



Standardized Connectivity Management Objects
For use with OMA Device Management
Approved Version 1.0 – 07 Nov 2008

Open Mobile Alliance
OMA-DDS-DM_ConnMO-V1_0- 20081107-A

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1.	SCOPE.....	4
2.	REFERENCES	5
2.1	NORMATIVE REFERENCES.....	5
2.2	NORMATIVE AUTHORITIES OF REFERENCES.....	5
2.3	INFORMATIVE REFERENCES.....	5
3.	TERMINOLOGY AND CONVENTIONS.....	6
3.1	CONVENTIONS.....	6
3.2	DEFINITIONS.....	6
3.3	ABBREVIATIONS.....	6
4.	INTRODUCTION	8
5.	JUSTIFICATION	9
5.1	STANDARDIZED CONNECTIVITY MANAGEMENT	9
5.2	APPLICATION-NEUTRAL.....	9
5.3	BEARER-NEUTRAL.....	9
6.	STANDARDIZED CONNECTIVITY MANAGEMENT OBJECTS.....	10
6.1	Introduction to Management Objects (Informative)	10
6.1.1	Definition and description of management objects.....	10
6.2	DDF COMPLIANCE	10
6.2.1	Conformance Definitions.....	11
6.3	THE OMA DM CONNECTIVITY MANAGEMENT OBJECTS.....	11
6.3.1	Relationship to WAP Client Provisioning (Informative).....	11
6.4	NAP OBJECT.....	11
6.4.1	Introduction.....	11
6.4.2	Graphical Representation (Informative)	12
6.4.3	Node Descriptions.....	14
6.5	PROXY OBJECT	33
6.5.1	Introduction.....	33
6.5.2	Graphical Representation (Informative)	33
6.5.3	Node Descriptions.....	33
7.	OPERATIONAL CONSIDERATIONS	39
APPENDIX A.	CHANGE HISTORY (INFORMATIVE).....	40
A.1	APPROVED VERSION HISTORY	40

Figures

Figure 1:	NAP Management Object (Informative).....	12
Figure 2:	Continuation of NAP Management Object (Informative).....	13
Figure 3:	Proxy Management Object (Informative).....	33

1. Scope

This document defines a set of managed objects which offer a standardized way to represent connectivity settings in a mobile device OMA Device Management tree. There were three main requirements that guided the drafting of this specification:

- All connectivity parameters bootstrapped using OMA Client Provisioning can be subsequently addressed and managed via an OMA DM server;
- An OMA DM server can add new or managing existing proxies and network access points using this enabler;
- It should be possible to extend management objects with proprietary extensions.

While these objects are optional for any OMA DM implementation, their widespread use will simplify the management of basic connectivity parameters in mobile terminals.

The objects are defined using the OMA DM Device Description Framework [DMTND]. And each of the objects 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

- [OMADM] *OMA Device Management Enabler, Version 1.2*, Open Mobile Alliance™
OMA-ERELED-DM-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:

- [AUTH-RFC791] *RFC 791, Internet Protocol*, DARPA, 1981,
URL: <http://www.ietf.org/rfc/rfc791.txt>
- [E212] *ITU-T E.212 Identification Plan For Land Mobile Stations*, ITU,
URL: <http://www.itu.org/>
- [TIA/EIA-136-005A] *Introduction, Identity, and Semi-Permanent Memory*, TIA/EIA

2.3 Informative References

- [DMStdObj] *OMA Device Management Standardized Objects, Version 1.2*, Open Mobile Alliance™
OMA-TS-DM-DMStdObj-V1_2,
URL: <http://www.openmobilealliance.org>
- [DMTND] *OMA Device Management Tree and Description, Version 1.2*, Open Mobile Alliance™
OMA-TS-DM-DMTND-V1_2,
URL: <http://www.openmobilealliance.org>
- [ProvCont] *Provisioning Content, Version 1.1*, Open Mobile Alliance™,
OMA-WAP-ProvCont-v1_1,
URL: <http://www.openmobilealliance.org>

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

HTTP Proxy	An endpoint for the HTTP protocol providing authenticated access, content caching, content encoding translation, address redirection, and other functions.
Logical Proxy	A logical proxy is a set of physical proxies that may, for example, share the same WSP and WTLS context (shared session id value space). This specification does not distinguish between logical and physical proxies but permits the configuration of both logical and physical elements of all proxy types.
Network Access Point	A physical access point is an interface point between the wireless network and the fixed network. It is often a Remote Access Server, an SMSC, a USSDC, an 802.11 Access Point, or something similar. It has an address (such as a telephone number or 802.11 SSID) and an access bearer.
Physical Proxy	A physical proxy is a specific address at which proxy functionality is provided. It can be the IP address plus port for an IP accessible proxy, or the SME-address plus port for an SMS accessible proxy. This specification does not distinguish between logical and physical proxies but permits the configuration of both logical and physical elements of all proxy types.
WAP Proxy	The WAP proxy is an endpoint for the WTP, WSP and WTLS protocols, as well as a proxy that is able to access WAP content. A WAP Proxy can have functionality such as that of, for example, a WSP Proxy or a WTA Proxy.
WSP Proxy	A generic WAP proxy; similar in functionality to an HTTP proxy. It is a variant of a WAP Proxy.
WTA Proxy	The WTA Proxy is a Wireless Telephony proxy as defined by WAP.

3.3 Abbreviations

AAA	Authentication, Authorization, and Accounting
APN	Access Point Name
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CHAP	Challenge Handshake Authentication Protocol
CSD	Circuit Swithed Data
DDF	Device Description Framework
DNS	Domain Name System
DTD	Document Type Definition
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HA	Home Agent
HTTP	HyperText Transfer Protocol
IP	Internet Protocol

MAN	Mobitex Subscription Number
NAP	Network Access Point
OTA	Over The Air
PAP	Password Authentication Protocol
SME	Short Message Entity
SMS	Short Message Service
SMSC	Short Message Service Centre
SPI	Security Parameter Index
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USSD	Unstructured Supplementary Service Data
USSDC	Unstructured Supplementary Service Data Centre
WAP	Wireless Application Protocol
WSP	Wireless Session Protocol
WTA	Wireless Telephony Application
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol
XML	Extensible Mark-up Language

4. Introduction

Other OMA DM and common specifications define the syntax and semantics of the OMA DM protocol. However, the usefulness of such a protocol would be limited if the managed entities in devices required different data formats and displayed different behaviors. Central to the management of any suite of devices is the ability to configure and update the basic connectivity settings in each device. To avoid the situation where each device vendor defines a specialized and non-standard arrangement for managing connectivity parameters, this specification defines a set of management objects to permit the standardized representation and management of connectivity parameters in devices.

