Attachment 4-2-6

WiMAX Forum® Network Architecture

Architecture, detailed Protocols and Procedures

WiMAX Over-The-Air Provisioning & Activation Protocol
based on OMA DM

WMF-T33-104-R015v02

WiMAX Forum® Network Architecture

Architecture, detailed Protocols and Procedures

WiMAX Over-The-Air Provisioning & Activation Protocol
based on OMA DM Specifications

WMF-T33-104-R015v02

WiMAX Forum® Approved

(2009-11-21)

WiMAX Forum Proprietary

Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. Revision History

Date	Version	Description
March 26, 2008	V01	
November 6, 2009	V02	Implemented CRs 1001, 1005, 1007.

2. Document Scope

Many different device types will be enabled by Worldwide Interoperability for Microwave Access (WiMAX) technologies, such as notebooks, ultra mobile devices (UMD), handsets, and consumer electronics. A WiMAX service provider would require a dynamic over the air provisioning solution to configure activate, enable subscription for, and manage these device types.

This document specifies Stage 2 and Stage 3 specifications for Over-The-Air (OTA) Provisioning and Activation based on OMA DM protocol for Model B WiMAX enabled devices (WiMAX MS).

The WiMAX Over-The-Air General Provisioning System Specification describes end to end over the air provisioning and activation [OTAGEN].

3. Abbreviations and Definitions

3.1 Abbreviations

Refer to section 3.1 of [OTAGEN] for other abbreviations which are not mentioned in this section.

3.2 Terms & Definitions

Term	Definition
Channel Plan	A Channel Plan is used by the device to speed up Network Access Provider (NAP) discover process. It contains physical information such as channel bandwidth (BW), center frequency, and PHY profile.
Contractual Agreement Preference List (CAPL)	A list consisting of Network Access Providers (NAP) preferred to be connected to the home network directly.
Device Management System	A background system capable to interact with a (set of) Device(s) for the purpose of Device Management.
DM System	A background system capable of interacting with a (set of) Devices for the purpose of DM.
Host Device	Refers to a standalone device or a submodule in which WiMAX modem (chipset) is embedded. This is the device that is to be managed, associated with MSID, and SHOULD appear in DevInfo or DevDetail Management Object (MO). Examples of the Host Devices are: 1) Removable Modem (e.g., Personal Computer (PC) Card, USB Modem, etc.) with an embedded WiMAX chipset; 2) WiMAX submodule physically attached to a Customer Premises Equipment (CPE); 3) WiMAX submodule temporarily or permanently built into a laptop; 4) WiMAX enabled CE (e.g., Digital Camera, PMP, etc.) that has an embedded WiMAX chipset; 5) Embedded laptop which has WiMAX submodule permanently built in.
NAP Based Channel Plan	A Channel Plan which is a subset of Root Channel Plan and is associated with a NAP.
Prior Connect Info	Specified in [NWGSTG3]
Roaming Agreement Preference List (RAPL)	A list consisting of Network Service Providers preferred to be connected when roaming.
Root Channel Plan	A Channel Plan which contains all Channel Plan Entries.
WiMAX Radio Module	Refers to WiMAX radio chipset and subsystem present in the host device and that enables WiMAX radio connectivity for the Host Device.
Terminal Equipment	Refers to the device in which host device is temporarily (through PC card slot, USB port etc.) or permanently (for example, embedded laptop) inserted to get WiMAX connectivity. Examples of terminal equipment are: 1) PC which has a PC card slot for peripheral devices, and PC Card (host device) is inserted in PC to get WiMAX connectivity; 2) WiMAX CPE Gateway which has a WiMAX sub-module; 3) Embedded laptop which has WiMAX sub-module permanently built in; 4) Consumer electronics that has a WiMAX submodule

Refer to section 3.2 of [OTAGEN] for other Terms & Definitions which are not mentioned in this section.

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

3.3 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 [RFC 2119].

4. References

	Description
[DMACMO]	"White Paper on Provisioning Objects". Open Mobile Alliance. OMA-WP-AC-MO. URL:http://www.openmobilealliance.org
[DMBOOT]	"OMA DM Bootstrap, Version 1.2". Open Mobile Alliance. OMA-TS-DM_Bootstrap-V1_2. URL:http://www.openmobilealliance.org
[DMCONNMO]	"Standardized Connectivity Management Objects, Version 1.0". Open Mobile Alliance. OMA-DDS-DM_ConnMO-V1_0. URL:http://www.openmobilealliance.org
[DMDDFDTD]	"OMA DM Device Description Framework Version 1.2 Document Type Definition". Open Mobile Alliance. OMA-SUP-dtd_dm_ddf-v1_2. URL:http://www.openmobilealliance.org
[DMNOTI]	"OMA DM Notification Initiated Session, Version 1.2". Open Mobile Alliance. OMA-TS-DM_Notification-V1_2. URL:http://www.openmobilealliance.org
[DMPRO]	"OMA DM Protocol, Version 1.2". Open Mobile Alliance. OMA-TS-DM_Protocol-V1_2. URL:http://www.openmobilealliance.org
[DMRD]	" DM Requirements Document, Version 1.2". Open Mobile Alliance. OMA-RD-DM-V1_2. URL:http://www.openmobilealliance.org
[DMREPU]	"OMA DM Representation Protocol, Version 1.2". Open Mobile Alliance. OMA-TS-DM_RepPro-V1_2. URL:http://www.openmobilealliance.org
[DMSEC]	"OMA DM Security, Version 1.2". Open Mobile Alliance. OMA-TS-DM_Security-V1_2. URL:http://www.openmobilealliance.org
[DMSYNCHTTP]	"SyncML HTTP Bidning, Version 1.2.1". Open Mobile Alliance. OMA-TS-SyncMLBinding-V1_2_1. URL: http://www.openmobilealliance.org
[DMSTDOBJ]	"OMA DM Standardized Objects, Version 1.2". Open Mobile Alliance. OMA-TS-DM_StdObj-V1_2. URL:http://www.openmobilealliance.org
[DMTND]	"OMA DM Tree and Description, Version 1.2". Open Mobile Alliance. OMA-TS-DM_TND-V1_2. URL:http://www.openmobilealliance.org
[DMTNDS]	"Standard Connectivity MOs, Version 1.0". Open Mobile Alliance. OMA-DDS-DM_ConnMO -V1_0. URL:http://www.openmobilealliance.org
[DMEAPMO]	"Standard Connectivity Management Objects EAP Paramets, Version 1.0". Open Mobile Alliance. OMA-DDS-DM_ConnMO_EAP-V1_0. URL:http://www.openmobilealliance.org
[DMIPMO]	"Standard Connectivity MOs Internet Protocol (IP) Paramets, Version 1.0". Open Mobile Alliance. OMA-DDS-DM_ConnMO_IP-V1_0. URL:http://www.openmobilealliance.org
[ERELDCP]	"Enabler Release Definition for Client Provisioning, Version 1.1". Open Mobile Alliance. OMA-ERELD-ClientProvisioning-V1_1. URL:http://www.openmobilealliance.org
[ERELDDM]	"Enabler Release Definition for OMA Device Management Approved Version 1.2". Open Mobile Alliance. OMA-ERELD-DM-V1_2. URL:http://www.openmobilealliance.org
[FUMO]	"Firmware Update Management Object (FUMO), Version 1.0". Open Mobile

	Description
	Alliance. OMA-TS-DM-FUMO-V1_0. URL:http://www.openmobilealliance.org
[IANA-EAPTYPE]	http://www.iana.org/assignments/eap-numbers
[NWGSTG2P3]	WiMAX Forum, T32-004-R015v01, “Architecture Tenets, Reference Model and Reference Points” Part3, Release 1.5
[NWGSTG3]	WiMAX Forum, T33-001-R015v01, “Detailed Protocols and Procedures, Base Specification", Release 1.5
[NWGMSPRO]	WiMAX Forum Mobile System Profile
[OTAGEN]	WiMAX Forum T33-103-R015v04, "Architecture, detailed Protocols and Procedures, WiMAX Over-The-Air General Provisioning System Specification", Release 1.5
[PUSHOTA]	“Push OTA Protocol”, Open Mobile Alliance, WAP-235-PushOTA-20010425-a, URL:http://www.openmobilealliance.org
[PUSHMSG]	“Push Message”, Open Mobile Alliance, WAP-251-PushMessage-20010322-a, URL:http://www.openmobilealliance.org
[RFC1766]	“Tag for the Identification of Language”, H Alvestrand, March 1995, URL:http://www.ietf.org/rfc/rfc1766.txt
[RFC2141]	“URN Syntax”, R. Moats, MAY 1997, URL:http://www.ietf.org/rfc/rfc2141.txt
[RFC4282]	“The Network Access Identifier,” URL: http://www.ietf.org/rfc/rfc4282.txt
[UAProf]	“User Agent Profile - Approved Version 2.0 – 06 Feb 2006,” Open Mobile Alliance URL: http://www.openmobilealliance.org/release_program/uap_v2_0.html
[XML]	W3C Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation, Version 6-October-2000.
[802.16]	IEEE 802.16e-2005 March 2006, Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands

1 Refer to section 4 of [OTAGEN] for other references which are not mentioned in this section.

5. OMA DM Protocol Overview

5.1 Introduction to OMA DM Protocol

The OMA DM Protocol [DMPRO] defines a management framework and a protocol for various management procedures. This section describes briefly the core components of OMA DM architecture.

5.1.1 Management Tree

Every device that supports OMA DM SHALL contain a management tree. All available MOs are logically grouped in the MS as a hierarchical tree structure called the management tree. Thus, the management of a service or application in the DM framework requires accessing nodes in the management tree corresponding to the service or application.

The management tree is structured on the basis of services, and applications. Each node in the management tree is addressed with a URI as described in the OMA DM Tree and Descriptions specification [DMTND].

Using the Device Description Framework (DDF) [DMDDFDTD] of the management tree, and the tree exchange mechanism [DMTND], the management server knows the URI [DMPRO] of the location to be referred to for a specific management action.

In the management tree, WiMAX objects would be specific sub-trees. Similarly application objects from other sub-trees of the management tree. Annex A describes the WiMAX management tree.

5.1.2 Device Description

The MOs in the management tree are made known to the management server through the DDF of the MS. The DDF document is an XML document [XML], which is made available to the management server. The DDF Document Type Definition (DTD) specified in [DMDDFDTD] is used to describe the management syntax and semantics for a particular MS.

The DDF description gives the properties, such as type, format, description etc of each object, and their relative location in the management tree. The server learns the MOs and how to manage the objects from the DDF description.

The DDF mechanism provides management of new and customized features in the device.

Features common to a class of devices can be grouped and standardized for interoperability and can coexist as a standardized MOs in the management tree of such a device along with non-standardized MOs. The elements, or nodes, that describe the common features of all WiMAX devices described in Annex A of this document, SHALL be grouped into a single standardized WiMAX MO that can be represented using the DDF DTD.

5.1.3 Bootstrap Mechanism

In order for the DM client of a device to initiate a management session, a bootstrap process MUST be performed to provision the device with the required settings to initiate a session with a specific DM server. OMA DM supports three possible methods for the bootstrap process: factory bootstrap, bootstrap from smartcard, or secure server-initiated bootstrap for initial provisioning. The bootstrap mechanism is defined in the OMA DM Bootstrap specification [DMBOOT].

If the network operator desires to ensure interoperability with all devices the bootstrap file interchange SHALL conform to [DMTND].

This document specifies how the server-initiated and WiMAX specific client-initiated bootstrap (WIB) are implemented in WiMAX. The other bootstrap methods are fully implemented in WiMAX as defined in [DMBOOT] except as stated otherwise in this specification.

5.1.4 OMA DM Packages and Messages

In OMA DM, a set of messages exchanged between the DM client and the management server, is conceptually combined into a package. In most situations a package corresponds to a single message, but when large objects are

involved in the transfer, each package is sent over multiple DM messages. A DM message is a well-formed XML document with header and body. The XML specification for OMA DM is described in the protocol specifications [DMREPU].

Limitations on package size, message boundaries etc., are defined in OMA DM representation protocol [DMREPU]. An example of a DM message is shown below.

```
<SyncML xmlns='SYNCML:SYNCML1.1'>
  <SyncHdr>
    <!---header information, credentials>
  </SyncHdr>
  <SyncBody>
    <!--- Message body – commands, alerts>
    <Final/>
  </SyncBody>
</SyncML>
```

Figure 1 - OMA DM Message

The SyncBody container element carries one or more OMA DM commands.

5.1.5 OMA DM Commands

OMA DM protocol allows commands to be executed on a node in the management tree, resulting in a specific management action. The management action can be get, replace, add, delete, execute etc., OMA DM management commands are used to represent the management actions and associated data elements that are transferred between the DM client and the DM server

OMA DM commands are transferred in the XML format defined in [DMREPU].

5.1.6 Notification Message

The OMA DM notification message causes the client to initiate a connection to the management server and begin a management session. The notification is a signed message, which the client can authenticate. There are several fields in the notification message, for example the UI-mode field is used for specifying user interaction when the client receives the notification.

Notification message can also originate within the device, thus triggering the establishment of a session, for example when a timer expires.

The format and security mechanism for OMA DM notification message are described in the OMA DM Notification Initiated Session specification [DMNOTI].

6. WiMAX Over-the-Air Provisioning and Activation Overview based on OMA DM

6.1 Server-initiated Bootstrapping & WIB Methods

This section describes the OMA DM server-initiated bootstrap (case #1) and the DM client-initiated bootstrap (case #2) methods.

The first step of the subscription and provisioning phase is bootstrapping. This step is required to establish a security association between the device and the provisioning server in order to initiate the first management session. Bootstrapping process may take place whenever the device does not have the required information to establish a security association with the server or when it fails to establish it based on the information it has (the definition of fail is not in scope of this document). With the successful execution of the bootstrapping process, a secure path between the device DM client and the DM server can be established and the provisioning process for the device can begin. See [DMSEC] for information concerning the existing OMA DM security mechanisms.

This section describes the OMA DM server-initiated bootstrap (case #1) and the DM client-initiated WIB (case #2) methods.

In the case of #1, the server-initiated bootstrap method is based on the UDP Push method as defined by OMA, where the DM server sends an encrypted OMA DM bootstrap document to the DM client.

In the case of #2, the client-initiated bootstrap method is based on WIB [OTAGEN], where the device gets the bootstrap document from the server using the WIB procedure, i.e., Domain Name Server (DNS) and HTTP GET. The client-initiated bootstrap method is used if the device does not support the server-initiated bootstrap method, e.g., laptops with firewall/NAT that prevent the reception of UDP Push messages.

The Figure 2 illustrates case #1 and case #2 of the UDP Push and WIB bootstrapping methods.

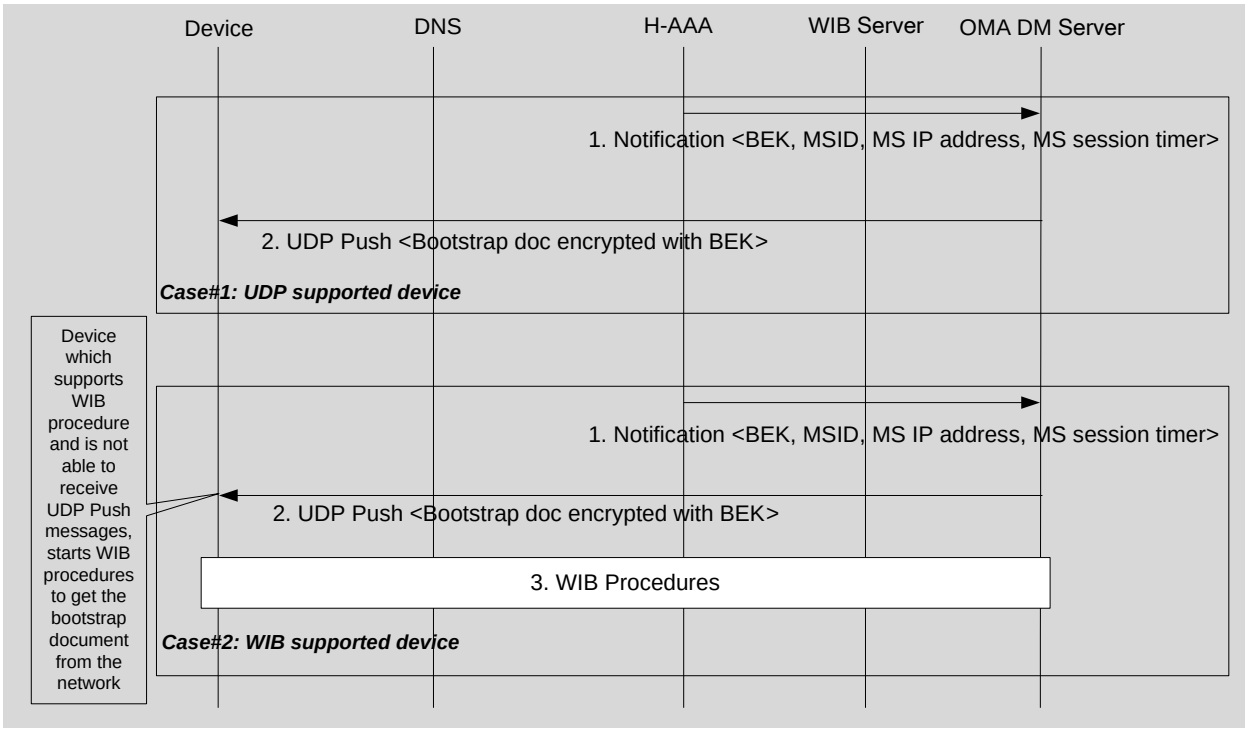


Figure 2- UDP Push and WIB Bootstrapping Methods

6.2 Requirements

6.2.1 General Requirements

1) The device and network MUST successfully complete the Pre-Provisioning Phase, as specified in [OTAGEN].
2) Default bootstrapping and device capabilities policy SHALL be installed by the operator at OMA DM server.
3) The device and the OMA DM server SHALL use the OMA DM Protocol [DMPRO] to establish a management session and interaction between each other.
4) The OMA DM bootstrap procedures as described in [DMBOOT] SHALL be applied for bootstrapping an unprovisioned WiMAX device.
5) The OMA DM server MUST support both the server-initiated bootstrapping procedure, as specified in section 6.1, and the WIB procedure, as specified in [OTAGEN].
6) The device SHALL support either the server-initiated bootstrapping procedures as specified in section 6.1 or the WIB bootstrapping procedures as specified in [OTAGEN], or both.
7) The client-initiated bootstrap method, i.e., WIB, MUST be used on devices that cannot support the server-initiated bootstrap method.
8) Delivery of the bootstrap data from OMA DM server to the device SHALL be done in a secure manner. The bootstrap data SHALL be protected as defined in [OTAGEN] Chapter 9 (Security Considerations).
9) Device SHALL process the bootstrap data, as specified in Section 7, Security Consideration.
10) The bootstrap data SHALL be mappable to the OMA DM WiMAX MO, as specified in ANNEX A.
11) Service provider locked devices SHALL include minimal pre-provisioning information such as.
    a. The network selection parameters
    b. Initial NAP/ Network Service Provider (NSP) connection rule/limitation, as specified in ANNEX A, CAPL and RAPL nodes,

    and MAY include

    c. OMA DM server bootstrap information

    to be able to select, connect and get activated to the network.

