Standardized Connectivity Management Objects IP Parameters

For use with OMA Device Management

Candidate Version 1.0 – 12 Aug 2008

Open Mobile Alliance

OMA-DDS-DM_ConnMO_IP-V1_0- 20080812-C

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.

Contents

Figures

Tables

1. Scope

This document defines Internet Protocol (IP) specific parameters used together with the standardized connectivity management object [CONNMO] in order to have a complete standardized Network Access Point definition, generic to various bearers, in the OMA DM management tree.

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] *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:

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

[RFC1034] *RFC1034, Domain Names - Concepts and Facilities*, P. Mockapetris, November 1987, URL:http://www.ietf.org/rfc/rfc1034.txt

[RFC1035] *RFC1035, Domain Names - Implementation and Specification*, P. Mockapetris, November 1987, URL:http://www.ietf.org/rfc/rfc1034.txt

[RFC2131] *RFC 2131, Dynamic Host Configuration Protocl*, R. Droms, March 1997, URL:http://www.ietf.org/rfc/rfc2131.txt

[RFC2132] *RFC2132, DHCP Options and BOOTP Vendor Extensions*, S. Alexander, March 1997, URL:http://www.ietf.org/rfc/rfc2132.txt

[RFC2462] *RFC 2462, IPv6 Stateless Addess Autoconfiguration*, S. Thomson, T. Narten, December 1998, URL:http://www.ietf.org/rfc/rfc2462.txt

[RFC2794] *RFC 2794, Mobile IP Network Access Identifier Extension for IPv4*, P. Calhoun, March 2000, URL:http://www.ietf.org/rfc/rfc2794.txt

[RFC3012] *RFC 3012, Mobile IPv4 Challenge/Response Extensions*, C. Perkins, P. Calhoun, November 2000, URL:http://www.ietf.org/rfc/rfc3012.txt

[RFC3024] *RFC 3024, Reverse Tunneling for Mobile IP, revised*, G. Montenegro, January 2001, URL:http://www.ietf.org/rfc/rfc3024.txt

[RFC3315] *RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, July 2003, URL:http://www.ietf.org/rfc/rfc3315.txt

[RFC3330] *RFC 3330, Special-Use IPv4 Address*, IANA, September 2002, URL:http://www.ietf.org/rfc/rfc3330.txt

[RFC3344] *RFC 3344, IP Mobility Support for IPv4*, C. Perkins, August 2002, URL:http://www.ietf.org/rfc/rfc3344.txt

[RFC3519] *RFC 3519, Mobile IP Traversal of Network Address Translation (NAT) Devices*, Apr 2003, URL:http://www.ietf.org/rfc/rfc3519.txt

[RFC3596] *RFC3596, DNS Extensions to Support IP Version 6*, S. Thomson, October 2003, URL:http://www.ietf.org/rfc/rfc3596.txt

[RFC3646] *RFC 3646, DNS Configuration options for Dynamic Host Configuration Protocol (DHCPv6)*, R.Droms, December 2003, URL:http://www.ietf.org/rfc/rfc3646.txt

[RFC3736] *RFC 3736, Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*, R. Droms, April 2004 , URL:http://www.ietf.org/rfc/rfc3736.txt

[RFC3775] *RFC 3775, Mobility Support in IPv6*, D. Johnson, C. Perkins, J. Arkko, June 2004, URL:http://www.ietf.org/rfc/rfc3775.txt

[RFC4282] *RFC 4282, The Network Access Identifier*, B. Aboba, M. Beadles, December 2005, URL:http://www.ietf.org/rfc/rfc4282.txt

[RFC4283] RFC 4283, *Mobile Node Identifier Option for Mobile IPv6 (MIPv6)*, A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury, November 2005, URL:http://www.ietf.org/rfc/rfc4283.txt

[RFC4285] *RFC 4285, Authentication Protocol for Mobile IPv6*, A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury, January 2006, URL:http://www.ietf.org/rfc/rfc4285.txt