Since device manufacturers will always develop new functions in their devices and since these functions often are proprietary, no standardized management objects will exist for them. To make these functions manageable in the devices that have them, a device description framework is needed that can provide servers with the necessary information they must have in order to manage the new functions. The intention with this framework is that device manufacturers will publish descriptions of their devices as they enter the market. Organizations operating device management servers should then only have to feed the new description to their servers for them to automatically recognize and manage the new functions in the devices.

The introduction of vendor-specific extensions to these standardized objects is anticipated. Each management object contains several points of extension for arbitrary use by client implementations to allow collocation of proprietary innovations along with the standardized parameters. It is anticipated that vendors will include their implementation-specific extensions in published DDF that describes the management objects supported by each terminal model.

Finally, it is usual to find over time that network protocols grow and are replaced as the market cycle plays out. These management objects are 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.

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. Standardized Connectivity Management Objects

6.1 Introduction to Management Objects (Informative)

Management objects are the entities that can be manipulated by management actions carried over the OMA DM protocol. A management object can be as small as an integer or large and complex like a background picture, screen saver, or security certificate. The OMA DM protocol is neutral about the contents, or values, of the management objects and treats the node values as opaque data.

6.1.1 Definition and description of management objects

OMA DM management objects are defined using the OMA DM Device Description Framework [DMTND], or DDF. The use of this description framework produces detailed information about the device in question. However, due to the high level of detail in these descriptions, they are sometimes hard for humans to digest and it can be a time consuming task to get an overview of a particular object's structure.

In order to make it easier to quickly get an overview of how a management object is organized and its intended use, a simplified graphical notation in the shape of a block diagram is used in this document. Even though the notation is graphical, it still uses some printable characters, e.g. to denote the number of occurrences of a node. These are mainly borrowed from the syntax of DTDs for XML. The characters and their meaning are defined in the following table.

Character	Meaning
+	one or many occurrences
*	zero or more occurrences
?	zero or one occurrences

If none of these characters is used the default occurrence is exactly once.

There is one more feature of the DDF that needs to have a corresponding graphical notation, the un-named block. These are blocks that act as placeholders in the description and are instantiated with information when the nodes are used at run-time. Un-named blocks in the description are represented by a name within less than and greater than character, e.g. <x>.

Each block in the graphical notation corresponds to a described node, and the text is the name of the node. If a block contains an *x*, it means that the name is not known in the description and that it will be assigned at run-time. The names of all ancestral nodes are used to construct the URI for each node in the management object. It is not possible to see the actual parameters, or data, stored in the nodes by looking at the graphical notation of a management object.

For a further introduction to this graphical notation, please refer to [DMStdObj].

6.2 DDF compliance

The management object descriptions in this document are normative. However, the descriptions also contain a number of informative aspects that could be included to enhance readability or serve as examples. Other informative aspects are, for instance, the ZeroOrMore and OneOrMore elements, where implementations may introduce restrictions. All these exceptions are listed here:

- All XML comments, e.g. “<!-- some text -->”, are informative.
- The descriptions do not contain an RTProperties element, or any of its child elements, but a description of an actual implementation of this object MAY include these.
- If a default value for a leaf node is specified in a description, by the DefaultValue element, an implementation MUST supply its own appropriate value for this element. If the DefaultValue element is present in the description of a node, it MUST be present in the implementation, but MAY have a different value.

- The value of all Man, Mod, Description and DFTitle elements are informative and included only as examples.
- Below the interior nodes Ext and BearerParams, an implementation may add further nodes at will.
- The contents of the AccessType element MAY be extended by an implementation.
- If any of the following AccessType values are specified, they MUST NOT be removed in an implementation: Copy, Delete, Exec, Get, and Replace.
- If the AccessType value Add is specified it MAY be removed in an implementation if the implementation only supports a fixed number of child nodes.
- An implementation MAY replace the ZeroOrMore or OneOrMore elements with ZeroOrN or OneOrN respectively. An appropriate value for *N* must also be given with the ...*OrN* elements.

6.2.1 Conformance Definitions

The status definition in the node definitions indicates if the client supports that node or not. If the status is “Required” then the client MUST support that node in the case the client supports the parent node. In other case the node MAY be supported by the client.

6.3 The OMA DM Connectivity management objects

This specification defines two management objects, that while distinct objects, should be considered together. A *NAP* object permits configuration of *network access points* and contains both bearer-neutral and bearer-specific parameters. A *Proxy* object facilitates configuring *network proxies* of various kinds and is bearer-neutral but may include parameters specific to particular proxy types.

6.3.1 Relationship to WAP Client Provisioning (Informative)

These management objects describe various kinds of network access points and proxies. Certain aspects of NAPDEF, PXLOGICAL, and PXPHYSICAL characteristics defined in WAP Client Provisioning [ProvCont] have been altered to improve generality. However, it remains possible to use these object definitions to manage the proxy settings provisioned using [ProvCont].

When compared to the OMA Client Provisioning specifications, specifically [ProvCont], the PXPHYSICAL parameters have been collapsed together with the PXLOGICAL parameters in this mapping. This simplifies other forms of proxy (e.g. HTTP or ISA proxies) and does not limit the ability to specify the mapping of logical to physical proxy.

6.4 NAP Object

6.4.1 Introduction

The NAP object facilitates management of network access point parameters.

OMA DM [OMADM] protocol compatibility for the NAP MO is version 1.2 or any later compatibility version to this version.

6.4.2 Graphical Representation

(Informative)

The following figure provides the structure of NAP DM management object.

