 802.11b, 802.11g, 802.11i, 802.11n, …).

5. Justification

This Reference Release includes several Management Object definitions for use, in conjunction with the OMA Device Management Enabler, to manage data network connectivity settings for mobile terminals over common bearer and proxy types.

5.1 Standardized Connectivity Management

Providing a standardized set of management objects for configuration of data network connectivity through the OMA Device Management system will improve the usability and customer experience of mobile terminals that rely upon data services. As proposed, the management object definitions may be used in conjunction with OMA Device Management Candidate and Approved Enabler Releases over a variety of transports including: HTTP, HTTPS, OBEX over IrDA, OBEX over Bluetooth, and various forms of Smart Card.

5.2 Application-Neutral

Producing these management object definitions in an application-neutral fashion, we avoid reinvention of solutions to the same set of problems for each of new application that requires data connectivity. This reduces the connectivity parameters that an application must define to a simple reference node, ConRef (Connectivity Reference).

5.3 Bearer-Neutral

By presenting the specifications in two parts, a bearer-neutral part and bearer-specific bindings, we reinforce the OMA principle of network neutrality while providing specificity where needed but without bias for or against any particular network type.

6. WLAN Management Object

6.1 Introduction

A general introduction of the connectivity management object is given in the connectivity management object document [CONNMO] as well as the needed compliance rules. This document specifies the WLAN bearer specific sub-tree that is placed under the general Network Access Point management object in order to enable the WLAN bearer specific parameter manipulation.

6.2 Definitions for NAP MO

The WLAN subtree specified in this document MUST be placed under the BearerParams node in [CONNMO].

BearerType

The *BearerType* node value specified in [CONNMO] MUST be "WLAN".

AddrType

The *AddrType* value in the NAP MO specified in [ConnMO] MUST be "SSID". The Addr value specified in the NAP MO [CONNMO] MUST be the primary SSID (name) of the WLAN network. A WLAN network identified by a SSID can contain several physical access points identified by the MAC address (BSSID).

AuthType

The AuthType value in the NAP MO specified in [ConnMO], if present, MUST be from the table below:

AuthType	Description
HTTP-BASIC	HTTP basic authentication performed according to [RFC2617].
HTTP-DIGEST	HTTP digest authentication performed according to [RFC2617].

Table 1: NAP Authentication Protocol Types

6.3 Graphical Representation (Informative)

The following figure provides the structure of WLAN management object.