    If the device does not include OMA DM server bootstrap information, the device SHALL be bootstrapped through WIB or UDP Push bootstrap procedure.
12) The unlocked devices MAY be factory bootstrapped with the operator network specific parameters.
13) The device capabilities query procedure MAY be performed after the device is bootstrapped.
14) The OMA DM OTA Provisioning protocol service SHALL be provisioned in the home DNS server as described in [OTAGEN].
15) The device SHALL decrypt and authenticate the bootstrap message as described in [OTAGEN] Chapter 9 (Security Considerations). If the bootstrap message is successfully decrypted and authenticated, the device SHALL process the bootstrap document as described in [DMBOOT]. If the authentication of the bootstrap message fails, the device SHALL discard the bootstrap message. The message MAY be displayed to the user to allow the user to accept or reject the initiation of provisioning manually. If the bootstrap message is not discarded, the OMA DM bootstrap information SHALL be persistently stored in the device for later use in communication with the OMA DM server.
16) Error cases in WIB procedures are defined in [OTAGEN].

17) The OMA DM server SHALL support assignment of different DDF files to every combination of values of Man (in DevInfo MO), Mod (in DevInfo MO) and SwV (in DevDetail MO) nodes in order to support all devices from all OEMs with all possible software versions.

18) The bootstrapping process (either server initiated or client initiated) should be performed whenever the device is not provisioned with the information (DM_Account) required to establish the secure association with the OMA DM server.

19) The bootstrapping process (either server initiated or client initiated) should be performed whenever the client fails (the decision of fail is out of scope of this specification) to establish the secure association with the OMA DM server based on it's provisioned information.

20) In case of client initiated bootstrap i.e. WIB – the server must respond with a bootstrap file as described in [OTAGEN] regardless of the device state in the operator network.

6.2.2 OMA DM Protocol Requirements

Additional requirements beyond [REPRO] and [DMREPU]:

1. Source element

When used in SyncHdr element, the LocURI element in the Source element SHALL contain the device identifier (DevInfo/DevId) as specified in Annex A.

The device and the OMA DM server MAY use the FUMO to update the device firmware. The WiMAX DM client and OMA DM server MAY support OMA DM download procedure, as specified in [FUMO].

The OMA DM client may commit all non atomic OMA commands at the successful end of the OMA DM session.

6.2.3 Bootstrap and Notification Requirements

This section provides the bootstrap and notification requirements.

- For Case #1 (server initiated method using the UDP push):
  1. The OMA DM server SHALL use the non-secure connectionless WSP session service (UDP port 2948) [PUSHOTA] to deliver the encrypted server initiated bootstrap document and the OMA DM notifications [DMNOTI] to the OMA DM client.
  2. The X-WAP-Application-ID header [PUSHMSG] SHALL contain the application-id associated with the SyncML Device Management user agent. The application-id code 0x07 MUST be used instead of the textual representation of the application-id.
  3. The Content-Type header [PUSHMSG] SHALL contain the MIME media type for WiMAX bootstrap (application/vnd.wmf.bootstrap) as defined in [OTAGEN] for the bootstrap message. The Content-Type code (0x0318) MUST be used instead of the textual representation.
  4. The Content-Type header [PUSHMSG] SHALL contain the MIME media type for OMA DM Package #0 (application/vnd.syncml.notification) as defined in [IANA] for OMA DM notifications. The Content-Type code 0x44 MUST be used instead of the textual representation.
- For Case #2 (client-initiated method using the WIB):
  1. The OMA DM Server SHALL respond with an HTTP Response message as specified in [OTAGEN], when OMA DM Server receives the HTTP Get message.
  2. The Content-Type header of the HTTP Response [RFC2616] SHALL contain the MIME media type for WiMAX bootstrap (application/vnd.wmf.bootstrap) as defined in [OTAGEN] and the WiMAX bootstrap message SHALL be delivered in the HTTP body.
- For Case #1 and #2:
  1. The device SHALL process the bootstrap document, as specified in [DMBOOT].

2. The OMA DM Server SHALL send the bootstrap message to the OMA DM client whenever it receives the notification message from H-AAA. The OMA DM server SHALL attempt to bootstrap the OMA DM client during the period of MS IP session timer. If the OMA DM server cannot bootstrap the OMA DM client during MS IP session timer, the OMA DM server SHALL delete the device (e.g., MS) record.
3. After successfully processing the bootstrap document, the OMA DM client SHALL initiate a session to OMA DM server configured in the bootstrap. OMA DM Package #1 sent by the client SHALL contain DevInfo as specified in Annex A.
4. The OMA DM server SHOULD re-send the bootstrap document until the client connects for the first time. The number of retry and duration of sending the bootstrap document are out of scope of this specification.
5. If the device detects an error during any of these phases the device SHOULD perform device initiated network exit procedure as described in [NWGSTG3]. The timer value to wait bootstrap message from the network to the device is out of scope of this document.
6. The content of notifications in both cases SHALL be the same, because if the device receives multiple notifications only one management session SHOULD be triggered as defined in [DMNOTI].
7. The content of bootstrap document in both cases SHALL be the same.

6.3 Bootstrap Message Format and Encoding

The OMA DM Bootstrap specification [DMBOOT] defines two formats for the inner content of the bootstrap message, called “bootstrap profiles”.

- **OMA Client Provisioning** - This profile specifies alignment of two existing enablers – OMA Client Provisioning [ERELDCP] and OMA Device Management [ERELDDM]. The profile defines how the information provisioned using OMA Client Provisioning can be transferred to the management tree specified in the OMA Device Management.
- **OMA Device Management** - This profile defines how the OMA Device Management [ERELDDM] can be used for bootstrapping.

WiMAX devices MUST support the OMA Device Management profile for the bootstrap message. This means the bootstrap document MUST be formatted in accordance with [ERELDDM], and then encrypted as described in [OTAGEN] Security Consideration section.

Support for OMA Client Provisioning over WiMAX is not prohibited, but is not recommended either.

The encrypted bootstrap message and the nonce value SHALL be transmitted to the client in a TLV encoded message as described in the “Bootstrap Message Encoding” section of the OTA General Specification [OTAGEN].

6.4 OMA Bootstrap Reliability and Retransmission

In the case of #1, the OMA Bootstrap document is sent to the device with an unacknowledged UDP message. Due to the unreliable nature of UDP in a wireless environment like WiMAX, the bootstrap message MAY not be received by the device for any number of potential reasons. Because of this, the OMA DM server SHALL be capable of retransmitting the bootstrap document.

Each time the OMA DM server retransmits a bootstrap document it SHALL encrypt and authenticate the document with the same BEK and nonce as the first time it transmitted the bootstrap document for the life of the BEK as described in [OTAGEN] Chapter 9 (Security Considerations). The contents of the bootstrap document MUST be unmodified when retransmission is necessary. Retransmission is performed to enhance the reliability of the delivery of the bootstrap document–not to enable the delivery of modified bootstrap documents. The device can treat any received bootstrap message as a retransmission, not as an updated copy of a bootstrap document. Once a new BEK is available a bootstrap file can be encrypted with the new BEK and a new nonce. It is therefore possible to modify the contents of the bootstrap document only after a new BEK is available.

The OMA server SHALL not re-transmit the bootstrap document after the first successful response, which is package #1, is received from the device. The successful reception of an package #1 from the device indicates that the bootstrapping process was successful and no further attempts to bootstrap the device are required. All further OMA based notification and request retries SHALL fall under the behavior defined in OMA for notification retry behavior.

6.5 Subscription & Provisioning

6.5.1 In-band Subscription Order with In-band Provisioning

The following message flow sequence Figure 3 illustrates the use case where the user establishes business relationship with the service provider by using the device to be provisioned. The ordering subscription steps MAY occur anytime prior to the step C.

It is a beneficial for the subscription subsystem to be aware of the device capability prior to offering the subscription plan to the user. To achieve this, the OMA DM server MAY send a query to the device via the OMA DM protocol, in the same OMA DM session.

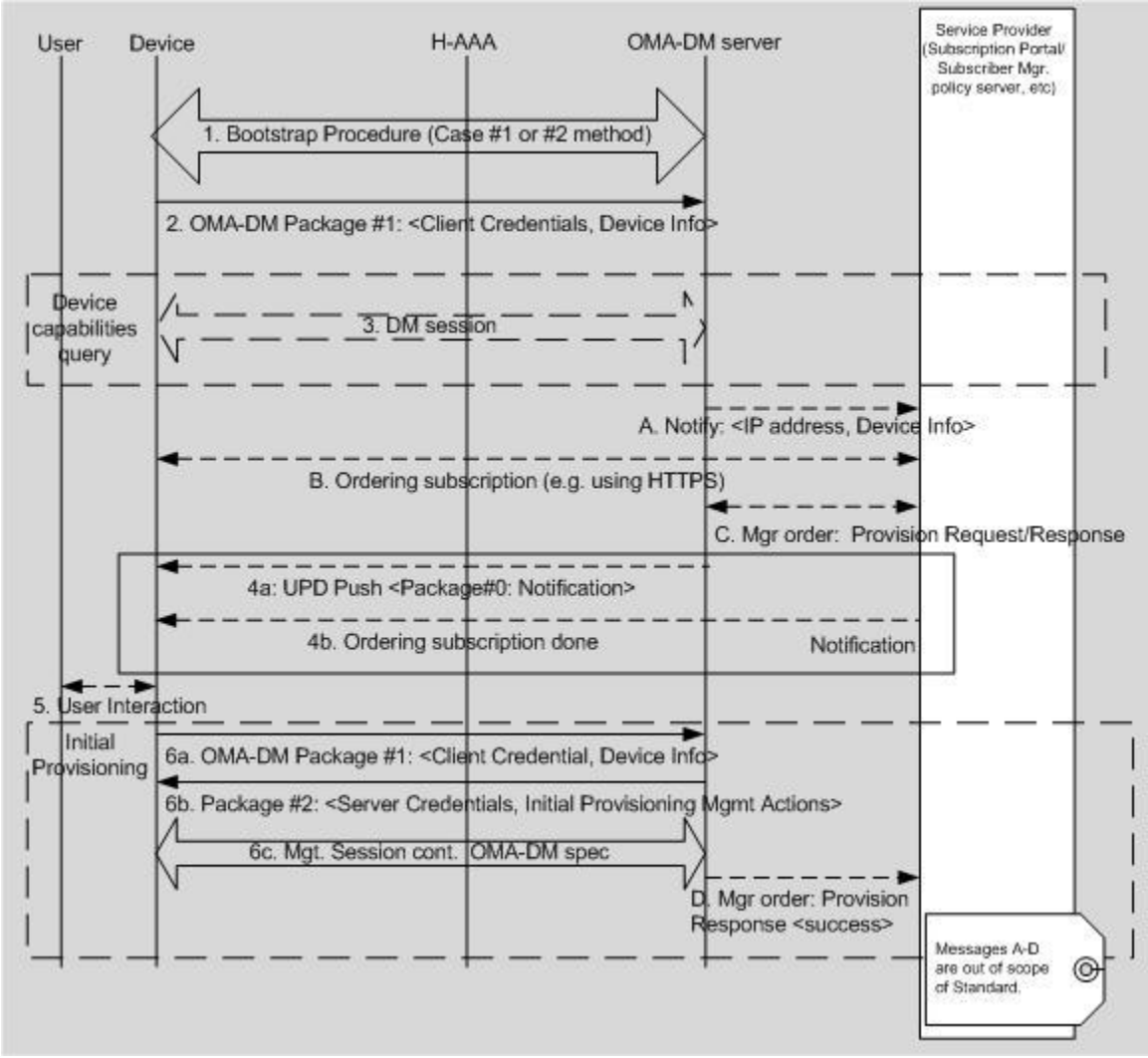


Figure 3 - Bootstrapping & Provisioning message flow sequence with in-band subscription order (Network initiated)

Message flow sequence:

1. The device and the OMA DM server SHALL perform either the case #1 or case #2 bootstrap procedure as specified in section 6.
2. After successfully processing the bootstrap, the OMA DM client SHALL initiate a management session to the OMA DM server configured in the bootstrap. The OMA DM client sends the OMA DM package #1, which includes credentials of the client and the device information (DevInfo MO) as specified in [DMBOOT], [DMPRO] and [DMSTOBJ].
3. Device capabilities query step:

   The OMA DM server MAY get the device capabilities information (e.g., WiMAX/DevCap) through the same OMA DM session which was used in step 2.

A. Upon completion of the OMA DM session, the OMA DM server SHALL send a notification with the device information, which includes the DevInfo described in Annex A, device capabilities, and bootstrap method flag to the service provider subscription portal subsystem. This Notification message MAY contain other information which the OMA DM server gets through the OMA DM session from the device as described in step 3.

B. The ordering subscription steps MAY vary depending on the implementation of the service provider subscription portal subsystem and it MAY occur anytime prior to step C. Within these steps, the user uses the subscription portal to create a business relationship with the attached NSP. Based on the user input and device capability query, the subscription portal creates a user account. The user account information is stored in a database where the AAA and the OMA DM server have access to the information.

C. Upon completion of the subscription ordering and account setup, the subscription portal sends a management provision request to the OMA DM server. The request includes the device and user credentials, and MSID and MAY includes the request for bootstrap information. .Upon receiving the subscription order from subscription portal, the OMA DM server SHALL perform either step 4a or 4b. In the case of step 4b, OMA DM server SHALL include a response message to the OMA DM client to initiate DM session, containing Package #0 Notification as defined in [DMPRO] for OMA DM notifications.

4. Notification Step:
   a. In the case of #1 (UDP Push): If the bootstrap method is UDP Push, the DM server SHALL send the notification message, which is the OMA DM package #0, to the device as specified in [DMPRO].
   b. In the case of #2 (WIB procedure): If the bootstrap method is WIB (i.e., HTTP), the subscription portal SHALL send an indicator to the device to trigger the OMA DM client to start the DM session. The indicator is carried in the HTTP response to the OMA DM client to initiate DM session. The Content-Type header of the HTTP response SHALL contain the MIME media type for OMA DM Package #0 (application/vnd.syncml.notification) as defined in [IANA] for OMA DM notifications.
5. Upon receiving the notification message, the device (OMA DM client) MAY require user interaction.
6. Upon receiving the notification message, and - if necessary - confirmed by user interaction, the device SHALL start an OMA DM session by sending an OMA DM Package #1 to the OMA DM server. Package #1 SHALL contain DevInfo as describer in Annex A. The OMA DM server SHALL proceed with the provisioning by managing the objects described in Annex A-C as specified in [DMPRO]. Upon successful completion of the provision phase, the OMA DM server SHALL set proper value for WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/Activated node. Once the provisioning is completed, the OMA DM server and client SHALL terminate the DM session.

D. The OMA DM server sends a management provision response to the subscription portal with a successful status.

The WIB procedure related error cases are defined in [OTAGEN]. OMA DM session related error cases are defined in [DMPRO], [DMREPU] and [DMSYNCHTTP].

6.5.2 Out of band subscription order with in-band provision

The following message flow sequence Figure 4 illustrates the following use cases:

1) Use case A: User establishes a business relationship with the service provider prior attaching an unprovisioned device to the service provider network. The user account setup is completed.

2) Use case B: User has already established account, and wishes to re-provision an existing device.