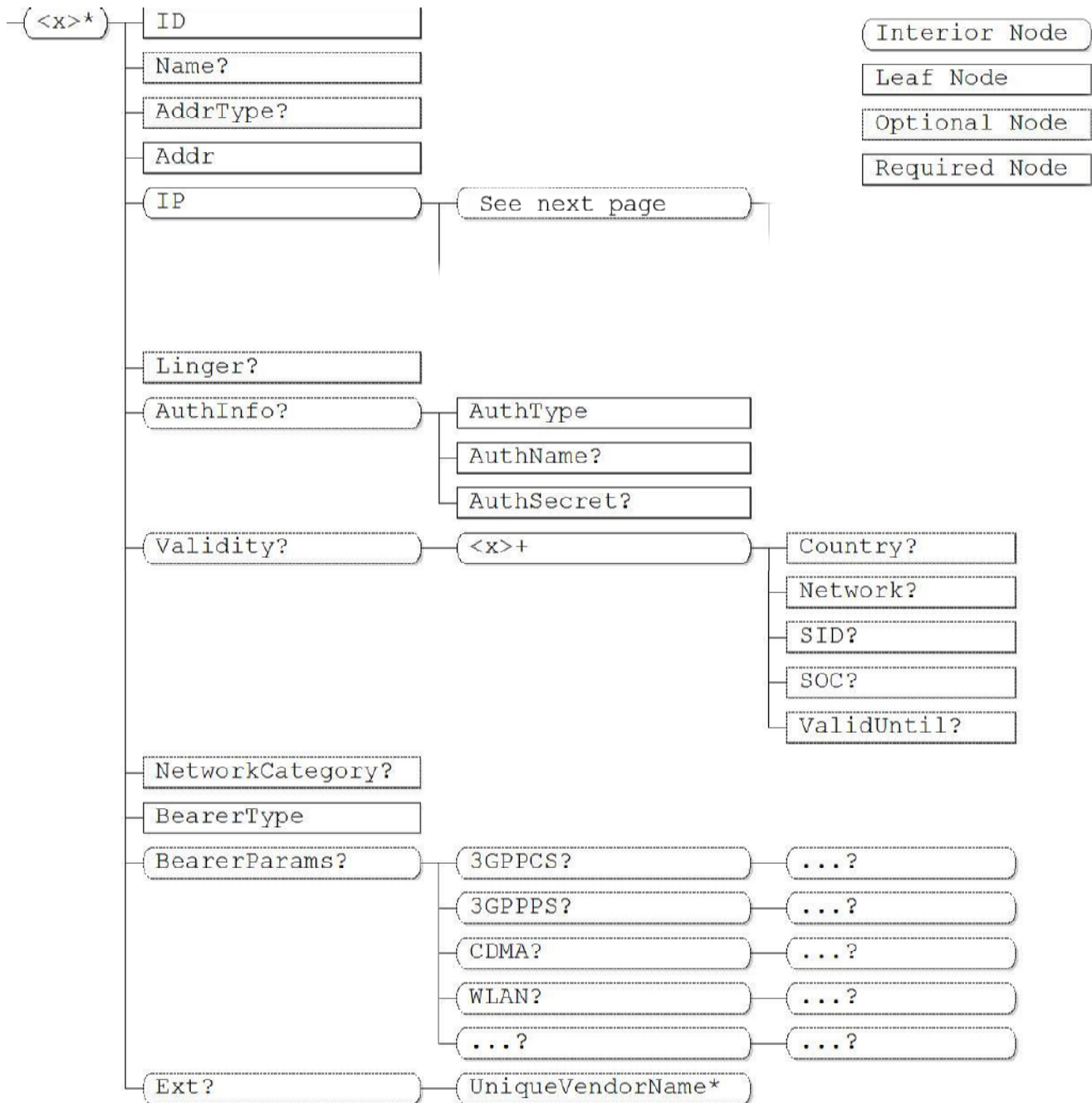


Figure 1: NAP Management Object (Informative)