[RFC4291] *RFC 4291, IP Version 6 Addressing Architecture*, R. Hinden, S. Deering, February 2006, URL:http://www.ietf.org/rfc/rfc4291.txt

[RFC4877] *RFC 4877, Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture*, V. Devarapalli, F. Dupont, April 2007, URL:http://www.ietf.org/rfc/rfc4877.txt

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

AAA	Authentication, Authorization and Accounting
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
GW	Gateway
HA	Home Agent
IP	Internet Protocol
MIP	Mobile Internet Protocol
NAI	Network Access Identifier
NAT	Network Address Translation
OMA	Open Mobile Alliance
SPI	Security Parameter Index

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 Internet Protocol (IP) management object, which is part of the general *Network Access Point* management object allowing vendor specific extensions. This specification is suitable for configuring access points in various bearers.

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. IP 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 IP specific subtree that is placed under the general NAP management object in order to enable IP specific parameter manipulation.

6.2 Definitions for IP MO

The IP sub-tree specified in this document MUST be placed under the IP node in [CONNMO].

6.3 Graphical Representation (Informative)

The following figure provides the structure of IP management object.

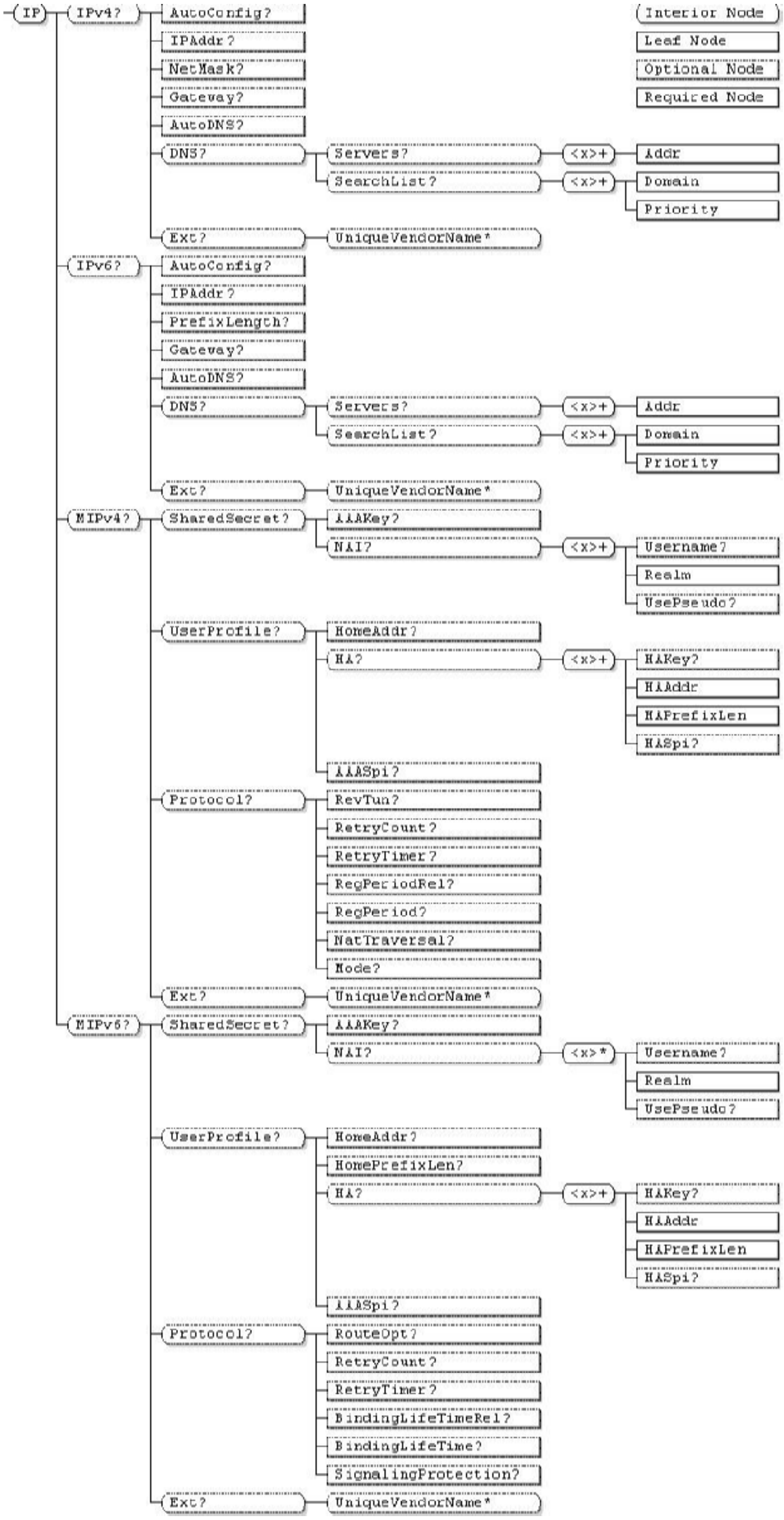

Figure 1. IP Management Object

6.4 Node Descriptions

IP

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

This interior node is parent node of the IP sub-tree. Management Object Identifier for this MO MUST be: "urn:oma:mo:oma-connmo-ip:1.0".

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.

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].

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.

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.

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.

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.

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].

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.

IPv4/DNS/Servers/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes DNS server addresses [RFC1034].

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.

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.

IPv4/DNS/SearchList/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes items in the DNS search list.

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.

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.

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.

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].

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.

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].

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].

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 sub-tree.

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.

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.

IPv6/DNS/Servers/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes DNS server addresses [RFC3596].

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].

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].

IPv6/DNS/SearchList/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

This interior node distinguishes items in the DNS search list.

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].

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.

MIPv4

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

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

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].

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].

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].

MIPv4/SharedSecret/AAAKey

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

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

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.

MIPv4/SharedSecret/NAI/<X>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get

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

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].

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].

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.