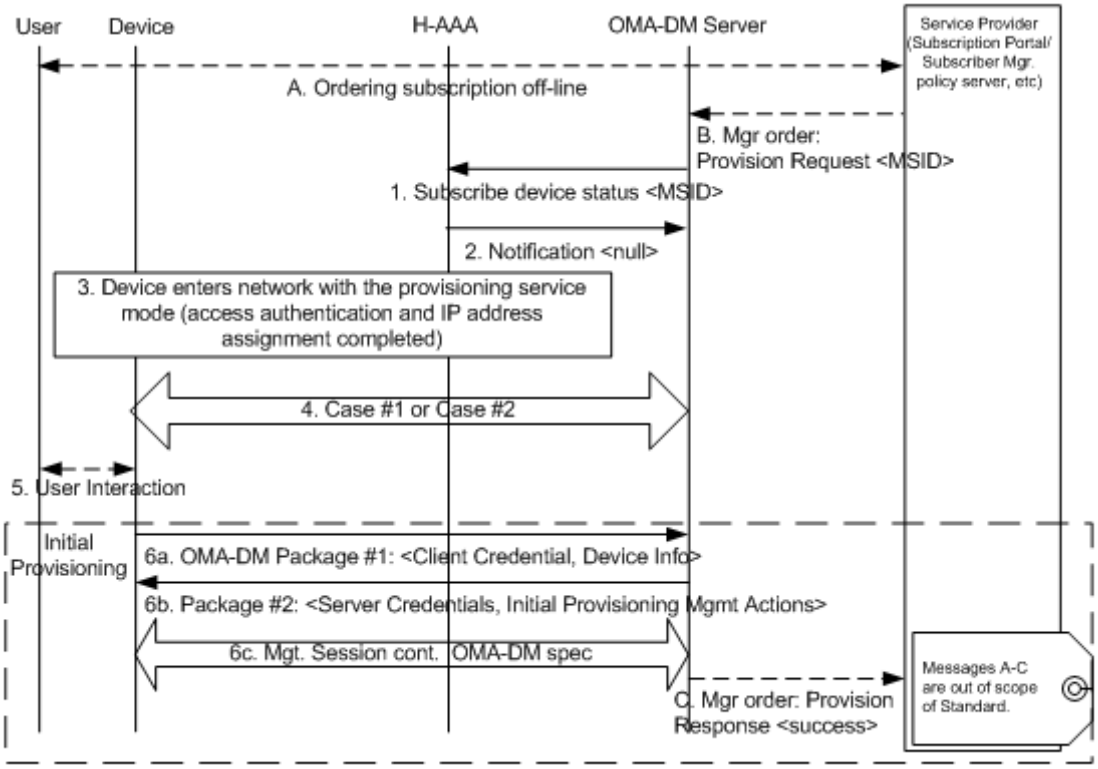


Figure 4 - Bootstrapping & Provisioning message flow sequence with out of band subscription order

Message flow sequence:

A. The user establishes a business relationship with the service provider prior attaching an unprovisioned device to the service provider network.

B. The subscription portal sends a management provision request to the OMA DM server. The request includes user credential, and MSID.

1. OMA DM server subscribes to the device status event with the H-AAA.

2. If the device does not have an IP Session with the network, the H-AAA SHALL send a notification with a "null" status.

3. Device enters the network in the provisioning service mode. The access authentication and IP address assignment is completed.

4. Device and OMA DM server SHALL perform either the case #1 or case #2 bootstrap procedure as specified in Chapter 6.2.3.

5. Upon receiving the bootstrap document, the device (OMA DM client) MAY require user interaction.

6. Upon receiving the bootstrap document, and - if necessary - confirmed by user interaction, the device SHALL start an OMA DM session by sending an OMA DM Package #1 to the OMA DM server. Package #1 SHALL

contain DevInfo as describer in Annex A. The OMA DM server SHALL proceed with the provisioning by managing the objects described in Annex A-C as specified in [DMPRO]. Upon successful completion of the provision phase, the OMA DM server SHALL set proper value for WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/Activated node. Once the provisioning is completed, the OMA DM server and client SHALL terminate the DM session.

C. The OMA DM server sends a management provision response to the subscription portal with a successful status.

The WIB procedure related error cases are defined in [OTAGEN]. OMA DM session related error cases are defined in [DMPRO], [DMREPU] and [DMSYNCHTTP].

6.6 Continuous Management

1) Devices that will be affected by the presence of a firewall blocking UDP Push notifications SHALL support client-initiated sessions tied to a timer.

2) The device using client-initiated update method (specified at WiMAX/DevCap/UpdateMethods/ClientInitiated) SHALL start a client-initiated management session to the OMA DM server of the operator every "X" number of minutes where "X" is defined under the "WiMAXSupp/Operator/<X>/NetworkParameters/PollingInterval" node.

3) The operator, upon first registration of the device on the network, SHOULD read the value of "WiMAX/DevCap/UpdateMethods/ServerInitiated" and "WiMAX/DevCap/UpdateMethods/ClientInitiated" nodes to determine the capabilities of the device. If the device reports a suggested polling interval in the "WiMAX/DevCap/UpdateMethods/ClientInitiated/PollingInterval" node, the operator MAY set the polling interval under the Operator node accordingly. This would ensure that the devices operate at their optimum settings.

The WIB procedure related error cases are defined in [OTAGEN]. OMA DM session related error cases are defined in [DMPRO], [DMREPU] and [DMSYNCHTTP].

6.7 Device Capabilities

1) If the Device Capabilities (e.g. UpdateMethods) are changed, the client SHALL send a notification to the DM server via a Generic Alert [DMPRO] message. The alert message includes the following data:

- The URI of the DevCap MO – Used to identify the source
- An alert type – The alert type "org.wimaxforum.ota.updatedevicecap" MUST be used.

2) Upon receiving the notification, the DM server SHALL update the Device Capabilities into the DM server.

7. Security Considerations

OMA DM security considerations SHALL use [OTAGEN].

ANNEX A. OMA DM WiMAX MO [NORMATIVE]

A3 Introduction

The size of format types are specified in [DMDDFDTD]. The encoding of Chr type of nodes is ASCII unless otherwise specified.

Maximum length of some of the nodes is defined within the node descriptions in the following way: "Maximum length SHOULD/SHALL be ." Whenever "SHALL" is used in this context, it means that the sending entity SHALL NOT populate the node with more data than defined by maximum length and the receiving entity SHALL support lengths up to this definition. Whenever "SHOULD" is used in this context, it means that the receiving entity SHALL support lengths up to this definition and it is implementation specific of what happens if maximum length is exceeded. If "SHOULD" is used the sending entity SHOULD populate the node with data less than or equal to maximum length but it MAY put more data although it is not recommended.

A WiMAX device's OMA DM tree MUST contain the following mandatory MOs:

- DMAcc
- DevInfo
- DevDetail
- WiMAX
- WiMAXSupp
- NAP

The DMAcc, DevInfo, DevDetail, and NAP are generic OMA DM MOs defined by OMA DM WG in [DMSTDOBJ] and [DMCONNMO]. This document describes how these objects are used in a WiMAX device.

WiMAX MO and WiMAX Supplementary MO are WiMAX specific and described in this document.

In addition, WiMAX device MAY use, inside the WiMAXSupp, several Extensible Authentication Protocol (EAP) MOs to contain the authentication settings for different subscriptions. This is defined in [DMEAPMO].

A4 Graphical Representation

Figure 5 shows the standard OMA DM tree for WiMAX devices. The WiMAXSupp and NAP MOs MAY be located anywhere in the DM tree.

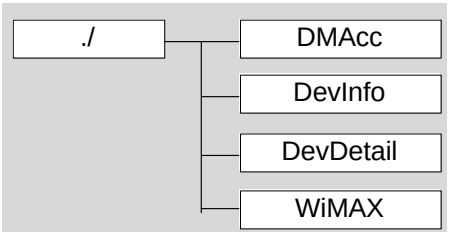


Figure 5 - Standard OMA DM tree for WiMAX devices

A5 Status and Occurrence Guidance

Refer to the OMA DM ACMO Whitepaper [DMACMO] for the definition and possible values for status and occurrence of each node.

A6 DevInfo MO

A6.1 Introduction

This section describes how the standard DevInfo MO [DMSTDOBJ] is used with WiMAX devices. See the standard OMA DM Objects definitions [DMSTDOBJ].

A6.2 Graphical Representation

Figure 6 shows the standard DevInfo MO.

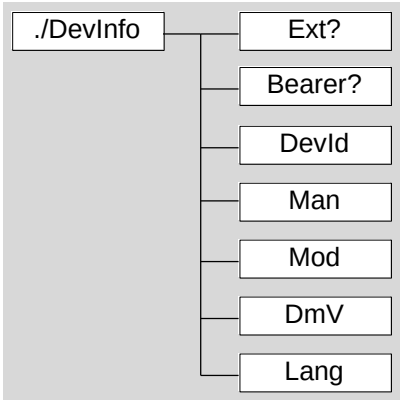


Figure 6 - Standard DevInfo MO

A6.3 Node Descriptions

A6.3.1 DevInfo

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node provides Host Device information for OMA DM server. The information is sent from the client to the server

A6.3.2 DevInfo/Ext

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This optional interior node is designated to be the only branch of the DevInfo sub tree into which extensions can be added permanently or dynamically.

A6.3.3 DevInfo/Bearer

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This optional interior node is used for stating what bearers the Host Device supports.

A6.3.4 DevInfo/DevId

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies globally unique identifier (GUID) for the Host Device. The identifier SHOULD be globally unique. The Host Device MAC address (i.e. MSID) MAY be provided as a DevId for both single-mode and dual-mode devices. WiMAX devices MAY use the MAC address as DevId in which case the format SHALL be the following.

<DevId> ::= < mac> ":" <mac_address>
<mac> ::= %d77.65.67
<mac_address> ::= 12 * 12 <hex>
<hex> ::= <numbers> | "A" | "B" | "C" | "D" | "E" | "F" | "a" | "b" | "c" | "d" | "e" | "f"
<numbers> ::= "0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" | "8" | "9"

Examples of valid DevIds:

MAC:112233445566
MAC:a12233445566
MAC:A12233445566

Examples of invalid DevIds:

mac:1122334455
MAC:11223344556
MAC:11-22-33-44-55-66
MAC:11:22:33:44:55:66

A6.3.5 DevInfo/Man

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the manufacturer identifier of the Host Device.

A6.3.6 DevInfo/Mod

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the model identifier of the Host Device.

A6.3.7 DevInfo/DmV

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies OMA DM client version identifier (manufacturer specified string).

A6.3.8 DevInfo/Lang

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the current language setting of the Host Device. The syntax of the language tags and their use are defined in [RFC1766]. Language codes are defined by ISO in the standard ISO 639.

A7 DM Account MO

A7.1 Introduction

This section lists the required modifications and extensions to the standard DM Account MO [DMSTDOBJ]. There MAY be multiple DMAcc MOs. A specific DMAcc MO represents a specific operator's OMA DM server.

A7.2 Graphical Representation

See [DMSTDOBJ] for graphical presentation of the DMAcc MO.

A7.3 Node Descriptions

A7.3.1 DMAcc/<X>/ServerID

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies a server identifier for the management server used in the management session. The ServerID MUST be unique per Home Network Service Provider (H-NSP). Each H-NSP MUST use only one ServerID value.

While it is not mandatory, it is recommended that one of the NSP-IDs of the operator (which are unique to that operator) be used as the ServerID.

A8 DevDetail MO

A8.1 Introduction

This Section lists required modification and extensions to the standard DevDetail MO [DMSTDOBJ]. Please also refer to the OMA DM Standard Objects definitions [DMSTDOBJ].

A8.2 Graphical Representation

Figure 7 shows the structure of the DevDetail MO.

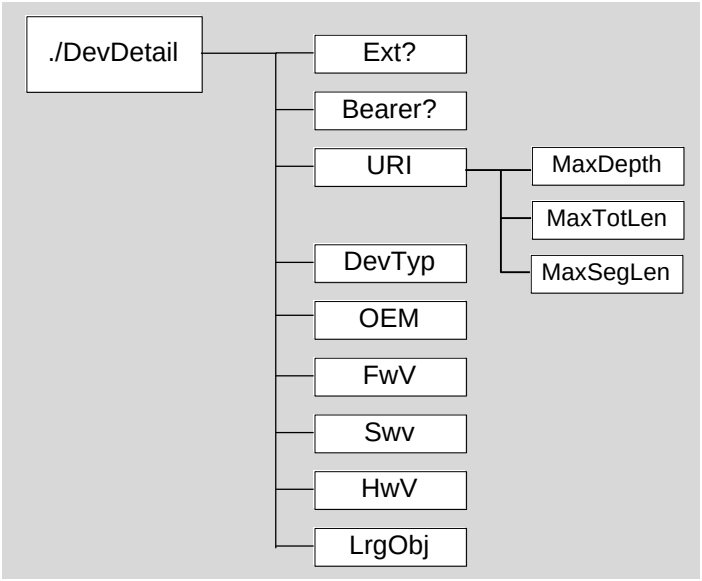


Figure 7 - DevDetail MO

A8.3 Node Descriptions

A8.3.1 DevDetail/Ext

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This optional interior node is designated to be the only branch of DevDetail sub tree into which extensions can be added permanently or dynamically.

A8.3.2 DevDetail/Bearer

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This optional interior node is designated to be a branch of the DevDetail sub tree into which items related to the bearer that the Host Device supports are stored.

A8.3.3 DevDetail/URI

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This mandatory interior node is used for information specific to URI supported by the client. See [DMSTDOBJ] for the child nodes and details.

A8.3.4 DevDetail/DevTyp

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This mandatory leaf node specifies device type of the Host Device. The possible values to be used to populate this leaf node are including but not limited to the followings (The first column indicates type of the device and the second column indicates character string for the respective device types. The last column indicates whether the WiMAX/TerminalEquipment node is required or not according to the DevTyp):

Table 1 - Values for DevTyp node

Type of the Device	DevType String for Population	TerminalEquipment Node
PC Card – Single Mode	SingleModePCCard	REQUIRED
PC Card – Multi Mode	MultiModePCCard	REQUIRED
Express Card – Single Mode	SingleModeExpressPCCard	REQUIRED
Express Card – Multi Mode	MultiModeExpressPCCard	REQUIRED
USB Card – Single Mode	SingleModeUSBCard	REQUIRED
USB Card – Multi Mode	MultiModeUSBCard	REQUIRED
Basic Modem	BasicModem	OPTIONAL
SOHO Modem	SOHOModem	OPTIONAL
Personal Media Player (PMP)	PMP	OPTIONAL
Multi Mode PMP	MultiModePMP	OPTIONAL
UMPC	UMPC	OPTIONAL
Netbook	Netbook	OPTIONAL
Laptop	Laptop	OPTIONAL
Internet Tablet	InternetTablet	OPTIONAL
Single Mode Handset	SingleModeHandset	OPTIONAL
Multi Mode Handset	MultiModeHandset	OPTIONAL
PDA	PDA	OPTIONAL
Gaming Device	GamingDev	OPTIONAL
Video Phone	VideoPhone	OPTIONAL

Type of the Device	DevType String for Population	TerminalEquipment Node
Machine to Machine	M2M	OPTIONAL
Digital Camera	Digital Camera	OPTIONAL
Digital Camcorder	Digital Camcorder	OPTIONAL
Wearable Device	WearableDev	OPTIONAL
Multi Mode Messaging Device	MultiModeMsgDev	OPTIONAL
Electronic Book	EBook	OPTIONAL
Navigation Device	NavigationDev	OPTIONAL
In-Vehicle Entertainment Device	InVehicleEntDev	OPTIONAL
Home Media Gateway	HomeMediaGW	OPTIONAL
Music Player	MusicPlayer	OPTIONAL

A8.3.5 DevDetail/OEM

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This mandatory leaf node specifies original equipment manufacturer of the Host Device.

A8.3.6 DevDetail/FwV

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This mandatory leaf node specifies firmware version of the Host Device.

A8.3.7 DevDetail/SwV

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This mandatory leaf node specifies software version of the Host Device.

In order to support the possibility of change in DDF due to software and/or firmware upgrade process, the SwV node SHALL be taken into account by the OMA DM server in the selection process of the correct DDF for the device.

A8.3.8 DevDetail/HwV

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This mandatory leaf node specifies hardware version of the Host Device.

A8.3.9 DevDetail/LrgObj

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This mandatory leaf node indicates whether the Host Device supports the OMA DM Large Object Handling specification, as defined in [DMPRO]

A9 WiMAX MO

A9.1 Introduction

The WiMAX MO facilitates management of WiMAX parameters.

The MO Identifier for the WiMAX MO MUST be: “urn:wmf:mo:wimax-mo:1.0”

The WiMAX MO MUST be located in the root (./).

A9.2 Graphical Representation

Figure 8 provides the structure of the WiMAX MO.

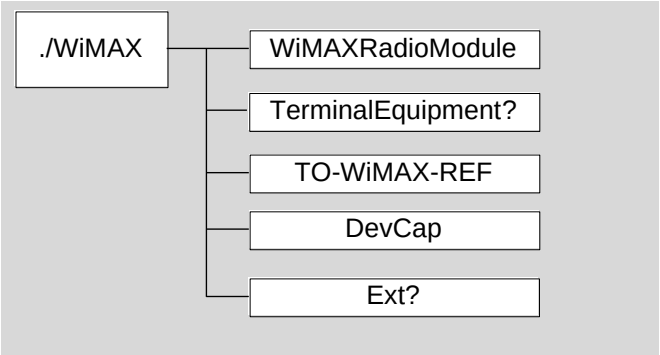


Figure 8 - WiMAX Management Object

A9.3 Node Descriptions

A9.3.1 WiMAX

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node specifies the WiMAX device configuration related information. This interior node as depicted in Figure 8 provides all required information about WiMAXRadioModule and Terminal Equipment and Device capabilities.