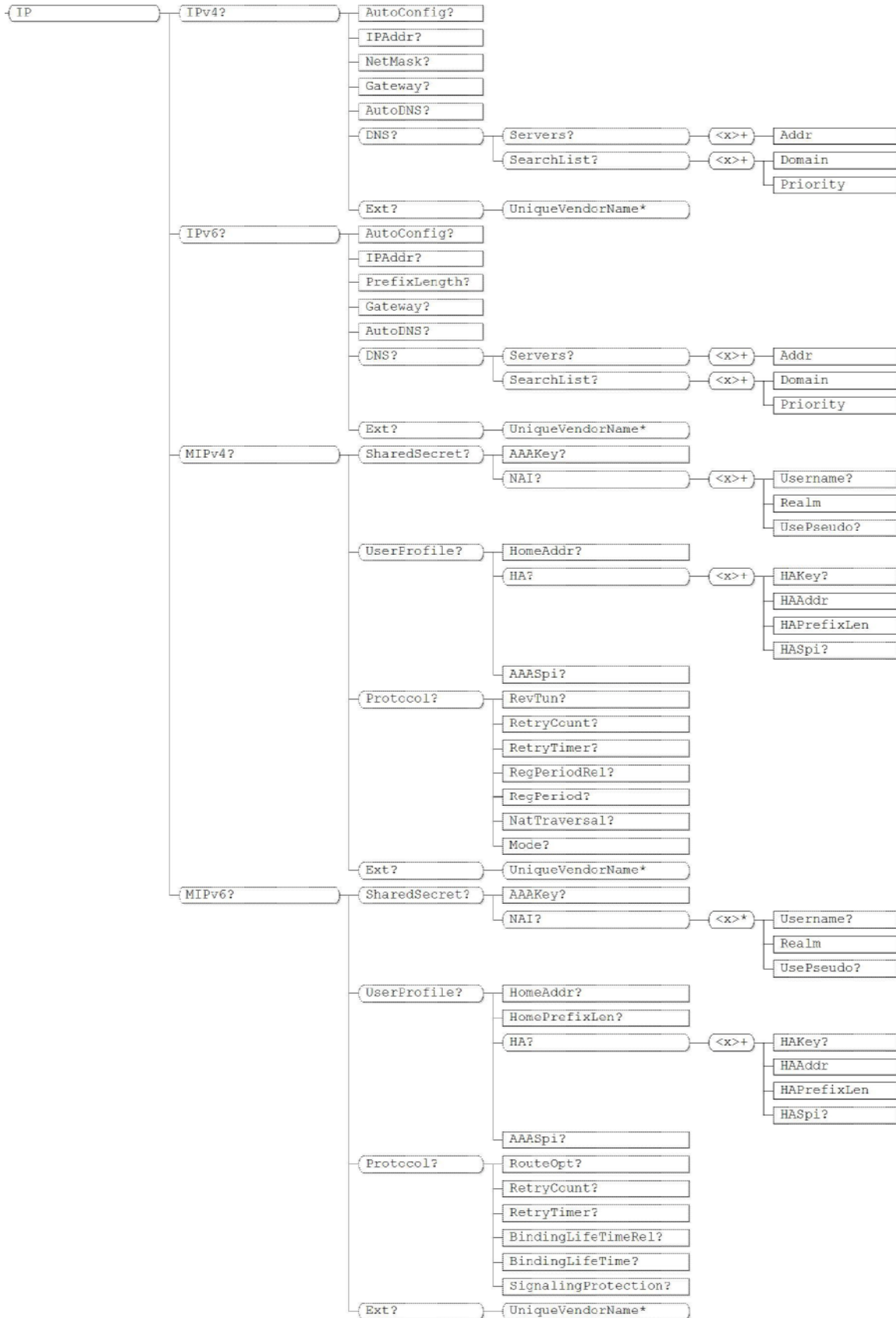


Figure 2: Continuation of NAP Management Object (Informative)

6.4.3 Node Descriptions

.../<x>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node specifies the unique object id of a *network access point*, or NAP, management object. The purpose of this interior node is to group together the parameters of a single NAP object. The ancestor elements of this node define the position in the management tree of the NAP object. But the structure of the DM tree and hence positions in the tree of management objects is out of scope of this specification. Management Object Identifier for the NAP MO MUST be: “urn:oma:mo:oma-connmo-nap:1.0”.

ID

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node defines the identity of the one specific network access point which an instance of this management object represents.

Name

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node provides an optional human readable name for the network access point.

AddrType

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node specifies the type of NAP address supplied as the **Addr** leaf node value. Authorities of reference and allowed values for **AddrType** are bearer-specific and are not listed here. Implementers are referred to the bearer specifications and the listed normative references describing each protocol for the proper usage context and details of each address type.

If the bearer type-specific parameter specification does not define a value for this node then the default value “IPv4” MUST be assumed and the **Addr** node MUST represent an IPv4 address [AUTH-RFC791] represented in string form dotted-decimal CIDR notation.

Addr

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node represents the address of the network access point. The value and mapping to a character representation are dependent upon the bearer type. (See the AddrType above for details on address format and acceptable values.)

IP

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

This interior node is parent node of the IP configuration sub-tree.

IP/IPv4

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node defines the IPv4 address configuration of the local terminal when this network access point is used. Two primary cases exist: the IPv4 address configuration is managed automatically by the network access point; the IPv4 address configuration is managed either by the terminal or by the device management server. In the event that auto-configuration is active, the terminal MAY modify the access type for selected IPv4 sub-tree nodes to disallow retrieval and/or modification of selected address parameters.

IPv4 address can be configured in two manners, dynamically and statically. When dynamic IP configuration is used the value of IPv4/AutoConfig node MUST be TRUE. When static IP configuration is used the value of IPv4/AutoConfig MUST be FALSE and IP address, network mask and gateway address are configured via IPv4/IPAddr, IPv4/NetMask and IPv4/Gateway.

DNS address(es) can be also configured dynamically and statically. When dynamic DNS configuration is used the value of IPv4/AutoDNS node MUST be TRUE. In case of static DNS configuration the value of that node MUST be FALSE and the static DNS address can be configured using IPv4/DNS/Server/<x>/Addr.

IP/IPv4/AutoConfig

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

If TRUE (or if this optional leaf node is absent), the terminal's IPv4 configuration SHOULD be generated automatically. If FALSE, the terminal MUST use the IPv4 configuration specified in the IPv4 sub-tree when connecting to the network. The specific mechanism used by the terminal to automatically configure its IPv4 interface is implementation specific and out of scope of this specification. However, this facility is anticipated by the standardized address configuration strategies detailed in the following references: [RFC2131] and [RFC3330].

IP/IPv4/IPAddr

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node specifies the IPv4 address [RFC791] of the device when connected using this network access point as a string in dotted-decimal notation.

IP/IPv4/NetMask

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node specifies the IPv4 network address mask [RFC791] of the device when connected using this network access point as a string in dotted-decimal notation.

IP/IPv4/Gateway

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This optional leaf node specifies the IPv4 address [RFC791] of the Internet gateway accessible when the device is connected using this network access point as a string in dotted-decimal notation.

IP/IPv4/AutoDNS

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

If TRUE (or if this optional leaf node is absent), the DNS addresses are to be configured automatically (for example using DHCP [RFC2132] protocol). If FALSE the DNS servers are described in the DNS sub-tree.

IP/IPv4/DNS

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node optionally specifies the DNS configuration for use while the device is connected using this network access point [RFC1034][RFC1035].

IP/IPv4/DNS/Servers

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node lists the DNS name servers [RFC1034] that should be used while the device is connected using this network access point.

IP/IPv4/DNS/Servers/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes DNS server addresses [RFC1034].

IP/IPv4/DNS/Servers/<X>/Addr

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node defines a single DNS server address [RFC791] as a string in dotted-decimal notation.

IP/IPv4/DNS/SearchList

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node optionally lists the DNS domains [RFC1034] that should be added to unqualified domain names when performing name service queries while the device is connected using this network access point.

IP/IPv4/DNS/SearchList/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes items in the DNS search list.

IP/IPv4/DNS/SearchList/<X>/Domain

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node defines a DNS domain [RFC1034] to be used in the domain search list.

IP/IPv4/DNS/SearchList/<X>/Priority

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node defines the priority of a DNS domain in the domain [RFC1034] search list.

IP/IPv6

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node defines the IPv6 address configuration of the device when this network access point is used.

IPv6 address can be configured in two manners, dynamically and statically. When dynamic IP configuration is used the value of IPv6/AutoConfig node MUST be TRUE. When static IP configuration is used the value of IPv6/AutoConfig MUST be FALSE and IP address, network mask and gateway address are configured via IPv6/IPAddr, IPv6/PrefixLength and IPv6/Gateway.

DNS address(es) can be also configured dynamically and statically. When dynamic DNS configuration is used the value of IPv6/AutoDNS node MUST be TRUE. In case of static DNS configuration the value of that node MUST be FALSE and the static DNS address can be configured using IPv6/DNS/Server/<x>/Addr.