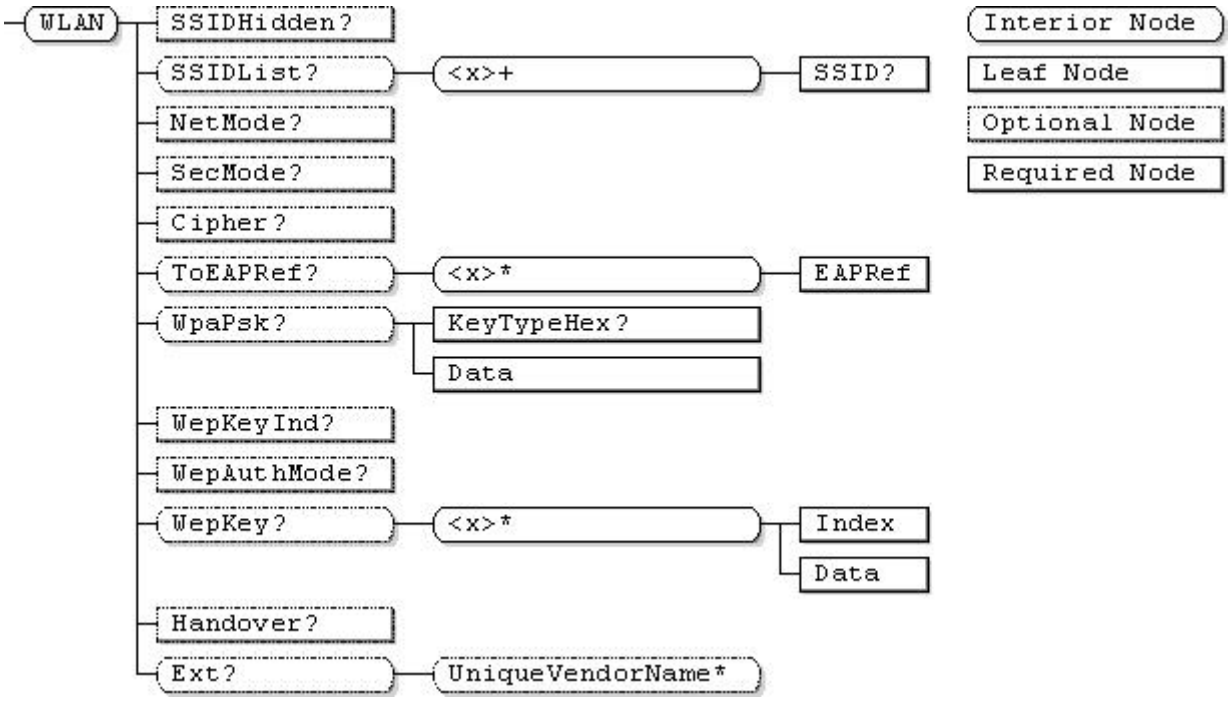

Figure 1. WLAN Management Object

6.4 Node descriptions

…/BearerParams/WLAN

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

This interior node specifies the bearer-specific parameters for a Network Access Point management object which describes a WLAN access point or *ad hoc* WLAN. Management Object Identifier for the WLAN MO MUST be: "urn:oma:mo:oma-connmo-wlan:1.0".

SSIDHidden

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

The SSIDHidden parameter indicates that the all SSID's in this NAP are hidden. If the value is "False" (or if this leaf node is absent) then the SSID is not hidden and if it is "True" then it is hidden. Direct scan is used to check if a hidden SSID is available.

SSIDList

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

SSIDList interior node defines the parameter list of additional SSIDs.

SSIDList/<x>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes different additional SSIDs.

SSIDList/<x>/SSID

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	Chr	Get

This node holds the SSID of a single additional SSID.

NetMode

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The NetMode node indicates the operational mode of the WLAN. Please refer to [WLAN] for details. If the parameter is not set or if the parameter is omitted, then infrastructure mode is assumed. Possible values are indicated in table below:

NetMode	Description
INFRA	Infrastructure network (default value)
ADHOC	Ad hoc network

Table 2: NetMode

SecMode

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The SecMode [WPA] parameter indicates security mode for the WLAN network. If parameter is omitted, no security is applied. Possible values are indicated in table below:

Value	Description of Security Mode
WEP	WEP security in use. Please refer to [WLAN] and [WPA] for details.
802.1X	802.1X security in use. This value indicates enterprise 802.1x operation, which uses dynamic WEP keys and 802.1x/EAP authentication. Please refer to [802.1X] and [WPA] for details.
WPA	Wi-Fi Protected Access security in use. Please refer to [WPA] for details.
WPA-PSK	Wi-Fi Protected Access security using pre-shared key in use. Please refer to [WPA] for details.
WPA2	Wi-Fi Protected Access 2 security in use. Please refer to [WPA] for details.
WPA2-PSK	Wi-Fi Protected Access 2 security using pre-shared key in use. Please refer to [WPA] for details.

Table 3: SecMode — Security Modes

Cipher

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The Cipher parameter specifies the encryption cipher to be used with this network access point. If parameter is omitted or its value is *null*, no encryption is applied. Possible values are indicated in table below. Not all combinations of SecMode and Cipher values are meaningful. Please refer to [WLAN] and [WPA] for details:

Value	Description of Cipher Suite
null	No encryption. [WLAN]
WEP	WEP encryption in use. [WPA]
TKIP	TKIP encryption. Temporal Key Integrity Protocol. [WPA]
AES	AES encryption. Advanced Encryption Standard. [WPA]

Table 4: Encryption Cipher

ToEAPRef

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

The ToEAPRef interior node is used for references to EAP MO definitions. Several instances of EAP settings may be listed under this interior node. The priority of the various EAP instances is implementation-specific.

ToEAPRef/<x>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node distinguishes different EAP references.

ToEAPRef/<x>/EAPRef

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

The EAPRef leaf indicates the linkage to EAP parameters. This parameter provides a run-time URI for the EAP parameter set described in [EAPMO].

WpaPsk

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node groups together the parameters of WpaPsk.

Note: This node and its sub-tree are meaningful only if SecMode value is WPA-PSK or WPA2-PSK.

WpaPsk/KeyTypeHex

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	bool	Get

The KeyTypeHex parameter indicates whether the following PSK Data is provided as an ASCII string or as a hexadecimal digit sequence.