A9.3.2 WiMAX/WiMAXRadioModule

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node specifies the WiMAX radio chipset specific information. See Section A9.4 for further details.

A9.3.3 WiMAX/TerminalEquipment

Status	Tree Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

This optional interior node specifies the Terminal Equipment device specific information. See Section A9.5 for further details. This node is not used for stand-alone Host Devices which have built in embedded WiMAX chipset and not connected to Terminal Equipment. This node is REQUIRED for some type of devices as specified in Table 2.

A9.3.4 WiMAX/TO-WiMAX-REF

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node contains the link to the WiMAXSupp. See Section A10 for further details about the WiMAXSupp. An example is presented in Annex B to show how the linkage between TO-WiMAX-REF node and WiMAXSupp is established.

A9.3.5 WiMAX/DevCap

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains WiMAX device capability information. See Section A9.6 for further details.

A9.3.6 WiMAX/Ext

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This optional interior node is designated to be the only branch of WiMAX sub tree into which extensions can be added, permanently or dynamically.

A9.4 WiMAX Radio Module

Figure 9 shows the structure of the WiMAXRadioModule MO.

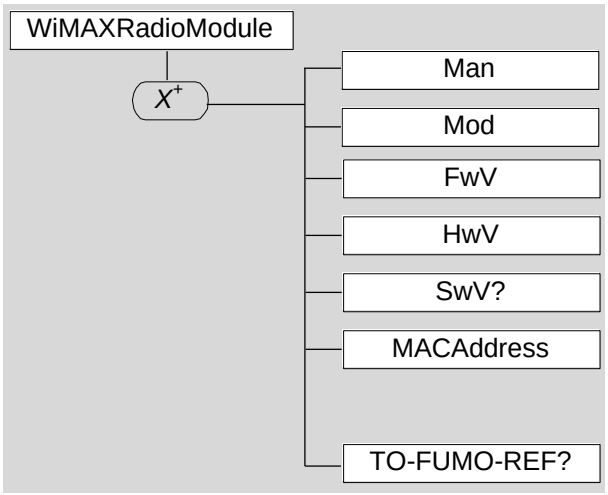


Figure 9 - WiMAX Radio Module

A9.4.1 WiMAX/WiMAXRadioModule/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get

This interior node is a placeholder for the WiMAX radio chipsets present in the Host Device to support WiMAX bearer on the Host Device. This interior node distinguishes different WiMAX radio chipsets and subsystems that are possibly present in the Host Device. There MUST be exactly one WiMAX radio chipset and subsystem for each of these interior nodes. There should be exactly one instance of the internal node in the radio module node. In the future versions of the WiMAX MO, only one radio module will be allowed.

A9.4.2 WiMAX/WiMAXRadioModule/<X>/Man

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the manufacturer of the WiMAX chipset embedded in the Host Device. The maximum length SHOULD be 50 characters.

A9.4.3 WiMAX/WiMAXRadioModule/<X>/Mod

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the model of the WiMAX radio chipset embedded in the Host Device. The maximum length SHOULD be 50 characters.

A9.4.4 WiMAX/WiMAXRadioModule/<X>/FwV

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the firmware version of the WiMAX radio chipset present in the Host Device. The maximum length SHOULD be 50 characters.

A9.4.5 WiMAX/WiMAXRadioModule/<X>/HwV

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the hardware version of the WiMAX radio chipset present in the Host Device. The maximum length SHOULD be 50 characters.

A9.4.6 WiMAX/WiMAXRadioModule/<X>/SwV

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Chr	Get

This optional leaf node specifies the WiMAX radio chipset driver version in connection with the Operating System of the terminal equipment into which the Host Device is inserted. This is applicable only when the Host Device is inserted into the Terminal Equipment. The maximum length SHOULD be 50 characters.

A9.4.7 WiMAX/WiMAXRadioModule/<X>/MACAddress

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bin	Get

This leaf node represents the 48-bit MSID associated with the WiMAX radio chipset and subsystem. When displayed on the device, the 48-bit MAC address SHOULD be displayed in hexadecimal representation with the octets of the MAC address separated by a hyphen.

A9.4.8 WiMAX/WiMAXRadioModule/<X>/TO-FUMO-REF

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Chr	Get

This optional leaf node contains the link to FUMO object that is used to update the firmware of the WiMAX radio chipset. This FUMO object is used to upgrade OEM SW or firmware related to the WiMAX radio module. The FUMO is defined in [FUMO].

A9.5 WiMAX Terminal Equipment

This interior node describes the Terminal Equipment device information. DevInfo and DevDetail DM standard object structure is reused to describe the terminal equipment., Figure 10 shows the structure of the TerminalEquipment MO.

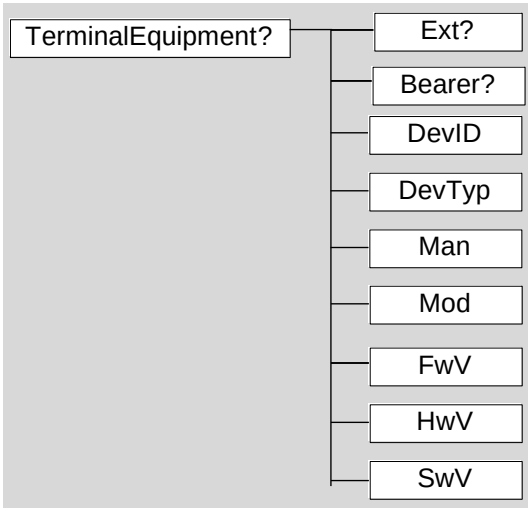


Figure 10 - Terminal Equipment

A9.5.1 WiMAX/TerminalEquipment/Ext

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This optional interior node is designated to be the only branch of Terminal Equipment sub tree into which extensions can be added permanently or dynamically.

A9.5.2 WiMAX/TerminalEquipment/Bearer

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This optional node specifies the bearer detailed information for the Terminal Equipment as defined by OMA DM. For example, it MAY contain WiFi connectivity settings.

A9.5.3 WiMAX/TerminalEquipment/DevID

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the device identifier of the Terminal Equipment. The value of this leaf node MUST be unique and formatted as a URN as defined in [RFC2141]. The value MUST be the concatenation of the node Man, the node Mod and the OEM-specific serial number of the Terminal Equipment, separated by ':'. If OEM does not supply a serial number, a GUID value in hexadecimal format MUST be used instead. The GUID value is assigned by the OMA DM client. The maximum length SHOULD be 50 characters.

Example: urn: LaptopMakerX:Model3:12345678

A9.5.4 WiMAX/TerminalEquipment/DevTyp

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This mandatory leaf node specifies device type of the Terminal Equipment. Possible values are including and not limited to the list in the Table 2. The maximum length SHOULD be 50 characters.

Table 2- Values for Terminal Equipment DevTyp

Type of the Device	DevType String for Population

Laptop	Laptop
Personal Media Player	PMP
Multi Mode PMP	MultiModePMP
UMPC	UMPC
Internet Tablet	InternetTablet
Gaming Device	GamingDev
Digital Camera	Digital Camera
Digital Camcorder	Digital Camcorder
Multi Mode Messaging Device	MultiModeMsgDev
E Book	EBook
Navigation Device	NavigationDev
In-Vehicle Entertainment Device	InVehicleEntDev
CPE	CPE

A9.5.5 WiMAX/TerminalEquipment/Man

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the manufacturer of the Terminal Equipment. The maximum length SHOULD be 50 characters.

A9.5.6 WiMAX/TerminalEquipment/Mod

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the model of Terminal Equipment. The maximum length SHOULD be 50 characters.

A9.5.7 WiMAX/TerminalEquipment/FwV

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the firmware version of the Terminal Equipment. Firmware refers to OEM specific SW embedded within the Terminal Equipment If the firmware version of the Terminal Equipment is not available this node SHALL contain the value “none”. The maximum length SHOULD be 50 characters.

A9.5.8 WiMAX/TerminalEquipment/HwV

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the hardware version of the Terminal Equipment. The maximum length SHOULD be 250 characters.

A9.5.9 WiMAX/TerminalEquipment/SwV

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node value SHALL be the concatenation of the current operating system name, the operating system version, and the operating system architecture of the Terminal Equipment separated by “:” as

follows: OS_Name:OS_Version:OS_Architecture (for example, Windows:XP:X86). If the Operating System version of the Terminal Equipment is not available this node SHALL contain the string “none”. The maximum length SHOULD be 50 characters.

A9.6 WiMAX Device Capabilities

The nodes covered in this sub-section specify the different feature capabilities of the WiMAX device in order to assist the provisioning entity on the network in determining what features and associated parameters can and will be provisioned into the device. Figure 10 shows the structure of the DevCap MO.

Please note that additional capability information MAY be added to this node in the future.
Figure 11 shows the structure of the DevCap MO.

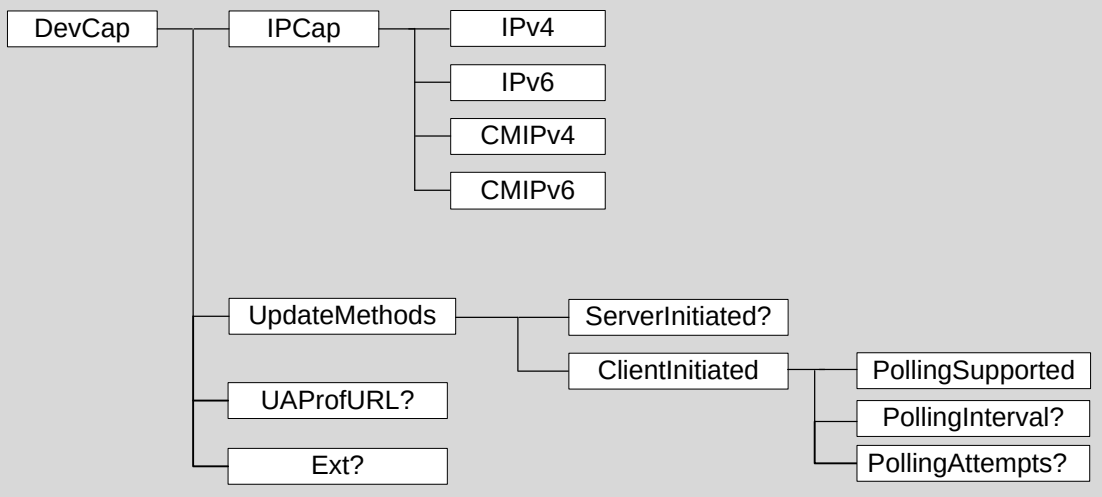


Figure 11 - WiMAX Device Capabilities

A9.6.1 WiMAX/DevCap/IPCap

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains IP specific WiMAX device capability information.

A9.6.2 WiMAX/DevCap/IPCap/IPv4

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get

This leaf node specifies if the WiMAX device is capable of supporting IPv4. ‘TRUE’ means that IPv4 is supported and ‘FALSE’ means that IPv4 is not supported.

A9.6.3 WiMAX/DevCap/IPCap/IPv6

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get

This leaf node specifies if the WiMAX device is capable of supporting IPv6. ‘TRUE’ means that IPv6 is supported and ‘FALSE’ means that IPv6 is not supported.

A9.6.4 WiMAX/DevCap/IPCap/CMIPv4

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get

This leaf node specifies if the WiMAX device is capable of supporting CMIPv4. ‘TRUE’ means that CMIPv4 is supported and ‘FALSE’ means that CMIPv4 is not supported.

A9.6.5 WiMAX/DevCap/IPCap/CMIPv6

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get

This leaf node specifies if the WiMAX device is capable of supporting CMIPv6. 'TRUE' means that CMIPv6 is supported and 'FALSE' means that CMIPv6 is not supported.

A9.6.6 WiMAX/DevCap/UAProfURL

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Chr	Get

This leaf node specifies the URL of the device capabilities via using [UAProf], as specfied in [UAProf]. The maximum length SHALL be 1024 characters.

A9.6.7 WiMAX/DevCap/UpdateMethods

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	**Node**	Get

This interior node contains device capabilities related to continuous management method.

A9.6.8 WiMAX/DevCap/UpdateMethods/ServerInitiated

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Bool	Get

This leaf node specifies whether the device is capable of receiving Notification Initiated Session Trigger Messages sent by the OMA DM server [DMNOTI]. If the value is 'FALSE', the device does not support server-initiated DM session. If the value is 'TRUE', the device supports server-initiated DM session. When this node does not exist, device behavior is the same as if the value was 'FALSE'.

A9.6.9 WiMAX/DevCap/UpdateMethods/ClientInitiated

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains information about the device's polling-based client-initiated DM capability.

A9.6.10 WiMAX/DevCap/UpdateMethods/ClientInitiated/PollingSupported

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get

This interior node specifies whether the device supports continuous management using client-initiated periodic polling. When the value is TRUE, the device supports client-initiated polling. If this node is not present then it is the same as being FALSE.

A9.6.11 WiMAX/DevCap/UpdateMethods/ClientInitiated/PollingInterval

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Int	Get

This leaf node specifies the device recommended value for the polling interval. This value MAY be used by the operator to configure its polling interval value. This value is presented in number of minutes. The value of this node is interpreted in the same way as WiMAXSupp/Operator/<X>/NetworkParameters/ PollingInterval node in Section A10.4.7.6. When this node does not exist, device behavior is the same as if the value was zero. This OPTIONAL node MAY NOT exist if the 'PollingSupported' is FALSE.

A9.6.12 WiMAX/DevCap/UpdateMethodes/ClientInitiated/PollingAttempts

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Int	Get

This leaf node specifies the recommended value for polling attempts as set by the manufacturer. This value may be used by the manufacturer to configure the number of times the device will attempt to access client-initiated polling at a periodic interval. This value represents the number of times the device shall perform client-initiated polling after the initial poll.

It is recommended that this parameter be set to a value that will continue client polling for at least 30 minutes. For example if the polling interval is set to 5 then polling attempts should be set to 5. Devices will make the first attempt after the first polling interval has expired and continue n times where n is the number of polling attempts. Setting polling attempts to a value of -1 will indicate that the MS should poll continuously. Setting the value of polling attempts to 0 will cause a device to never poll and this should never be set in the DevCap node. If it is desired by an operator that the device SHOULD never perform client initiated polling it should be set in the WiMAXSupp/Operator/<X>/NetworkParameters/PollingAttempts node of the operator.

This OPTIONAL node MAY NOT exist if the 'PollingSupported' is FALSE.

A9.6.13 WiMAX/Ext

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This optional interior node is designated to be the only branch of DevCap sub-tree into which vendor-specific extensions can be added.

A10 WiMAX Supplementary MO

A10.1 Introduction

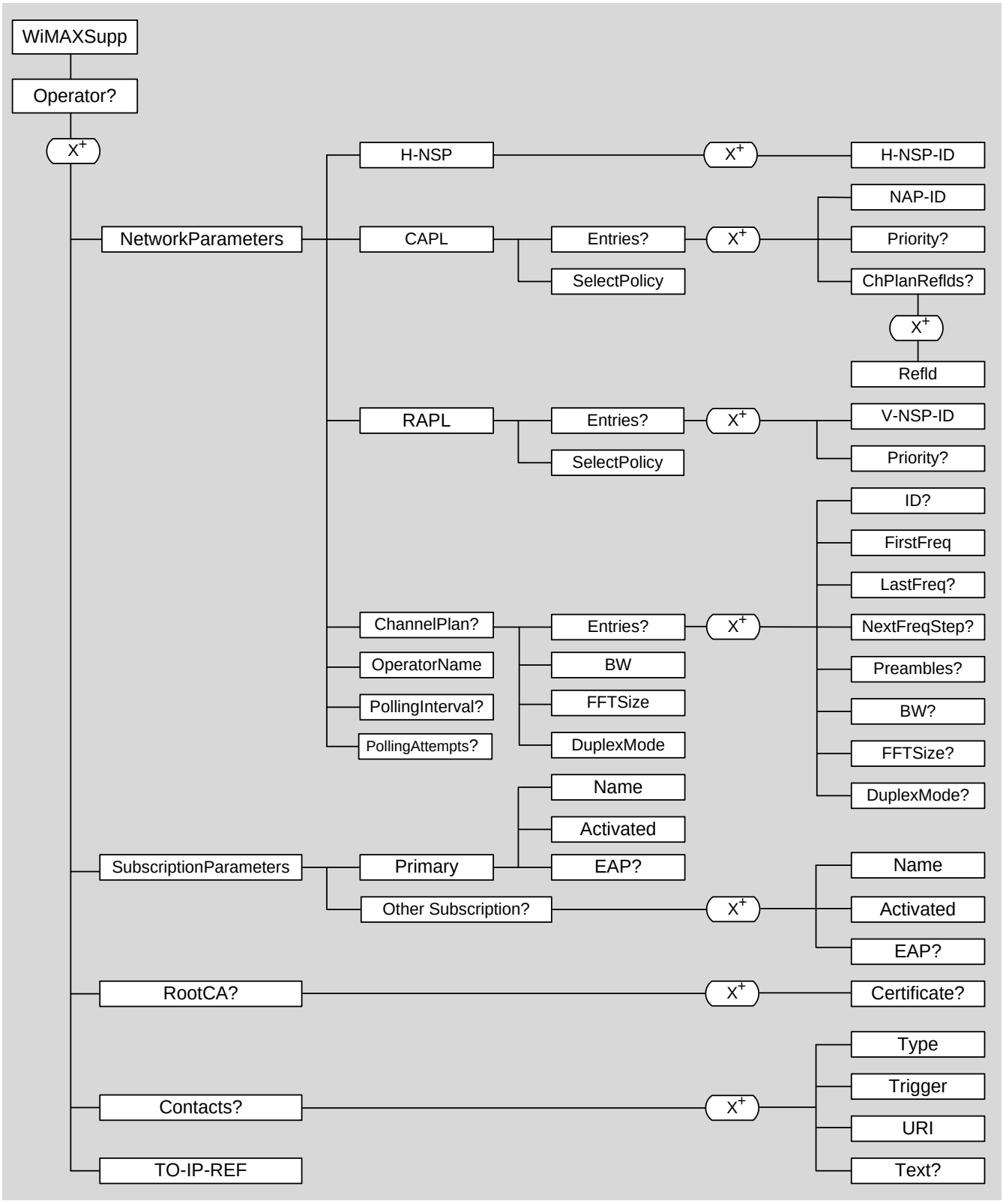
The WiMAX Supplementary object facilitates management of WiMAX parameters.