IP/IPv6/AutoConfig

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

If TRUE (or if this optional leaf node is absent), the devices's IPv6 configuration is generated automatically. If FALSE, the device's IPv6 configuration is provided in the IPv6 subtree. The specific mechanism used by the device to configure its IPv6 interface is implementation specific and out of scope of this specification. However, this facility is anticipated by the standardized address configuration strategies detailed in the following references: [RFC3315] and [RFC2462].

IP/IPv6/IPAddr

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node specifies the IPv6 address, defined and formatted as string as specified in [RFC4291]. This value is the IPv6 address of the device when connected to this network access point.

IP/IPv6/PrefixLength

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node specifies the IPv6 network address prefix length [RFC4291] of the device as an 7-bit unsigned integer when connected using this network access point as a string as specified in [RFC4291].

IP/IPv6/Gateway

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This optional leaf node specifies the IPv6 address [RFC4291] of the Internet gateway accessible when the device is connected using this network access point as a string as specified in [RFC4291].

IP/IPv6/AutoDNS

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

If TRUE (or if this optional leaf node is absent), the DNS addresses are to be configured automatically (for example using following references [RFC3736] and [RFC3646]. If FALSE the DNS servers are described in the DNS subtree.

IP/IPv6/DNS

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node optionally lists one or more DNS server addresses [RFC3596] for use while the device is connected using this network access point.

IP/IPv6/DNS/Servers

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node lists the DNS name servers [RFC3596] that should be used while the device is connected using this network access point.

IP/IPv6/DNS/Servers/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes DNS server addresses [RFC3596].

IP/IPv6/DNS/Servers/<X>/Addr

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node defines a single DNS server address [RFC4291] as a string as specified in [RFC4291].

IP/IPv6/DNS/SearchList

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node optionally lists the DNS domains that should be added to unqualified domain names when performing name service queries while the device is connected using this network access point [RFC1034].

IP/IPv6/DNS/SearchList/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes items in the DNS search list.

IP/IPv6/DNS/SearchList/<X>/Domain

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node defines a DNS domain to be used in the domain search list [RFC3646].

IP/IPv6/DNS/SearchList/<X>/Priority

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node defines the priority of a DNS domain in the domain search list [RFC1034] as an unsigned 8-bit unsigned integer.

IP/MIPv4

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node defined the Mobile IP Version 4 (MIPv4) configurations [RFC3344].

IP/MIPv4/SharedSecret

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node defines the shared secrets used for securing the MIPv4 signaling [RFC3344].

IP/MIPv4/UserProfile

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node defines the parameters needed for establishing a mobility session with a Home Agent [RFC3344].

IP/MIPv4/Protocol

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node defines the specific parameters for tuning the MIPv4 protocol behaviour [RFC3344].

IP/MIPv4/SharedSecret/AAAKey

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	NO Get

This leaf node defines the shared secret key between the Mobile Phone and the Authorization, Authentication and Accounting (AAA) or Radius Server [RFC3012].

IP/MIPv4/SharedSecret/NAI

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node lists all the Network Access Identifiers (NAI) [RFC4282] to be used in MIP registration.

IP/MIPv4/SharedSecret/NAI/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes the Network Access Identifiers [RFC4282].

IP/MIPv4/SharedSecret/NAI/<X>/Username

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node defines the user name portion of Network Access Identifier (NAI), encoded in UTF-8 string, refer to [RFC4282]. The NAI is of the form user@realm [RFC2794].

IP/MIPv4/SharedSecret/NAI/<X>/Realm

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node defines the realm portion of Network Access Identifier (NAI), encoded in UTF-8 string, refer to [RFC4282]. The NAI is of the form user@realm [RFC2794].

IP/MIPv4/SharedSecret/NAI/<X>/UsePseudo

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

This leaf node defines if the user portion is pseudo generated. When the value is TRUE, pseudo user portion is used, when the values is FALSE user portion provided in user node SHALL be used. The default value is FALSE, which is used when the node is omitted. The way the user portion is generated is technology specific and hence is not specified in this document.

IP/MIPv4/UserProfile/HomeAddr

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node defines the home address of the device. If this node is omitted then the home address can be requested dynamically from the network [RFC3344]. The address presented as a string in dotted-decimal notation.

IP/MIPv4/UserProfile/HA

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node lists Home Agent (HA) parameters.

IP/MIPv4/UserProfile/HA/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node defines the Home Agents used for MIPv4 registration.

IP/MIPv4/UserProfile/HA/<X>/HAKey

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	NO Get

This leaf node defines the shared secret key between the Mobile Phone and the Home Agent (HA) [RFC3344].

IP/MIPv4/UserProfile/HA/<X>/HAAddr

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node specifies the Home Agent (HA) address. If this node is omitted then the HA address is obtained dynamically from the network [RFC3344].

IP/MIPv4/UserProfile/HA/<X>/HAPrefixLen

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node specifies the home network prefix length of the Home Agent (HA) [RFC3344] as an 32-bit unsigned integer. If the node is omitted the way how the HA prefix is detected is implementation specific.

IP/MIPv4/UserProfile/HA/<X>/HASpi

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the Security Parameter Index (SPI) for the MIP authentication of registration between the device and the Home Agent (HA) [RFC3344] as a 32-bit unsigned integer.

IP/MIPv4/UserProfile/AAASpi

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the SPI for the MIP authentication of registration between the device and the AAA or Radius Server [RFC3012] as a 32-bit unsigned integer.

IP/MIPv4/Protocol/RevTun

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

This leaf node defines if reverse tunneling between a) in FA mode, the FA and the HA b) in CoA mode, the MN and the HA [RFC3024]. When the value is TRUE, reverse tunneling is used and when the value is FALSE reverse tunneling is not used. The default value is FALSE, which is used when the node is omitted.

IP/MIPv4/Protocol/RetryCount

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the maximum number of registration retry attempts [RFC3344] as an 8 bit unsigned integer. Thi minimum value is one an the default value is 3, which is used when the node is omitted.

IP/MIPv4/Protocol/RetryTimer

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the initial registration timer used in before new registration attempt as an unsigned integer. Exponential backoff algorithm defines the time interval between subsequent registration attempts [RFC3344]. The default value is 1 second, which is used when the node is omitted. The minimum value is 1 and the maximum value is 16.