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.

MIPv4/UserProfile/HA

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node lists Home Agent (HA) parameters.

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.

MIPv4/UserProfile/HA/<X>/HAKey

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

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

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].

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.

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.

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.

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.

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.

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 algoritm 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.

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.

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.

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.

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

MIPv6

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

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

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].

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].

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.

MIPv6/SharedSecret/AAAKey

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

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

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.

MIPv6/SharedSecret/NAI/<X>

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

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

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].

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].

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.

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].

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.

MIPv6/UserProfile/HA

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

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

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].

MIPv6/UserProfile/HA/<X>/HAKey

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

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

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].

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.

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].

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].

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 valus is FALSE route optimization SHALL not be used. The default value is FALSE, which used when the node is omitted.

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.

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.

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.

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.

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]
AUTHOPT	Authentication Protocol [RFC4285]

Table 2: Values of signaling_protection in MIPv6/Protocol

IPv4/Ext

MIPv4/Ext

IPv6/Ext

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.

IPv4/Ext/UniqueVendorName

MIPv4/Ext/UniqueVendorName

IPv6/Ext/UniqueVendorName

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.

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
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-DDS-DM_ConnMO_IP	17 Oct 2007	All	First draft.
	6 Nov 2007	7	Editorial update from the approved ETR
	4 Dec 2007	All	Editorial updates after closure review
	8 Jan 2008	All	Editorial update from the closure review
	25 Feb 2008	All	Editorial update from closure review + new template + New table format for node definitions.
	26 Feb 2008	6.4	Editorial updates
	15 Apr 2008	6	Editorial update: Updating according to the move to RR.
	16 April 2008	6	Updated with CR: OMA-DM-ConnMO-2008-0002-CR_Editorial_Update_of_IP Including editorial update.
	9 May 2008	2, 6	Editorial update according to consistency review comment L001 & partly L002
	23 Jun 2008	6.4	Editorial update to solve consistency review comment L002.
Candidate Versions OMA-DDS-DM_ConnMO_IP	12 Aug 2008	n/a	Status changed to Candidate by TP TP ref#: OMA-TP-2008-0286-INP_Connectivity_Management_Objects_V1_0_RRP_for_Candidate_Approval