The MO Identifier for the WiMAXSupp MUST be: “urn:wmf:mo:wimax-supp-mo:1.0”

A10.2 Graphical Representation

Figure 12 provides the structure of WiMAX Supplementary MO.

1



2
3

Figure 12 - WiMAX Supplementary MO Tree Structure

A10.3 Node Descriptions

A10.3.1 WiMAXSupp/Operator

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

This mandatory interior node lists the operator specific WiMAX parameters. See Section A10.4 for further details.

A10.4 Operator Node

A10.4.1 WiMAXSupp/Operator/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node distinguishes the different operator object and parameters. There MUST be exactly one operator node for each of these interior nodes.

A10.4.2 WiMAXSupp/Operator/<X>/NetworkParameters

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the WiMAX network specific parameters like roaming lists, Channel Plans and home network information. See Section A10.4.7 for further details.

A10.4.3 WiMAXSupp/Operator/<X>/SubscriptionParameters

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the WiMAX subscription parameters like user authentication types and parameters. See Section A10.4.8 for further details.

A10.4.4 WiMAXSupp/Operator/<X>/RootCA

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This interior node contains the additional root CAs trusted by operator and is used by the device to authenticate the operator's networks. See Section A10.4.9 for further information.

A10.4.5 WiMAXSupp/Operator/<X>/Contacts

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This interior node contains multiple groups of contact addresses. Each group can be used to connect the user to different network or administrative function, such as emergency, subscription purchasing or technical support. See Section A10.4.10 for further information.

A10.4.6 WiMAXSupp/Operator/<X>/TO-IP-REF

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This interior node contains a path to the IP MO. The IP MO defines parameters for WiMAX connectivity. The IP MO is defined in [DMIPMO]. See Section B4 for further details.

A10.4.7 Network Parameters Node

Network parameters node defines a set of nodes used by the device during network discovery and selection procedures, as defined in [NWGSTG3].

A10.4.7.1 WiMAXSupp/Operator/<X>/NetworkParameters/H-NSP

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the H-NSP parameters. See Section A10.4.7.8 for further details.

A10.4.7.2 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the CAPL. The list contains the NAP-IDs, who have direct relationship with the H-NSP. See Section A10.4.7.9 for further details.

Figure A-1 in [NWGSTG2P3] clarifies how the business relationships are handled between subscriber, NAPs and NSPs in WiMAX.

A10.4.7.3 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the RAPL. The list contains the Visited Network Service Providers (V-NSP), who have direct relationship with the H-NSP. See Section A10.4.7.10 for further details.

Figure A-1 in [NWGSTG2P3] clarifies how the business relationships are handled between subscriber, NAPs and NSPs in WiMAX.

A10.4.7.4 WiMAXSupp/Operator/<X>/NetworkParameters/OperatorName

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Replace

This leaf node defines the human readable name of the operator, e.g., “Operator”. In the case that the “activated” node is FALSE, the operator name received from the WiMAX Medium Access Control (MAC) layer, NSP verbose name MAY be used to overwrite the value provided in the OperatorName node. The MIME type of the node SHALL be 'text/plain; charset=utf-8’. The maximum length SHOULD be 255 bytes. In utf-8 format, each character MAY take one to four bytes.

A10.4.7.5 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

This interior node contains a Channel Plan, which holds such information as frequencies and channel BWs. The Channel Plan is used for optimizing the time used in network search. The WiMAX Forum Mobile Profile [NWGMSPRO] defines how the Channel Plan information is mapped to the band classes. See Section A10.4.7.11 for further details.

A10.4.7.6 WiMAXSupp/Operator/<X>/NetworkParameters/PollingInterval

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Int	Get, Replace

This leaf node specifies how frequently the OMA DM client SHOULD connect to the OMA DM server for polling-based client-initiated management sessions. It is only used for those devices that cannot receive server-initiated sessions. This value is presented in number of minutes.

1) If the value is “-1” (minus 1), then the device SHALL perform ONLY ONE polling-based client-initiated management session to the OMA DM server whenever entering the operator’s network and

obtaining an IP address. The device will immediately poll and the value of PollingAttempts SHALL be ignored.

2) If the value is "0" (zero), then the device SHALL NOT perform any polling based client-initiated management session to the OMA DM server.

3) If the value is greater than zero, then the device SHALL perform a polling-based client-initiated management session to the OMA DM server every "X" minutes (the value specified in this leaf node), starting with one poll immediately after the device obtains an IP address from the operator's network and continuing for n+1 iterations where n is the value of polling attempts. As an example if this is set to 5 and polling attempts is set to 10 the device will poll once after receiving an IP address and 10 times at 5 minute interval for a total of 11 attempts.

A10.4.7.7 WiMAXSupp/Operator/<X>/NetworkParameters/PollingAttempts

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Int	Get, Replace

This leaf node specifies the value for number polling attempts as set by the operator and it supersedes the value set in the device capabilities node set by the manufacturer. This value may be used by the operator to configure the number of times the device will attempt to access client-initiated polling at a periodic interval after the initial polling attempt. As an example if this is set to 10 and PollingInterval is set to 5 the device will poll once after receiving an IP address and 10 times after for a total of 11 attempts. Setting polling attempts to a value of -1 will indicate that the MS shall poll continuously. Setting the value of PollingAttempts to 0 will cause a device to never poll. This OPTIONAL node MAY NOT exist if the 'PollingSupported' is FALSE.

A10.4.7.8 H-NSP Node

This node specifies the H-NSP. All the Home Network Service Provider Identifiers (H-NSP-ID) of a single H-NSP are mapped into one NSP realm and one NSP verbose name, since the NSP is selected via the realm in the Network Access Identifier (NAI) and the WiMAXSupps MOs contain only one realm in the subscription parameters.

A10.4.7.8.1 WiMAXSupp/Operator/<X>/NetworkParameters/H-NSP/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node contains the H-NSP information. All of these interior nodes MUST be located in one H-NSP node.

A10.4.7.8.2 WiMAXSupp/Operator/<X>/NetworkParameters/H-NSP/<X>/H-NSP-ID

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Replace

This leaf node specifies the H-NSP-ID. The format of the NSP-ID is specified in [NWGSTG3] and 24-bit long. All NSP-IDs have the same priority.

A10.4.7.9 CAPL Node

The information in this node is used in network discovery and selection phase. The node instructs which NAP SHALL be selected to establish connection to the home network. ANNEX C represents examples how the nodes are used in network discovery and selection.

A10.4.7.9.1 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/SelectPolicy

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Replace

This leaf node specifies NAP Selection Policy (defined in [Annex E.]) that SHALL be respected for CAPL. Table 3 defines the possible values for SelectPolicy node.

Table 3 - Values for NAP Selection Policy node of CAPL

Value	NAP Selection Policy
0	Reserved.
1	Strict Policy (defined in [ND&S CHANGES])
2	Partially Flexible Policy (defined in [ND&S CHANGES])
3	Fully Flexible Policy (defined in [ND&S CHANGES])

A10.4.7.9.2 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

This interior node contains the entries of **CAPL**.

A10.4.7.9.3 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a place holder of the **CAPL**.

A10.4.7.9.4 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/NAP-ID

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Replace

This leaf node specifies the NAP-ID. The format of the NAP ID is 24 bit-long integer and specified in [NWGSTG3].

A10.4.7.9.5 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/Priority

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Replace

This leaf node specifies the Priority (defined in [ND&S CHANGES]) of the NAP. Table 4 shows the possible values of the priority.

Table 4 - Values of priority in CAPL node

Value	Description
0	Reserved.
1	Highest priority value.
2-249	Values for other priorities.
250	Lowest priority value
251-254	Reserved.
255	Forbidden. Device is not allowed use this NAP to connect to the H-NSP.

A10.4.7.9.6 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/ChPlanRefIds

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This interior node allows an operator to associate one or more Channel Plan entries to a NAP and specifies a NAP Based Channel Plan for a specific NAP. See [ND&S CHANGES] for more information about NAP Based Channel Plan.

A10.4.7.9.7 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/ChPlanRefIds/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a place holder of reference IDs linking to Channel Plan entries.

A10.4.7.9.8 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/ChPlanRefIds/<X>/RefId

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Replace

This leaf node specifies a reference ID to a Channel Plan entry identified by ID located at WiMAXSuppMO/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/Id. The maximum length SHALL be 20 characters.

A10.4.7.10 RAPL Node

The information provided in these nodes are used in network discovery and selection phase for roaming when NAPs, which have direct connection to the H-NSP, are not available. The nodes specify which V-NSP are allowed to be used. ANNEX C represents examples how the nodes are used in network discovery and selection.

A10.4.7.10.1 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/SelectPolicy

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Replace

This leaf node specifies V-NSP Selection Policy (defined in [ND&S CHANGES]) that SHALL be respected for RAPL. Table 5 defines the possible values for SelectPolicy node.

Table 5 - Values for V-NSP Selection Policy Node of RAPL

Value	V-NSP Selection Policy
0	Reserved.
1	Strict Policy (defined in [ND&S CHANGES])
2	Partially Flexible Policy (defined in [ND&S CHANGES])
3	Fully Flexible Policy (defined in [ND&S CHANGES])

A10.4.7.10.2 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

This interior node contains the entries of RAPL.

A10.4.7.10.3 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a place holder of the RAPL.

A10.4.7.10.4 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries/<X>/V-NSP-ID

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Replace

This leaf node specifies the V-NSP-ID. The format of the NSP ID is 24 bit-long integer and specified in [NWGSTG3].

A10.4.7.10.5 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries/<X>/Priority

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Replace

This leaf node specifies the Priority (defined in [ND&S CHANGES]) of the V-NSP. Table 6 shows the possible values of the priority.

Table 6 - Value of priority in RAPL node

Value	Description
0	Reserved.
1	Highest priority value.
2-249	Values for other priorities.
250	Lowest priority value
251-254	Reserved.
255	Forbidden. Device is not allowed to use this V-NSP to connect to the H-NSP.

A10.4.7.11 Channel Plan Node

Channel Plan node specifies Channel Plan configurations that can be used in network discovery and selection procedure. It is up to the service provider how to populate the Channel Plans. More information on different kind of Channel Plans and their usage can be found from [ND&S CHANGES].

A10.4.7.11.1 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

This interior node contains the entries for Channel Plan

A10.4.7.11.2 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/BW

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Replace

This leaf node specifies the default BW value in kHz for all the Channel Plan entries. If /ChannelPlan/Entries/<X>/BW does not specify any value for BW, this value SHALL be used.

A10.4.7.11.3 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/FFTSize

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Replace

This leaf node specifies the default FFT size for all the Channel Plan entries. If /ChannelPlan/Entries/<X>/FFTSize does not specify any value for FFT size, this value SHALL be used.

A10.4.7.11.4 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/DuplexMode

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Replace

This leaf node specifies the default duplex modes for all the Channel Plan entries. If /ChannelPlan/Entries/<X>/DublexMode does not specify any value for DuplexMode, this value MUST be used. See the possible values in the Section A.10.4.7.11.5.9.

A10.4.7.11.5 Channel Plan Entries

Channel Plan information is used in the network discovery and selection procedures. All Channel Plan entries are part of the Root Channel Plan. The entries of Root Channel Plan SHALL be in preferred order. It is recommended to design Channel Plan entries in a way that the same physical information is not defined in multiple entries.

A.10.4.7.11.5.1 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a placeholder of the channels or channel-ranges of the Channel Plan.

A.10.4.7.11.5.2 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/Id

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Chr	Get, Replace

This leaf node allows an operator to associate a Channel Plan entry to one or more NAPs. References to Channel Plan entries within CAPL are specified in /CAPL/Entries/<X>/ChPlanRefIds node. Entries which are referred to are part of one or more NAP Based Channel Plans. One Channel Plan entry can be associated with multiple NAPs. This optional node MUST be supported by the client that supports NAP Based Channel Plan (i.e. /CAPL/Entries/<X>/ChPlanRefIds). See ANNEX C for recommendation on implementation details. The maximum length SHALL be 20 characters.

A.10.4.7.11.5.3 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/FirstFreq

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Replace

This leaf node specifies the first center frequency (in kHz) for this channel range.

A.10.4.7.11.5.4 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/LastFreq

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Replace

This leaf node specifies the last center frequency (in kHz) for this channel range. If this value equals to the FirstFreq or the node is omitted, then this entry refers to a single channel rather than a channel range. If this field is present, NextFreqStep field SHALL be present as well.

A.10.4.7.11.5.5 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/NextFreqStep

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Replace

This leaf node defines the frequency step (in kHz) to reach the next central frequency when defining the frequency range using FirstFreq and LastFreq. When the node is omitted there is only one central frequency in this entry that is FirstFreq. If this field is present, LastFreq field SHALL be present as well.

The formula to calculate the next central frequencies is:

CurrentFreq = FirstFreq

While (CurrentFreq <= LastFreq) CurrentFreq = CurrentFreq + NextFreqStep

A.10.4.7.11.5.6 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/Preambles

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Chr	Get, Replace

A bitmap of 114 bits specifying the valid preambles for each channel in this channel range

The value is a hexadecimal string, which is 29 digit long. The two MSB are zeroed and the LSB indicates channel 0.

A.10.4.7.11.5.7 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/BW

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Replace

This leaf node specifies the individual channel BW (in kHz) for the channel in this entry.

Note: The client uses this value for the BW for this specific channel entry instead of the default BW value specified in /ChannelPlan/BW.

A.10.4.7.11.5.8 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/FFTSize

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Replace

This leaf node specifies the size of the channel's FFT in this entry.

Note. The client uses this value for the FFT size for this specific channel entry instead of the default FFT size value specified in /ChannelPlan/FFTSize

A.10.4.7.11.5.9 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries <X>/DuplexMode

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Replace

This leaf node specifies the duplex mode of the channel in this entry. Table 7 defines the values of the DublexMode.

Note: The client uses this value for the duplex mode for this specific channel entry instead of the default duplex mode value specified in /ChannelPlan/DuplexMode.

Table 7 - Values of Duplex Mode node

Value	Description
0	Reserved
1	TDD
2	FDD
3	HFDD

4-255	Reserved

A10.4.8 Subscription Parameters Node

The subscription parameter interior node contains information associated with user subscription. A user is allowed to have more than one subscription with an operator. This node enables a user and the operators to manage authentication parameters that are associated with user's subscriptions. The decision of which subscription parameters are used during network entry authentication is out of the scope of this specification.

A10.4.8.1 WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the primary subscription parameters. See Section A10.4.8.3 for further details.

A10.4.8.2 WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions

Status	Tree Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

This interior node contains the subscription parameters, which are associated with additional subscriptions present on the device. See Section A10.4.8.4 for further details.

A10.4.8.3 Primary Subscription parameters

This interior node contains the primary subscriber parameters.

A10.4.8.3.1 WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/Name

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Replace

This leaf node specifies the human readable name of the primary subscriber. The operator SHALL assure the human readable name of the primary subscriber is unique from all other subscriptions of the same operator, so that the operator can differentiate between subscriptions.

The MIME type of the node SHALL be 'text/plain; charset=utf-8'. The maximum length SHALL be 255 bytes. In UTF-8 format, each character MAY take one to four bytes.

A10.4.8.3.2 WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/Activated

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get, Replace

This leaf node indicates the provisioning status of the Primary Subscriber. If the value of the node is FALSE, the device SHALL enter the network in the provisioning mode when using primary subscription, by providing a WiMAX decorated NAI during the EAP negotiation that indicates the provisioning service mode as described in [OTAGEN] section 8.2. Upon completion of the provisioning phase, the OMA DM server SHALL set the value to TRUE to indicate that the device SHALL use regular network entry using the provisioned parameters. As long as this leaf node value is true, all provisioned parameters should be considered by the device as the most updated parameters hence the device should first use the provisioned operator name and subscription parameters for its normal operation and only afterwards can use other alternative sources for the same parameters, if needed, such as 802.16 MAC messages. This node SHALL be included into the last OMA DM Package message from the Device Management Server to the device. When this node is sent to the device, it is able to know that all configurations are uploaded to the device.