IP/MIPv4/Protocol/RegPeriodRel

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the relative re-registration period. It defines the period in percentages, when the re-registration process is started. E.g. if the re-registration lifetime is 100 minutes and the relative re-registration lifetime is 90%, then the re-registration process MUST be started after 90 minutes [RFC3344]. The default value is 90%, which is used when the node is omitted.

IP/MIPv4/Protocol/RegPeriod

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the registration period. It defines the number of minutes prior to the end of the registration period, when re-registration process is started. E.g. If the registration lifetime is 3600 seconds and the re-registration period is 600 seconds, the re-registration process MUST be started after 50min at the registration [RFC3344]. Default value is 600 seconds, which is used when the node is omitted. The minimum value is 1sek and the maximum value is 65535 sec.

IP/MIPv4/Protocol/NatTraversal

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

This leaf node defines if Network Address Translation (NAT) traversal (UDP tunneling) is used. When the value is TRUE, NAT traversal is used. When the value is FALSE, NAT traversal is not used [RFC3519]. Default value is FALSE, which is used when the node is omitted.

IP/MIPv4/Protocol/Mode

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node defines the MIP mode that is used. The default value for mode node is CO, which is used when the node is omitted. The allowed values for this node is:

Value	Description
CO	Co-located CoA Mode. [RFC3344]
FA	Foreign Agent Mode [RFC3344] (direct delivery style)
FA-ENCAPS	Foreign Agent Mode [RFC3024] (encapsulating delivery style)

Table 1: Values of Mode in MIPv4/Protocol

IP/MIPv6

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node defined the Mobile IP Version 6 (MIPv6) configurations [RFC3775].

IP/MIPv6/SharedSecret

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node defines the shared secrets used for securing the MIPv6 signaling [RFC3775].

IP/MIPv6/UserProfile

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node defines the parameters needed for establishing a mobility session with a Home Agent [RFC3775].

IP/MIPv6/Protocol

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node defines the specific parameters for tuning the MIPv6 protocol behaviour.

IP/MIPv6/SharedSecret/AAKey

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	NO Get

This leaf node defines the shared secret key between the Mobile Phone and the Authorization, Authentication and Accounting (AAA) or Radius Server [RFC4285].

IP/MIPv6/SharedSecret/NAI

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node lists all the Network Access Identifiers (NAI) [RFC4283] to be used in MIP registration.

IP/MIPv6/SharedSecret/NAI/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Relace & Add

This interior node distinguishes the Network Access Identifiers [RFC4283].

IP/MIPv6/SharedSecret/NAI/<X>/Username

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node defines the user name portion of Network Access Identifier (NAI), encoded in UTF-8 string, refer to [RFC4282]. The NAI is of the form user@realm [RFC4283].

IP/MIPv6/SharedSecret/NAI/<X>/Realm

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node defines the realm portion of Network Access Identifier (NAI), encoded in UTF-8 string, refer to [RFC4282]. The NAI is of the form user@realm [RFC4283].

IP/MIPv6/SharedSecret/NAI/<X>/UsePseudo

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

This leaf node defines if the user portion is pseudo generated. When the value is TRUE, pseudo user portion is used, when the values is FALSE user portion provided in user node SHALL be used. The default value is FALSE, which is used when the node is omitted. The way how the user portion is generated is technology specific and hence is not specified in this document.

IP/MIPv6/UserProfile/HomeAddr

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node defines the home address of the device. If this node is omitted then the home address can be requested dynamically from the network [RFC3775]. The address is presented as a hexadecimal string [RFC4291].

IP/MIPv6/UserProfile/HomePrefixLen

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the prefix length of the home address as an 7-bit unsigned integer. If the node is omitted the way how the prefix length is detected is implementation specific.

IP/MIPv6/UserProfile/HA

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node lists Home Agent (HA) parameters [RFC3775].

IP/MIPv6/UserProfile/HA/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node defines the Home Agents used for MIPv6 registration [RFC3775].

IP/MIPv6/UserProfile/HA/<X>/HAKey

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	NO Get

This leaf node defines the shared secret key between the Mobile Phone and the HA [RFC4285].

IP/MIPv6/UserProfile/HA/<X>/HAAddr

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node specifies the Home Agent (HA) address. If this leaf node is omitted, dynamic home agent address discovery will be used [RFC3775]. The address is presented as a hexadecimal string [RFC4291].

IP/MIPv6/UserProfile/HA/<X>/HAPrefixLen

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node specifies the home network prefix length of the HA [RFC3775] as an 7-bit unsigned integer. If this node is omitted the way how the prefix length is detected is implementation specific.

IP/MIPv6/UserProfile/HA/<X>/HASpi

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the unsigned 32-bit SPI for the MIP authentication of registration between the device and the HA [RFC4285].

IP/MIPv6/UserProfile/AAASpi

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the unsigned 32-bit SPI for the MIP authentication of registration between the device and the AAA or Radius Server [RFC4285].

IP/MIPv6/Protocol/RouteOpt

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

This leaf node defines whether the route optimization feature is enabled [RFC3775]. When the value is TRUE route optimization SHALL be used, when the value is FALSE route optimization SHALL not be used. The default value is FALSE, which used when the node is omitted.

IP/MIPv6/Protocol/RetryCount

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the maximum number of binding update retry attempts [RFC3775]. The default value is 3, which is used when the node is omitted. This is an 8 bit unsigned integer.

IP/MIPv6/Protocol/RetryTimer

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the initial binding update timer used in before new binding attempt. Exponential backoff algorithm defines the time interval between subsequent binding attempts [RFC3775]. The default value is 1 second, which is used when the node is omitted. Allowed value range is 1-10 seconds for this node.

IP/MIPv6/Protocol/BindingLifeTimeRel

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the binding period. It defines the binding period in percentages, when the rebinding process is started. E.g. if the binding lifetime is 100 minutes and the relative binding lifetime is 90%, then the rebinding process MUST be started after 90 minutes [RFC3775]. The default value is 90%, which is used when the node is omitted. Valid value range for this node is 0 to 100.

IP/MIPv6/Protocol/BindingLifeTime

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node defines the binding lifetime [RFC3775] in seconds proposed to the Home Agent in a binding update. Default value is 3600 seconds, which is used when the node is omitted. Allowed value range for this node is 4 to 262140 seconds.

IP/MIPv6/Protocol/SignalingProtection

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get.