Possible values are indicated in the table below:

Value	Description of PSK Data Type
False or absent	The PSK data is an ASCII string.
True	The PSK data is a hexadecimal digit sequence.

Table 5: KEY-TYPE — PSK Data Type

WpaPsk/Data

Status	Occurrence	Format	Min. Access Types
Required	One	chr	NO Get

The Data parameter is used to deliver the PSK data.

In the WPA-PSK mode, the following two forms are defined as a Pre-Shared Key:

- The first is an ASCII string. It is a passphrase for generating the key used for pre-shared key authentication. A WLAN device receiving the passphrase generates the 256bit key (from the passphrase and the SSID string) with the hash algorithm defined in IEEE802.11i.
- The second is a hexadecimal digit sequence. In this case, a user can specify the 256bit key directly in the form of 64 hex characters. (See **[WPA]** for more detail.)

When the KEY-TYPE value is False or absent, the Data value SHALL be an ASCII string of between 8 and 63 characters in length. When the KeyTypeHex value is True, it SHALL be a 256bit key of 64 hex characters. For any hexadecimal digits in the range "a" through "f", the case of letters is not significant and either upper or lower case letters MAY be used.

WepKeyInd

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

The WepKeyInd [WPA] indicates the value of the Index node in the WepKey sub-tree representing the default WEP key (0-3). Note: The keys specified in the WepKey subtree and the value of WepKeyInd are meaningful only if SecMode value is WEP.

WepAuthMode

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The WepAuthMode [WPA] indicates WEP authentication mode. Note: This node is meaningful only if SecMode value is WEP. Possible values are indicated in the table below:

WepAuthMode	Description
OPEN	Authentication Mode in use is open
SHARED	Shared Authentication Mode in use

Table 6: WepAuthMode

WepKey

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node defines the length and the data for the WepKey [WPA]. The maximum number of keys is 4. Client MUST use the key with an Index value matching the value of the WepKeyInd node (if that node is included). If no WepKeyInd node value is present, the order of selection of the WepKey values is implementation specific.

WepKey/<x>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOr4	node	Get

This interior node distinguishes different WepKeys. There MUST NOT be more than four interior nodes at this level.

Note: The term "ZeroOr4" in Occurance is defined in Section 9.4.3.18 in [DMTND].

WepKey/<x>/Index

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

Specifies the index of this WEP key as an integer value between 0 and 3. Each value of WepKey/…/Index MUST be unique with respect to other values of WepKey/…/Index within the same Network Access Point management object.

WepKey/<x>/Data

Status	Occurrence	Format	Min. Access Types
Required	One	chr	NO Get

The Data parameter indicates the WEP key data.WEP keys are either 40 bits or 104 bits in length. [WPA] The key SHALL be an ASCII string of hexadecimal digits. For any hexadecimal digits in the range "a" through "f", the case of letters is not significant and either upper or lower case letters MAY be used.

Handover

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

The Handover parameter, if *true*, indicates if handover from this access point to another access point with the same SSID is allowed. If the Handover parameter is *false* or not present, handover is not allowed.

Ext

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node designates the single top-level branch of the WLAN management object tree into which vendor extensions MAY be added, permanently or dynamically. Ext sub trees, such as this one, are included at various places in the DM connectivity management objects to provide flexible points of extension for implementation-specific parameters. However, vendor extensions MUST NOT be defined outside of the `Ext` sub-trees.

Ext/UniqueVendorName

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrMore	node	Get

This interior node is supplied by a vendor to distinguish their extension from those of other vendors. The *UniqueVendorName* SHOULD be a trademark or company name controlled by each vendor to ensure uniqueness. The structure of any sub-tree below a *UniqueVendorName* interior node is implementation-specific.

7. Operational Considerations

ConnMO is normatively dependent on the DM 1.2 specifications. However, this normative dependency should not be seen as restricting these MO definitions only to DM clients implementing that version of the DM enabler.

For example, a management authority may exchange ConnMO data-files using means not specifically defined in the DM 1.2 enabler.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-DDS-DM_ConnMO_WLAN-V1_0-20081024-A	24 Oct 2008	Approved by OMA Technical Plenary: Ref TP#: OMA-TP-2008-0405-INP_ConnMO_V1_0_RRP_for_Notification_and_Final_Approval