The point of time when the OMA-Session, in which this node was set, was completed is considered as the completion point of provisioning phase by the device. (if the device needs to trigger something at the end of activation, it will use this point as the trigger).

A10.4.8.3.3 WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/EAP

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

The EAP interior node contains parameters for EAP authentication methods. It contains EAP MO as specified in [DMEAPMO]. Only a single EAP method is allowed to be configured for the MS to use with a specific operator. In the case it is a tunneled method (such as TTLS): the definition shall include the outer and the inner method nodes.

See B3 for further details. In case EAP node is not populated, authentication is not performed.

A10.4.8.4 Other Subscription Parameters

This interior node contains subscription parameters, which are associated with additional subscriptions present on the device.

A10.4.8.4.1 WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node lists the entries in the Other Subscription Parameters. There MUST be exactly one OtherSubscriptions node for each of these interior nodes.

A10.4.8.4.2 WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X>/Name

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Replace

This leaf node defines the human readable name of an additional subscription. The operator SHALL assure the human readable name of the additional subscription is unique from all other subscriptions of the same operator, so that the operator can differentiate between subscriptions.

The MIME type of the node SHALL be 'text/plain; charset=utf-8'. The maximum length SHALL be 255 bytes. In UTF-8 format, each character MAY take one to four bytes.

A10.4.8.4.3 WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X>/Activated

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get, Replace

This leaf node indicates the provisioning status of Other Subscriber. If the value of the node is FALSE, the device SHALL enter the network in the provisioning mode when using this subscription data, i.e., by providing a WiMAX decorated NAI during the EAP negotiation that indicates the provisioning service mode as described in [OTAGEN] section 8.2. Upon completion of the provisioning phase, the OMA DM server SHALL set the value to TRUE to indicate that the device SHALL use regular network entry using the provisioned parameters. As long as this leaf node value is true, all provisioned parameters should be considered by the device as the most updated parameters hence the device should first use the provisioned operator name and subscription parameters for its normal operation and only afterwards can use other alternative sources for the same parameters, if needed, such as 802.16 MAC messages.

The point of time when the OMA-Session, in which this node was set, was completed is considered as the completion point of provisioning phase by the device. (if the device needs to trigger something at the end of activation, it will use this point as the trigger).

A10.4.8.4.4 WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X>/EAP

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

The EAP interior node contains parameters for EAP authentication methods. It contains EAP MO as specified in [DMEAPMO]. Only a single EAP method is allowed to be configured for the MS to use with a

specific operator. In the case it is a tunneled method (such as TTLS): the definition shall include the outer and the inner method nodes.

See B3 for further details. In case EAP node is not populated authentication is not performed.

A10.4.9 RootCA Node

The RootCA node contains an additional list of trusted rootCA certificates to be used during mutual authentication between the device and the network. Since the RootCA node is defined under each operator, the following practices MUST be followed:

1. For Operators:
   1.1. The operator SHOULD send its trusted rootCA certificates at the end of the initial activation and provisioning flow.
   1.2. The operator SHOULD update the list of trusted rootCA certificates to ensure that the device does not lose its capability to validate the network (AAA server) due to the lack of proper CA certificates.
2. For Devices:
   2.1. The used root CA certificates MUST be specified by the CERT nodes of the current operator's effective EAP MO [DMEAPMO] in a normal network entry which uses provisioned information. The device MUST NOT use any other root CA certificates.
   2.2. The device MUST EITHER use:
      2.2.1. RootCA certificates embedded in the device at the point of manufacturing (POM), OR
      2.2.2. The RootCA node's certificates in the mutual authentication between the device and the network (AAA server).

A10.4.9.1 WiMAXSupp/Operator/<X>/RootCA/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a placeholder of the additional root CA Certificates trusted by a specific operator.

A10.4.9.2 WiMAXSupp/Operator/<X>/RootCA/<X>/Certificate

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bin	No Get

This leaf node contains the actual binary Root Certificate. The format of Root CA SHALL be X.509 and DER.

A10.4.10 Contacts Node

This node contains a number of contact info nodes an operator MAY wish to make available to its subscribers. Two types, one for technical support and another for subscription portal, are mandatory, others are available for use by operators.

A10.4.10.1 WiMAXSupp/Operator/<X>/Contacts/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a placeholder of multiple support contact addresses.

A10.4.10.2 WiMAXSupp/Operator/<X>/Contacts/<X>/Type

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Replace

This leaf node defines a URI contact type that will be made visible to the user.

Table 8 - Values of URI Type

Value	Availability	Description
0	Reserved	Mandatory contact node for the operator's technical support contact information.
1	Reserved	Mandatory contact node for operator's subscription portal contact information.
2 – 199	Reserved	Reserved for future use.
200 -255	Available	Operator defined URI types (e.g., My account, FAQ, etc.)

A10.4.10.3 WiMAXSupp/Operator/<X>/Contacts/<X>/Trigger

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Null	Exec

This leaf node specifies a trigger to start the contact action or process. The client device SHOULD indicate to a user interface application that there is a message waiting for the user. The user interface application SHOULD, upon receipt of user approval, execute the URI within the context of the device.

For example, if the device is a laptop the user interface application MAY launch the default web browser for a "http://" prefixed URI or MAY launch a VoIP client application for a "sip://" prefixed URI.

The types of actionable URI prefixes are outside the scope of this specification and are implementation specific.

The execution of the URI-based contact action or process SHALL be performed either synchronously as part of the current DM session (i.e., run to completion before executing the next DM operation or terminating the current DM session) or asynchronously from the current DM session (i.e., run in parallel with the DM session continuing to execute the next DM operations and/or terminating the current DM session). After execution of the URI-based contact action or process, the client MAY issue a generic alert, as described in [DMPRO], to the DM server indicating the result of the contact action or process after it completes or fails. The URI of the WiMAX Supplementary MO SHALL be sent as the source element of the generic alert in order to allow the DM server to identify the origin of the alert. The definition of the alert type returned as the meta type element in the generic alert is beyond of scope of this document but MAY be defined in future revisions of this spec.

A10.4.10.4 WiMAXSupp/Operator/<X>/Contacts/<X>/URI

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Replace

This leaf node specifies a contact address in URI format.

The URI string will most often be a telephone number (e.g., tel:+ 911), a SIP VoIP contact (e.g., sip:alice@wonderland.com) or a URL (e.g., http://wireless.com/TechnicalSupport). Other URI resource types MAY be specified, but the device MAY NOT implement support for all URI formats. The maximum length SHALL be 1024 characters.

A10.4.10.5 WiMAXSupp/Operator/<X>/Contacts/<X>/Text

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Chr	Get, Replace

This leaf node specifies a simple string that can be displayed to the user for the given contact type. For example this could be "Technical Support" or "Subscription Portal". The maximum length SHOULD be 255 characters.

ANNEX B. OMA Connectivity Management Objects [Normative]

B3 OMA EAP Management Object

This section describes how the generic EAP MO [DMEAPMO] is used in WiMAX. The statuses and descriptions of the nodes are modified according to the following table to fit the generic EAP MO to the WiMAX needs. The definitions for the usage of the nodes listed in this table MUST be followed. The non-listed nodes MUST be used as specified in [DMEAPMO].

Node	Status	Comment
EAP/<X>/METHOD-TYPE	[DMEAPMO]	See the node description [DMEAPMO]. The node can be used for referring to EAP methods which do not require using expanded EAP type identifiers, e.g. EAP-TLS, EAP-TTLS, and EAP-AKA.
EAP/<X>/VENDOR-ID	[DMEAPMO]	See the node description [DMEAPMO]. The node MUST be used for Plain-MSCHAPV2. VENDOR-ID MUST be 24757 (WMF) for Plain-MSCHAPV2.
EAP/<X>/VENDOR-TYPE	[DMEAPMO]	See the node description [DMEAPMO]. The node MUST be used for Plain-MSCHAPV2. VENDOR-TYPE MUST be 1 for Plain-MSCHAPV2.
EAP/<X>/PASSWORD	[DMEAPMO]	See the node description [DMEAPMO]. The maximum length in WiMAX is 253 characters. REQUIRED for Plain-MSCHAPv2.
EAP/<X>/PROVISIONED-PSEUDO-IDENTITY	[DMEAPMO]	In WiMAX this leaf node contains the provisioned pseudonym identity to be used in the first network entry, when EAP-AKA is used for the user authentication. When this node is present, the provisioned pseudonym identity SHALL be used and the permanent identity SHALL NOT be sent to the network during the first authentication. If this node is not present then the permanent identity is used for the first authentication.

Node	Status	Comment
EAP/<*X*>/USE-PRIVACY	[DMEAPMO]	In WiMAX EAP-AKA, there are two possible ways the device can operate upon receipt of a permanent identity request from the AAA server [RFC 4187 Section 4.1.6]. This leaf node defines which way the device SHALL perform upon that request, i.e., AT_PERMANENT_ID_REQ. If the value of this node is TRUE and if the device has a pseudonym identity available then the permanent identity SHALL NOT be sent to the network even if it is explicitly requested by the server. If this node is FALSE or missing, then the permanent identity SHALL be sent to the network when the permanent identity is requested by the server. If the device has no pseudonym identity available then the permanent identity SHALL be sent to the network when requested, regardless of this node. In other WiMAX EAP methods excluding EAP-TLS, e.g., EAP-TTLS, if this node is TRUE then the device SHALL use a randomly generated username in outer EAP-Response/Identity. If this node is FALSE or missing then any type of identity conforming to each EAP method can be used. Realm portion of the NAI (Network Access Identified) is still required to route authentication to the home network in all cases.
EAP/<X>/EAP-AKA/USE-CHECKCODE	REQUIRED	In WiMAX, if USE-CHECKCODE is TRUE then AT_CHECKCODE SHALL be included in EAP Response/AKA-Challenge or EAP-Response/AKA-Reauthentication message. If this is FALSE or missing then AT_CHECKCODE is not sent by the device. However, regardless of this node, AT_CHECKCODE MUST be used when new attributes are included in EAP-Request/AKA-Identity or EAP-Response/AKA-Identity message [RFC 4187 Chapter 8.2].
EAP/<X>/CERT	REQUIRED	See the node description [DMEAPMO].
EAP/<X>/CERT/<X>/CERT-TYPE	[DMEAPMO]	See the node description [DMEAPMO]. At least DEVICE and CA certificate types are REQUIRED in WiMAX.
EAP/<X>/CERT/<X>/SER-NUM	REQUIRED	See the node description [DMEAPMO].
EAP/<X>/CERT/<X>/ISSUER	REQUIRED	See the node description [DMEAPMO].

B3.1 Method Related Parameters

The following Table 9 provides an overview of the EAP settings used together with each EAP Method.

Table 9 - EAP Method versus Used Parameters

EAP Method/Used Parameters	EAP-AKA	EAP-TLS	EAP-TTLS	PLAIN-MSCHAPv2
METHOD-TYPE	X	X	X	

EAP Method/Used Parameters	EAP-AKA	EAP-TLS	EAP-TTLS	PLAIN-MSCHAPv2
VENDOR-ID				X
VENDOR-TYPE				X
USER-IDENTITY	X	X	X	X
PASSWORD				X
REALM	X	X	X	
PROVISIONED-PSEUDO-IDENTITY	X			
USE-PRIVACY	X	X	X	
EAP-AKA/USE-CHECKCODE	X			
ENCAPS	X	X		X
VFY-SRV-REALM		X	X	
SERVER-REALMS/<X>/SERVER-REALM		X	X	
CA-CERT				
CERT-TYPE		X	X	
ISSUER		X	X	
SER-NUM		X	X	
DEVICE-CERT				
CERT-TYPE		X	X	

1

2

B3.2 Example: EAP-TTLSv0 and Plain-MSCHAPv2

Figure 13 illustrates how EAP-TTLSv0 and PLAIN-MSCHAPv2 parameters can be used and linked together using the ENCAPS node.

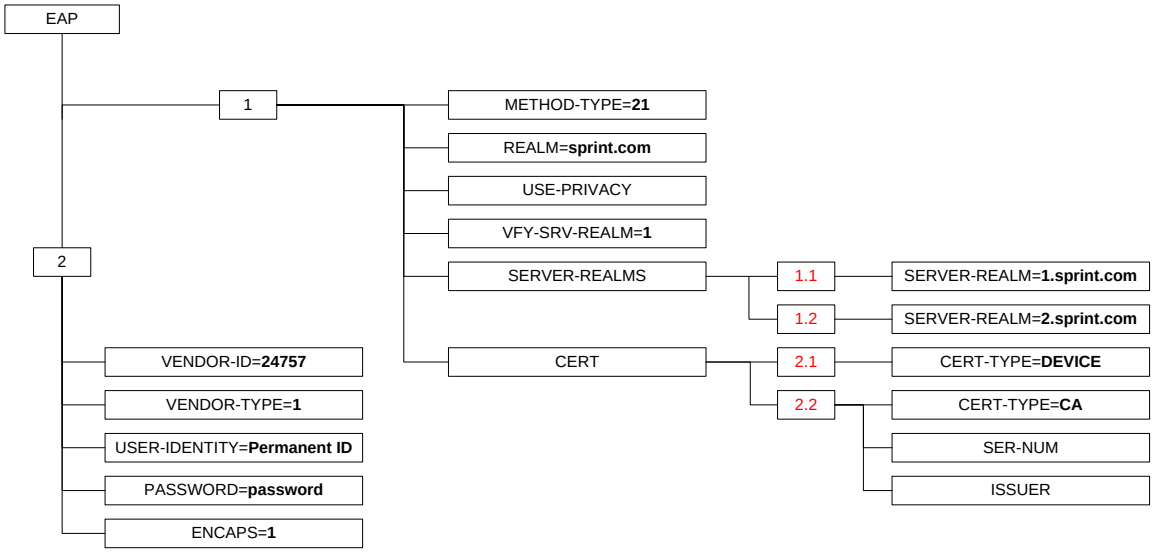


Figure 13 - Example of EAP-TTLSv0 and PLAIN-MSCHAPv2 parameters

Example: EAP-TLS, EAP-TTLSv0 and Plain-MSCHAPv2

In the case the device falls back from TTLS to TLS as defined in NWGSTG3 4.4.1.4.1.1.1 – all the parameters for the TLS authentication will be taken from the TTLS node which is node number 1 in this example.

B3.3 Example: EAP-AKA in Stand alone Mode

Figure 14 illustrates an example of how the leaf nodes can be constructed in the EAP node when the EAP-AKA is used for the user authentication.

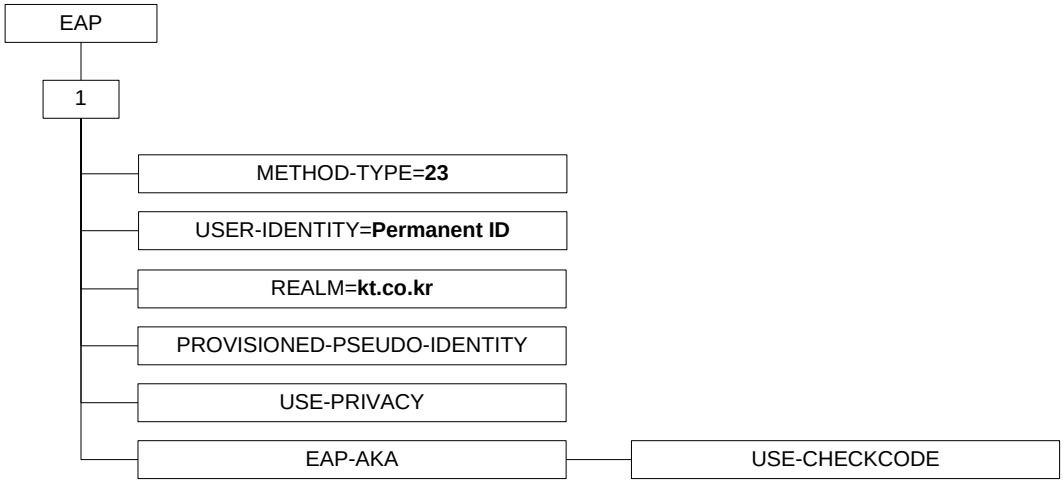


Figure 14 - Example of EAP-AKA parameters

B3.4 Example: EAP-AKA with EAP-TTLS Encapsulation

Figure 15 illustrates an example of how the leaf nodes can be constructed in the EAP node when the EAP-AKA is used with EAP-TTLS encapsulation for the device and user authentication.