This leaf node defines what type of protection is used for MIPv6 signaling messages between MN-HA. This node can be used to define either IPsec [RFC4877] or authentication protocol [RFC4285] is used. If the node is omitted the signaling protection selection is implementation specific. The allowed values for this node is:

Value	Description
IPSEC	IPsec + IKEv2 [RFC4877]
AUHOPT	Authentication Protocol [RFC4285]

Table 2: Values of signaling_protection in MIPv6/Protocol

IP/IPv4/Ext**IP/MIPv4/Ext****IP/IPv6/Ext****IP/MIPv6/Ext**

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node designates the single top-level branch of this management object tree into which vendor extensions MAY be supported, 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 one of these Ext sub-trees.

IP/IPv4/Ext/UniqueVendorName**IP/MIPv4/Ext/UniqueVendorName****IP/IPv6/Ext/UniqueVendorName****IP/MIPv6/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.

Linger

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This optional leaf node, if present, defines how long a connection should be kept active without any traffic. The value is expressed in seconds as a 16 bit unsigned integer.

AuthInfo

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node optionally provides authentication credentials to support various forms of network access point authentication.

AuthInfo/AuthType

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node identifies one type of authentication protocol used by the represented network access point. The means for selecting a particular authentication protocol to be used when connecting to the network access point is out of scope of this specification—this node merely links the specified authentication method to the AUTHNAME and AUTHSECRET.

Authorities of reference and allowed values for these authentication protocols are bearer-specific and are not listed here. Implementers are referred to the bearer specifications and the listed normative references describing each protocol for the proper usage context and details of each authentication type.

AuthInfo/AuthName

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	chr	Get

The *name* (or user id) credential.

AuthInfo/AuthSecret

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

The *secret* (or password) credential.

Validity

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node is used to indicate where this NAP is valid.

Validity/<x>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes different Validity rules.

Validity/<x>/Country

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This optional leaf node indicates a Mobile Country Code as defined by ITU-T [E212]. The parameter is used to identify in which country this NAP is valid.

Validity/<x>/Network

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This optional leaf node indicates a list of comma separated Mobile Network Codes in decimal format as defined by ITU-T [E212]. The parameter is used to identify in which network this NAP is valid.

Validity/<x>/SID

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This optional leaf node indicates a list of comma separated System IDs in decimal format as defined by [TIA/EIA-136-005A]. The parameter is used to identify in which SID this NAP is valid.

Validity/<x>/SOC

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This optional leaf node indicates a System Operator Code as defined by [TIA/EIA-136-005A]. The parameter is used to identify in which SOC this NAP is valid.

Validity/<x>/ValidUntil

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This optional leaf node defines the end of the (time) period of validity. The parameter is expressed as a 32bit unsigned integer in seconds, from the time it is received by the client device. When the server receives this value, for example using the Get Command, the device MUST calculate and deliver the remaining valid time in seconds.

NetworkCategory

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This optional leaf node describes the network category name that can be used to categorize NAP definitions. The value is an arbitrary identifier, e.g. INTERNET, and it can be shared by different NAP definitions.

BearerType

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node is used to define the bearer type used to reach this network access point. Conforming management objects describing NAPs reachable over bearers MUST use the associated BearerType value specified in the sub-tree management objects specification representing the bearer-specific configuration parameters. Management objects describing NAPs reachable over bearers not specified are still considered conforming if they otherwise conform to this management object specification. If a BearerType value is not understood, the NAP object MUST be ignored.

BearerParams

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node defines the specific parameters of the bearer concerned with BearerType. These parameters are used to reach this network access point.

BearerParams/3GPPCS**BearerParams/3GPPCS/...****BearerParams/3GPPPS****BearerParams/3GPPPS/...****BearerParams/CDMA****BearerParams/CDMA/...****BearerParams/WLAN****BearerParams/WLAN/...****BearerParams/...****BearerParams/.../...**

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

The Names of BearerParams child nodes (eg. 3GPPPS) and the bearer parameters are defined in separate specifications. Nodes in these sub-trees represent the bearer-specific configuration parameters. Bearer parameters in these sub-trees are defined in separate specifications.

Ext

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node designates the single top-level branch of the NAP DM management object tree into which vendor extensions MAY be supported, 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 one of these 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 su-btree below a *UniqueVendorName* interior node is implementation-specific.

6.5 Proxy Object

6.5.1 Introduction

The Proxy object is used to configure and update proxy settings for network proxies of various types in a standardized way.

OMA DM protocol compatibility for the Proxy MO is version 1.2 or any later compatibility version to this version.

6.5.2 Graphical Representation (Informative)

The following figure shows the structure of the Proxy management object:

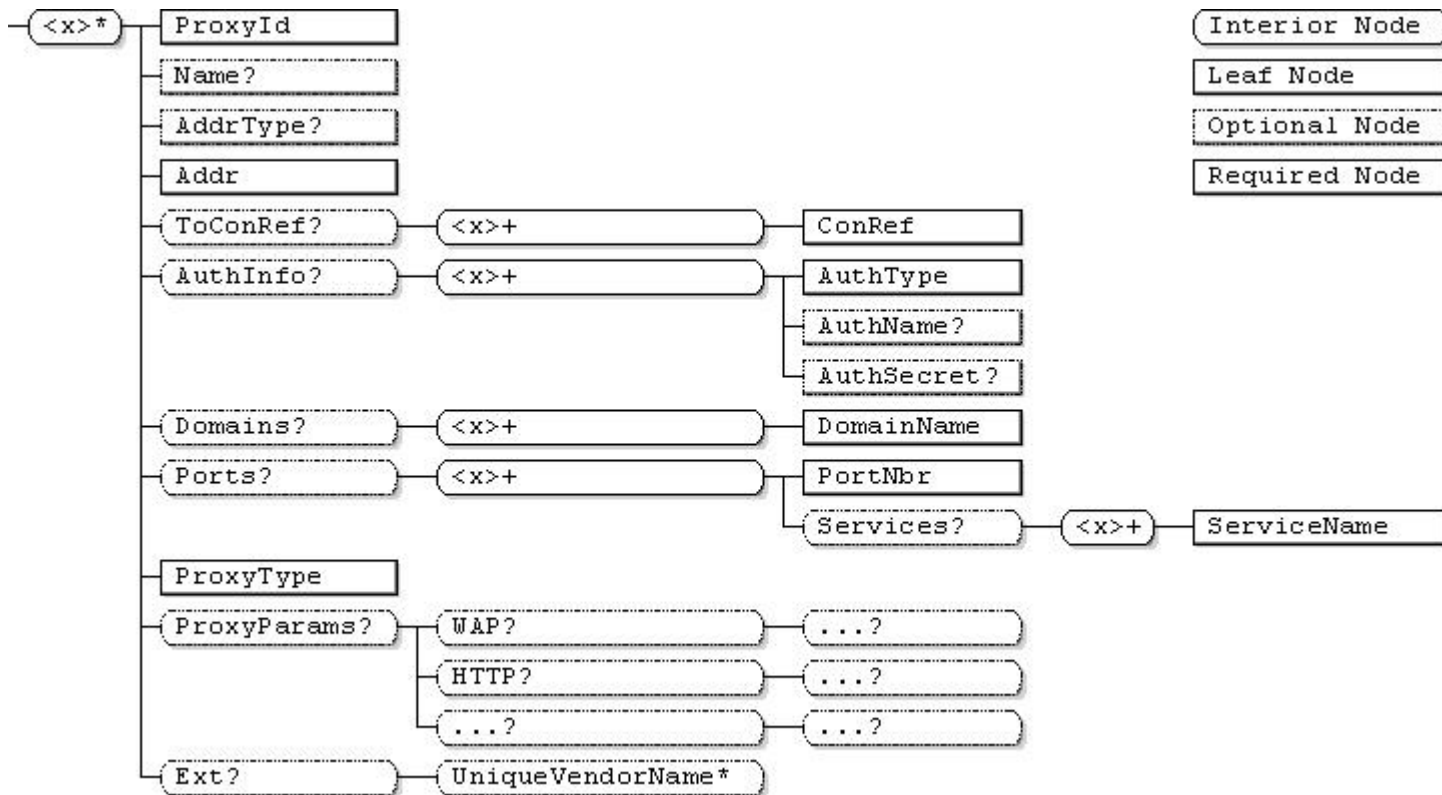


Figure 3: Proxy Management Object (Informative)

6.5.3 Node Descriptions

.../<x>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node specifies the unique object id of a proxy management object. The purpose of this interior node is to group together the parameters of a single proxy object. The ancestor elements of this node define the position in the management tree of the proxy object. But the structure of the DM tree and hence positions in the tree of management objects is out of scope of this specification. Management Object Identifier for the Proxy MO MUST be: "urn:oma:mo:oma-connmo-proxy:1.0".

ProxyId

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node uniquely identifies this Proxy Management Object.

Name

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node provides an optional human readable name for the proxy.

AddrType

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This optional leaf node specifies the type of proxy address supplied as the **Addr** leaf node value. Authorities of reference and allowed values for **AddrType** are proxy-specific and are not listed here. Implementers are referred to the proxy specifications and the listed normative references describing each protocol for the proper usage context and details of each address type.

If the proxy type-specific parameter specification does not define a value for this node then the default value "IPv4" MUST be assumed and the **Addr** node MUST represent an IPv4 address [AUTH-RFC791] represented in string form dotted-decimal CIDR notation.

Addr

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node provides the address of the proxy. The Addr node can specify addresses of different types, for example an IP address or an SME number. The type of address in the field is defined by the AddrType node. This node MUST be present for the proxy object to be valid.

ToConRef

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node lists network access points (or other connection objects) used by this proxy to reach a network. One proxy could utilize any of several different network access points.

ToConRef/<x>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes the connection object identifier nodes. There must be exactly one ConRef node for each of these interior nodes.

ToConRef/<x>/ConRef

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This node specifies a reference to the connectivity. It is expected that either a Proxy or NAP MO is specified, but other, implementation-specific connections may be referenced..

AuthInfo

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node optionally provides authentication credentials to support various forms of proxy authentication.

AuthInfo/<x>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes different AuthInfo parameters.

AuthInfo/<x>/AuthType

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node identifies one type of authentication protocol used by the represented proxy. The means for selecting a particular authentication protocol to be used is out of scope of this specification—this node merely links the specified authentication method to the AUTHNAME and AUTHSECRET. The AuthType value must be unique within a proxy MO.

Authorities of reference and allowed values for these authentication protocols are proxy-specific and are not listed here. Implementers are referred to the proxy specifications and the listed normative references describing each protocol for the proper usage context and details of each authentication type.

AuthInfo/<x>/AuthName

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The *name* (or user id) credential.

AuthInfo/<x>/AuthSecret

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	NO Get

The *secret* (or password) credential.

Domains

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional node lists the domains which can be reached via this proxy.

Domains/<x>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes the domain name nodes.

Domains/<x>/DomainName

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node names a single domain which can be reached via this proxy.

Ports

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node lists the ports which can be traversed via this proxy. A port number is defined for each port along with an optional list of services offered by the proxy at that port.

Ports/<x>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes the ports opened by this proxy.

Ports/<x>/PortNbr

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node defines the number of a single port as a 16bit unsigned integer which is opened by this proxy.

Ports/<x>/Services

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node lists the services offered at the specified port.

Ports/<x>/Services/<y>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

These interior nodes distinguish the services offered at the specified port.

Ports/<x>/Services/<y>/ServiceName

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node identifies the name of a single service offered at the specified port.

ProxyType

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node is used to define the proxy type. A conforming management object describing a proxy MUST use the associated ProxyType value specified in the sub-tree management objects specification representing the proxy-specific configuration parameters. Management objects describing types of network proxy not specified are still considered conforming if they otherwise conform to this management object specification. If a ProxyType value is not understood, the Proxy object MUST be ignored.

ProxyParams

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node defines the specific parameters of the proxy concerned with ProxyType. These parameters are used to configure the proxy.

ProxyParams/WAP**ProxyParams/WAP/...****ProxyParams/HTTP****ProxyParams/HTTP/...****ProxyParams/...****ProxyParams/.../...**

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

Nodes in these sub-trees represent the configuration parameters specific to a single proxy type. Specific Proxy support in these sub-trees is defined in separate specifications.

Ext

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node designates the single top-level branch of the Proxy DM management object tree into which vendor extensions MAY be supported, 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 one of these 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 subtree 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-V1_0-20081107-A	11 Nov 2008	Approved by TP TP Ref#: OMA-TP-2008-0438-INP_ConnMO_V1_0_RRP_for_Notification