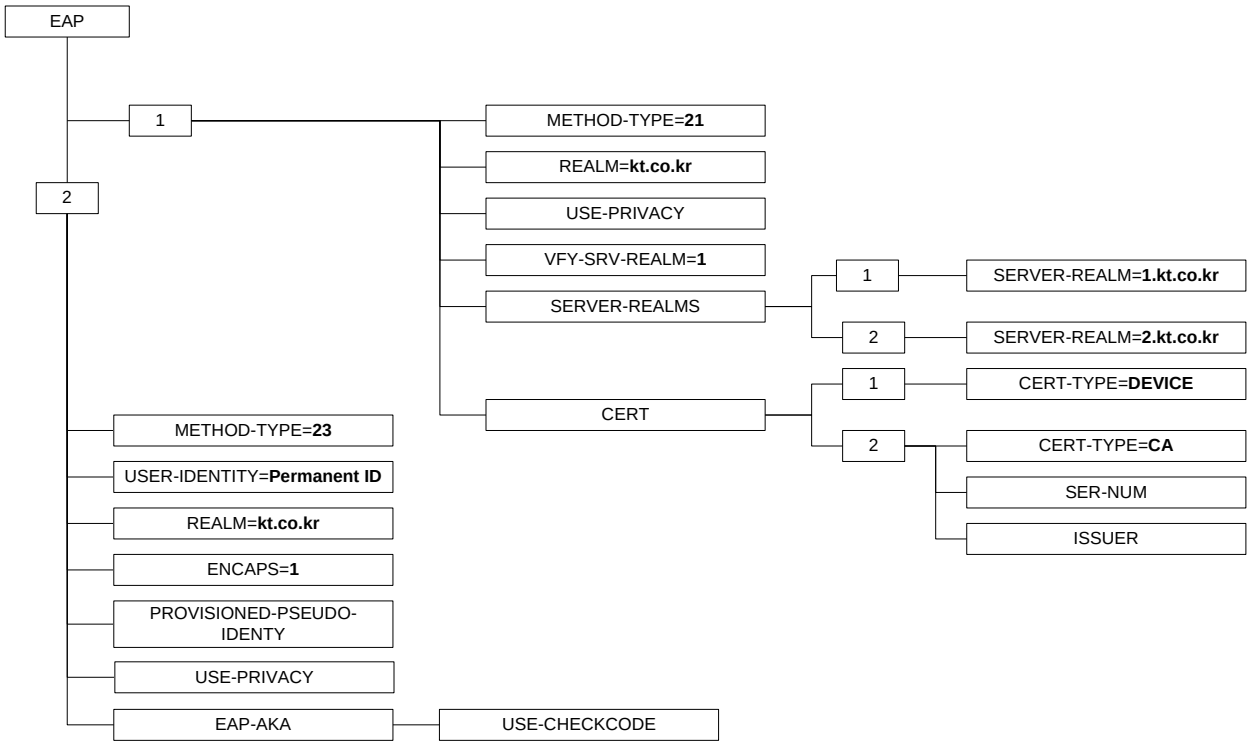


Figure 15 - Example of EAP-AKA and EAP-TTLS parameters

B4 OMA IP Management Object

This Section describes how the generic IP MO [DMIPMO] is used in WiMAX. The description of the nodes is in [DMIPMO] but the status of some nodes MUST be changed as the following table for WiMAX to fit the generic IP MO to the WiMAX needs.

Node	Status	Comment
MIPv4/SharedSecret	REQUIRED	Contains the NAI configuration for the MIPv4 registration. In WiMAX, the SharedSecret key is generated dynamically and locally. See [NWGSTAGE3].
MIPv4/SharedSecret/NAI/<X>/Use-Pseudo	REQUIRED	Indicates to the MIPv4 stack to use pseudo username in the MIPv4 registration.
MIPv4/Protocol/	REQUIRED	Specifies the MIPv4 protocol configuration.
MIPv4/Protocol/RevTun	REQUIRED	In WiMAX, the value SHOULD be TRUE.
MIPv4/Protocol/RetryCount	REQUIRED	See the node description in [DMIPMO].
MIPv4/Protocol/RetryTimer	REQUIRED	See the node description in [DMIPMO].
MIPv4/Protocol/RegPeriod	REQUIRED	See the node description in [DMIPMO].

MIPv4/Protocol/RegPeriodRel	REQUIRED	See the node description in [DMIPMO].
MIPv4/Protocol/NatTraversal	OPTIONAL	NAT Traversal is not used in WiMAX so this node SHOULD not be supported.
MIPv6/SharedSecret	REQUIRED	Contains the NAI configuration for the MIPv6 registration. The SharedSecret key is generated dynamically and locally. See [NWGSTAGE3].
MIPv6/SharedSecret/NAI/<X>/Use-Pseudo	REQUIRED	Indicates to the MIPv6 stack to use pseudo username in the MIPv6 registration.
MIPv6/Protocol/	REQUIRED	Specifies the MIPv6 protocol configuration.
MIPv6/Protocol/RouteOpt	REQUIRED	In WiMAX the value MAY be FALSE.
MIPv6/Protocol/RetryCount	REQUIRED	See the node description in [DMIPMO].
MIPv6/Protocol/RetryTimer	REQUIRED	See the node description in [DMIPMO].
MIPv6/Protocol/BindingLifeTime	REQUIRED	See the node description in [DMIPMO].
MIPv6/Protocol/BindingLifeTimeRel	REQUIRED	See the node description in [DMIPMO].
MIPv6/Protocol/SignalingProtection	REQUIRED	In WiMAX the value SHOULD be AUTHOPT.

B5 OMA NAP Management Object

B5.1 Definitions for OMA Network Access Point (NAP) Management Object

The WIMAX sub-tree specified in this Section SHALL be placed under the BearerParams node in [DMCONNMO]. See B5.2 for examples. Device Management servers SHALL support OMA NAP MO for WiMAX bearer configuration while devices MAY support it.

B5.1.1 ../BearerType

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

The *BearerType* node value specified in [DMCONNMO] MUST be “WIMAX”.

B5.1.2 ../AddrType

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

The *AddrType* in the OMA NAP MO specified in [DMCONNMO] MUST be supported and the value MUST be from the Table 10:

Table 10 - NAP Address Types

AddrType	Description
NAI	The Addr field SHALL identify a unique subscription under the WiMAX Supplementary MO. The Addr value SHALL be formatted as an NAI [RFC4282]

B5.1.3 ../Addr

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

The username portion of the NAI is used to identify a unique subscriber under the operator's subscription parameters. The primary subscription is identified with an empty username, i.e. using the value "@realm". A subscription other than the primary is identified with a non-empty username and in this case the value of the username SHALL be the same as the name of the dynamic node under *WiMAXSupp/SubscriptionParameters/OtherSubscriptions/<X>*, e.g. "1@realm".

B5.1.4 ../BearerParams/WIMAX

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the WiMAX bearer specific parameters for Network Access Point Management Object.

B5.1.5 ../BearerParams/WIMAX/TO-WIMAXSUPP-REF

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This interior node specifies a link to the operator specific dynamic node *WiMAXSupp/Operator/<X>*.

B5.2 Example: Linkage Between the OMA Network Access Point (NAP) MO WiMAX Supplementary MO

The Figure 16 shows how the OMA NAP MO is used to specify a WiMAX Bearer configuration using the primary subscription parameters. The primary subscription is identified by an Addr value "@realm", where the username is empty.

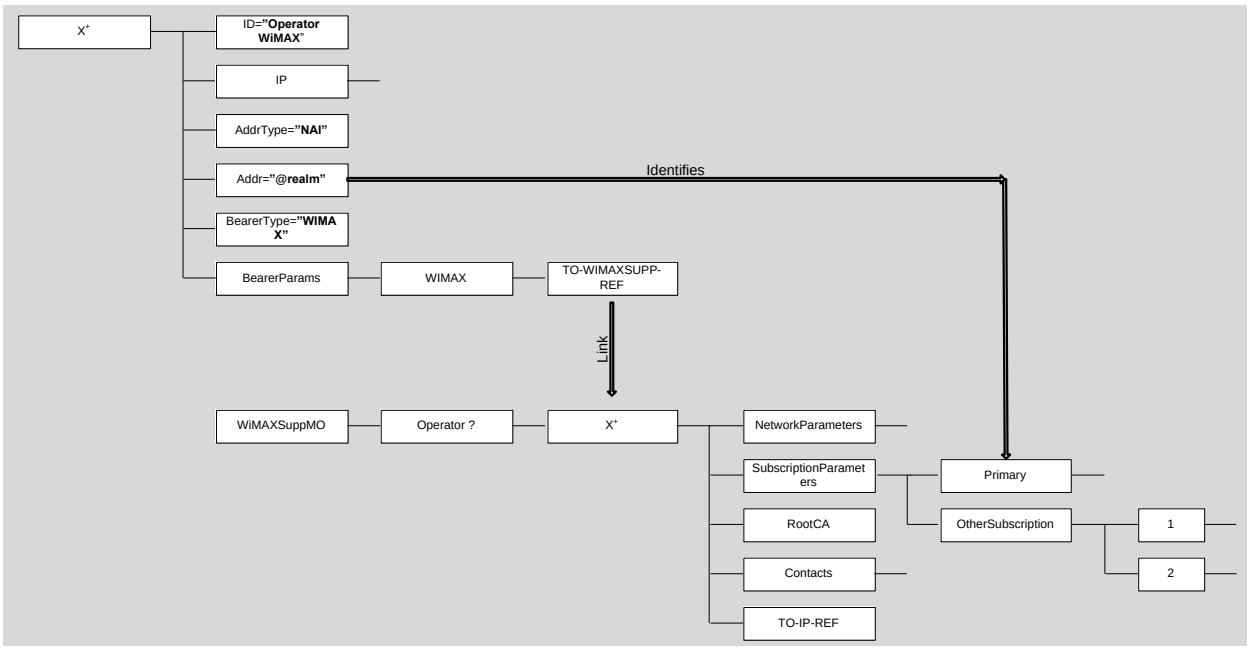


Figure 16 - Linkage Between NAP MO and WiMAXSupp (Primary Subscription)

The Figure 17 shows how the OMA NAP MO is used to specify a WiMAX Bearer configuration using a non-primary subscription parameters. The non-primary subscription is identified by Addr value "1@realm", where the "1" is the name of the dynamic node of the non-primary subscription.

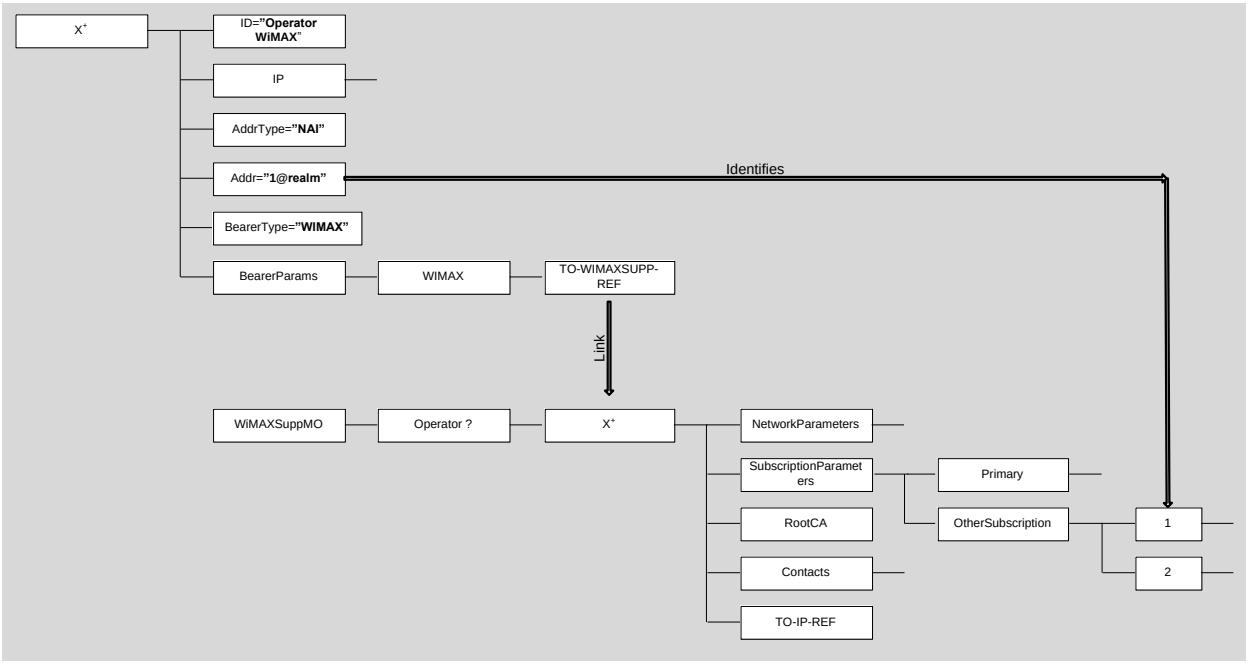


Figure 17 - Linkage Between NAP MO and WiMAXSupp (Other Subscriptions)

ANNEX C. CAPL, RAPL and Channel Plan Examples

[Add a new Annex into NWG Rel 1, Version 1.2.0, Stage 3]

All examples in this section refer to the situation where the device is using an operator controlled CAPL and RAPL from a single operator, a user controlled CAPL and RAPL (having higher priority than the operator controlled CAPL and RAPL), does not exist and prior connection information is not available.

The operator is recommended to configure the selection policy and priorities of the NAPs and V-NSPs taking into account the time to acquire a connection and its effect on the user experience. In addition, when several H-NSPs exist in a device, connection to a particular H-NSP may be skipped if an acceptable NAP (according to configuration information) is not found before a valid attempt to connect to another H-NSP occurs (acceptable NAP of the other H-NSP found).

C3 Parameters used in CAPL and RAPL nodes

C3.1 Example: Strict CAPL and RAPL with Priority – Networks Available

Figure 18 and Figure 19 illustrate an example of how CAPL and RAPL can be used in a strict way, which means that only NAPs in CAPL, and V-NSPs in RAPL, are allowed to be used for establishing the connection to the network.

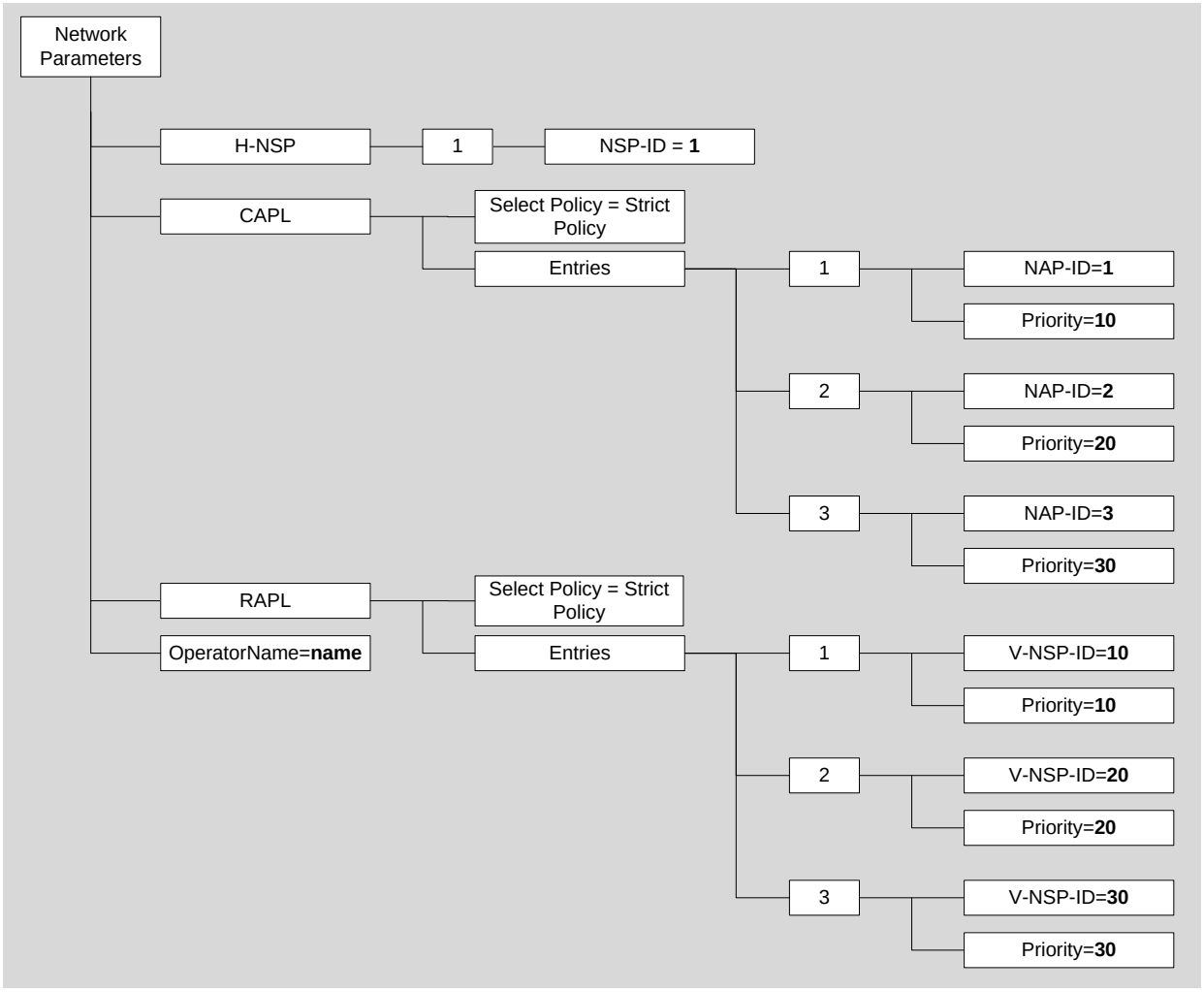


Figure 18 - An example configuration how strict CAPL and RAPL are used with priority

Network Service Provider MAY have Contractual Agreement with NAPs, which are not in the CAPL due to

- Deployment and agreement reasons; different access types e.g., fixed, portable or mobility MAY have different kind of configurations and network coverage restrictions.
- The provisioned information in the device is not up-to-date.

These same reasons MAY apply to RAPL as well.

Note! Strict CAPL MAY be used when the RAPL is flexible and vice versa.

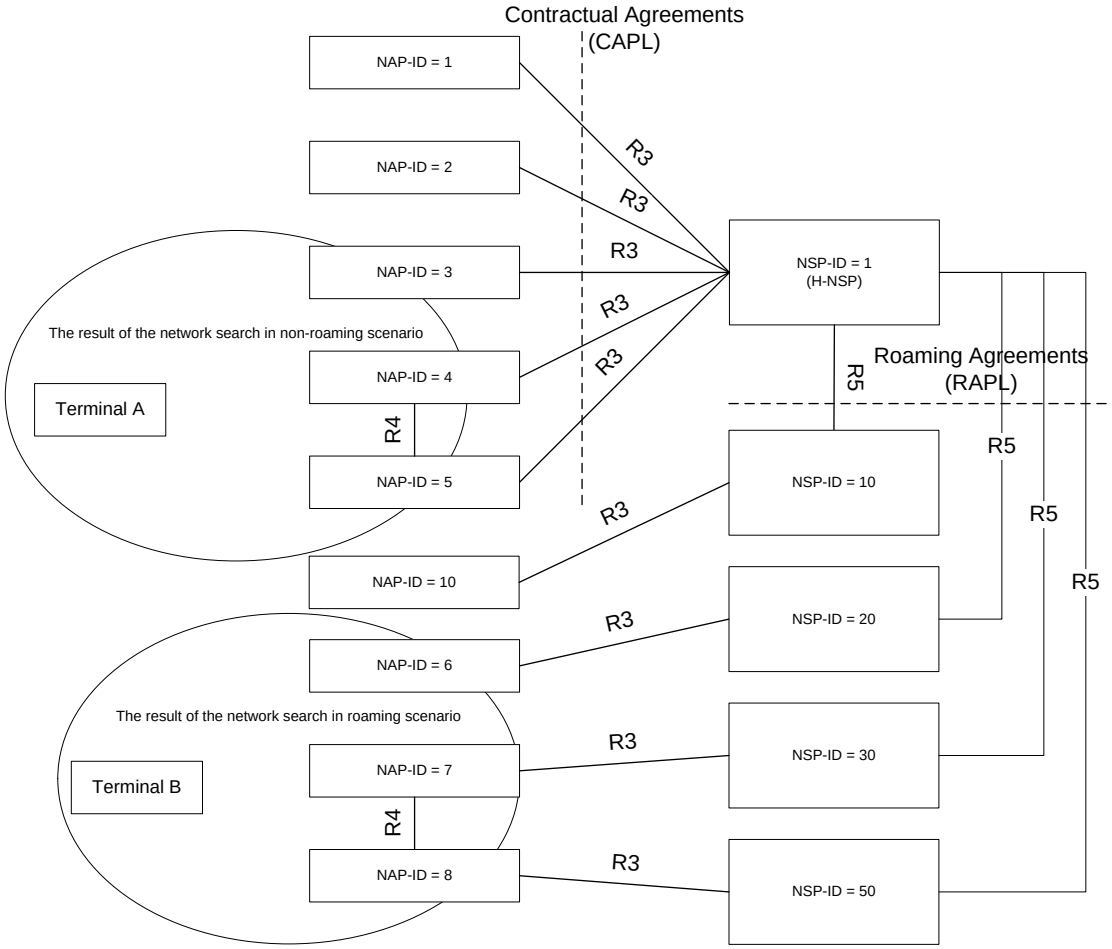


Figure 19 - Network setup

C3.1.1 Non-roaming Scenario with Terminal A:

The result of the network search is

NAP-ID = 3 -> NSP-ID = 1

NAP-ID = 4 -> (not in CAPL)

NAP-ID = 5 -> (not in CAPL)

The device SHALL use NAP-ID=3 to connect to the home network, since it is the only NAP found in the network search that is in the CAPL.

C3.1.2 Roaming Scenario with Terminal B:

The result of the network search is

NAP-ID = 6 -> NSP-ID = 20 -> NSP-ID = 1

NAP-ID = 7 -> NSP-ID = 30 -> NSP-ID = 1

NAP-ID = 8 -> NSP-ID = 50 -> NSP-ID = 1

NAPs listed in CAPL are not found and therefore the device resorts to RAPL. The device SHALL use NAP-ID = 6 and V-NSP-ID = 20 to connect to the home network, since NSP-ID=20 has the highest priority in the RAPL.

C3.2 Example: No Restrictions in CAPL and RAPL

Figure 20 illustrates an example of how the device is allowed to establish connection to any NAP or V-NSP, which has direct connection to the H-NSP, in non-roaming and roaming scenario.

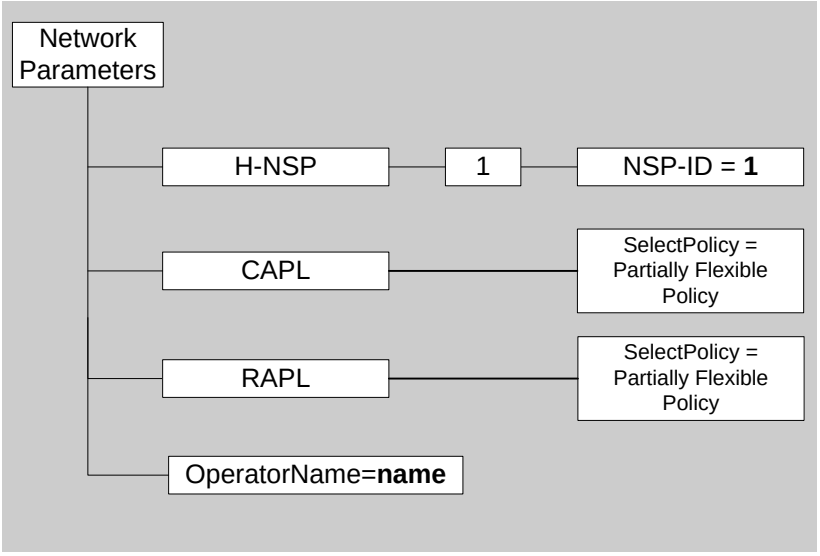


Figure 20 - An example configuration of no restrictions in CAPL and RAPL

C3.2.1 Non-roaming Scenario:

The device is allowed to use whatever NAP, which has a direct connection to the H-NSP.

C3.2.2 Roaming Scenario:

NAPs which have direct connection to the H-NSP are not found and therefore the device resorts to RAPL. The device is allowed to use whatever V-NSP, which has direct connection to the H-NSP. Determination of how the device knows that a V-NSP has direct connection to the H-NSP is out of scope of this specification.

C3.3 Example: Flexible CAPL and RAPL with Priority

Figure 21 and Figure 22 illustrate an example of how the operator can specify a set of NAPs and V-NSPs and still allow the device to establish connections using NAPs and/or V-NSPs, which are not listed in CAPL or RAPL.

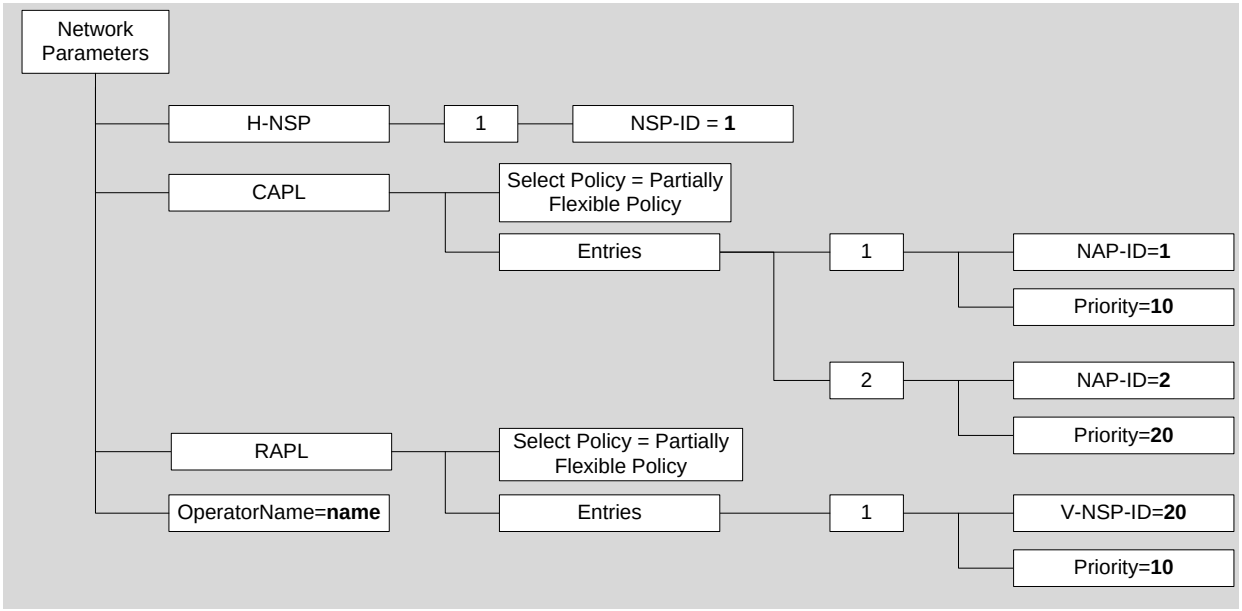


Figure 21 - An example configuration of flexible CAPL and RAPL with priority

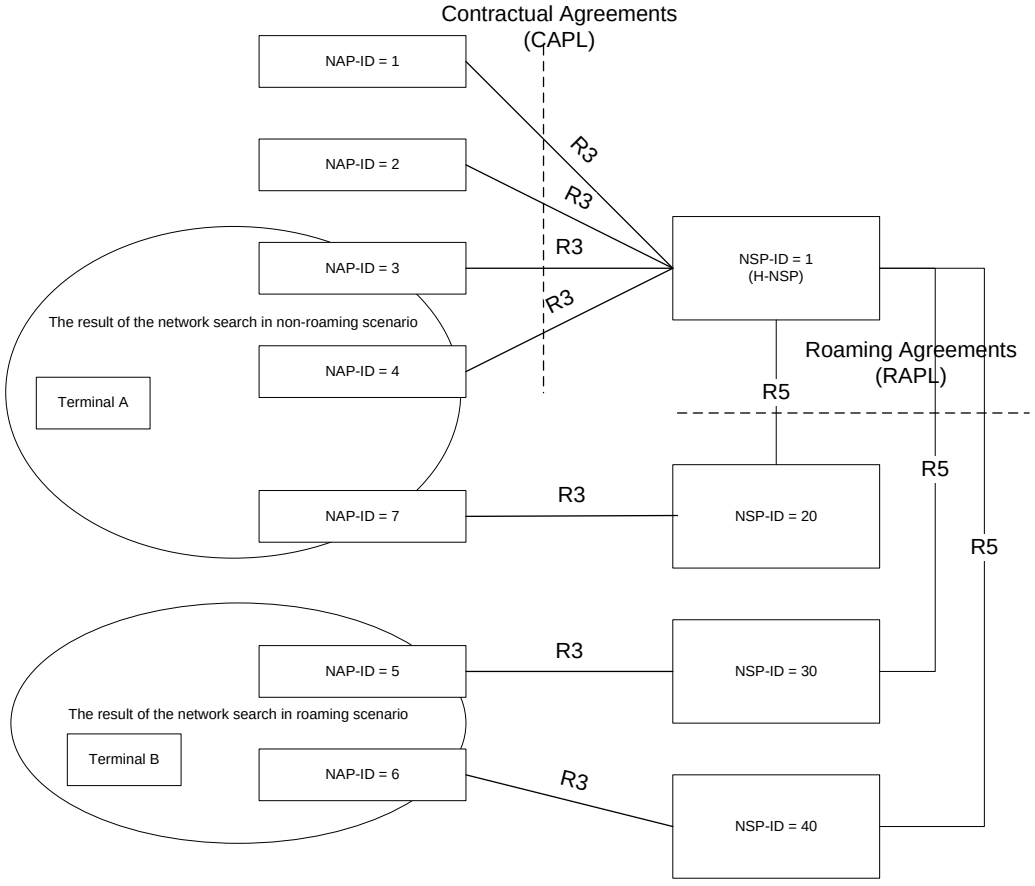


Figure 22 - Network setup

C3.3.1 Non-roaming Scenario with Terminal A:

The result of the network search is

NAP-ID = 3 -> NSP-ID = 1

NAP-ID = 4 -> NSP-ID = 1

NAP-ID = 7 -> NSP-ID = 20 -> NSP-ID = 1

The device MAY use either NAP-ID = 3 or NAP-ID = 4 to connect to the home network. It is implementation specific which one is selected. However the device SHALL NOT use NAP-ID = 7 because it does not have direct connection to the H-NSP and the result of the network search contained NAPs, which have direct connection to the H-NSP.

C3.3.2 Roaming Scenario with Terminal B:

The result of the network search is

NAP-ID = 5 -> NSP-ID = 30 -> NSP-ID = 1

NAP-ID = 6 -> NSP-ID = 40 -> NSP-ID = 1

NAPs listed in CAPL are not found and therefore the device resorts to RAPL. The device MAY use either NAP-ID = 5 or NAP-ID = 6 to connect to the home network via NSP-ID = 30 or NSP-ID = 40. It is implementation specific which one is selected.

C3.4 Example: Strict CAPL and RAPL with Priority – Networks Not Available

Figure 23 and Figure 24 illustrate an example of how CAPL and RAPL can be used in a strict way, which means that only NAPs, which are listed in CAPL, and V-NSPs, which are listed in RAPL, are allowed to be used to connect the network. In this example the terminal is not allowed to connect to the network because the network search does not return any NAPs or V-NSPs which are in CAPL or RAPL.

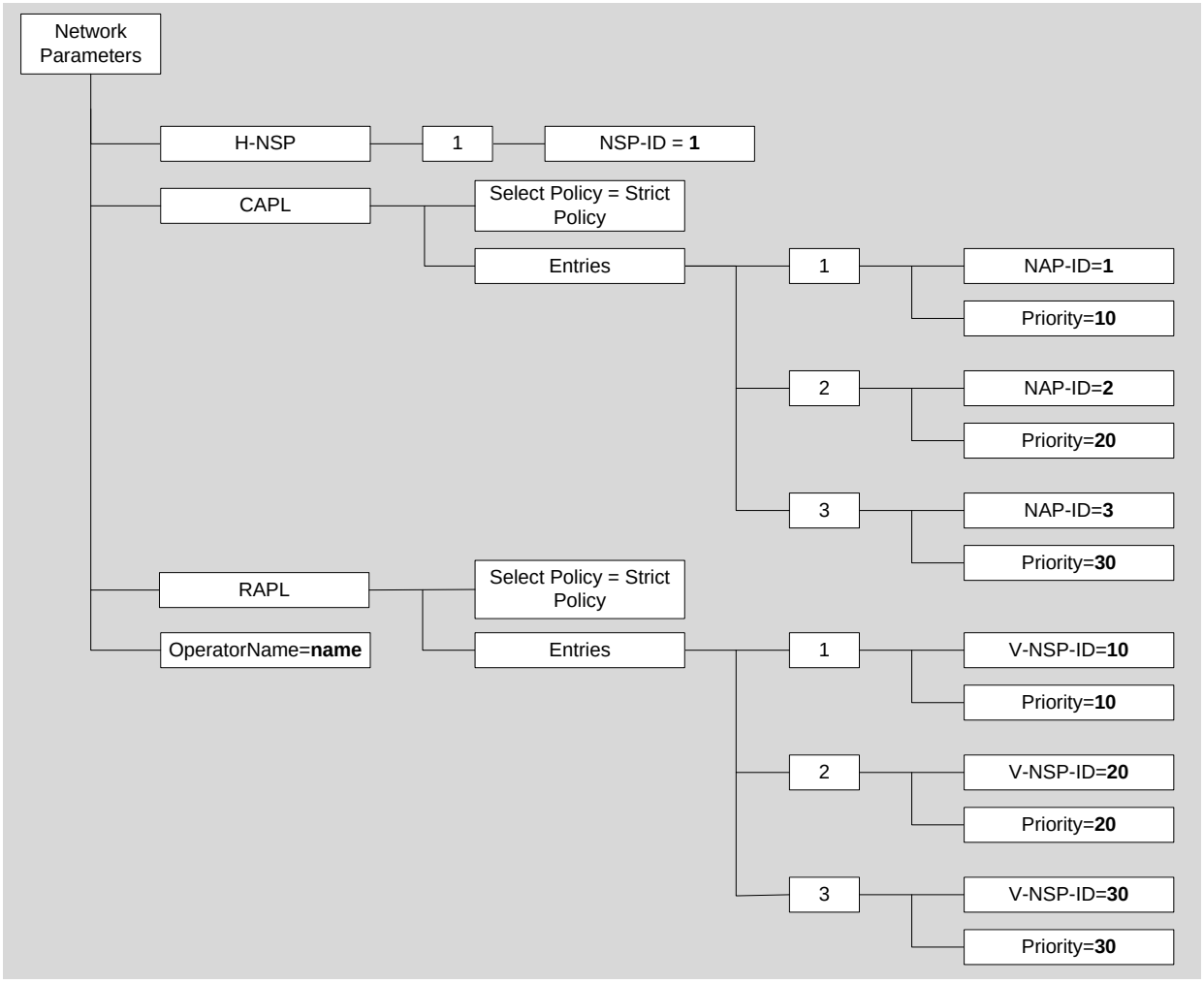


Figure 23 - An example configuration how strict CAPL and RAPL are used with priority

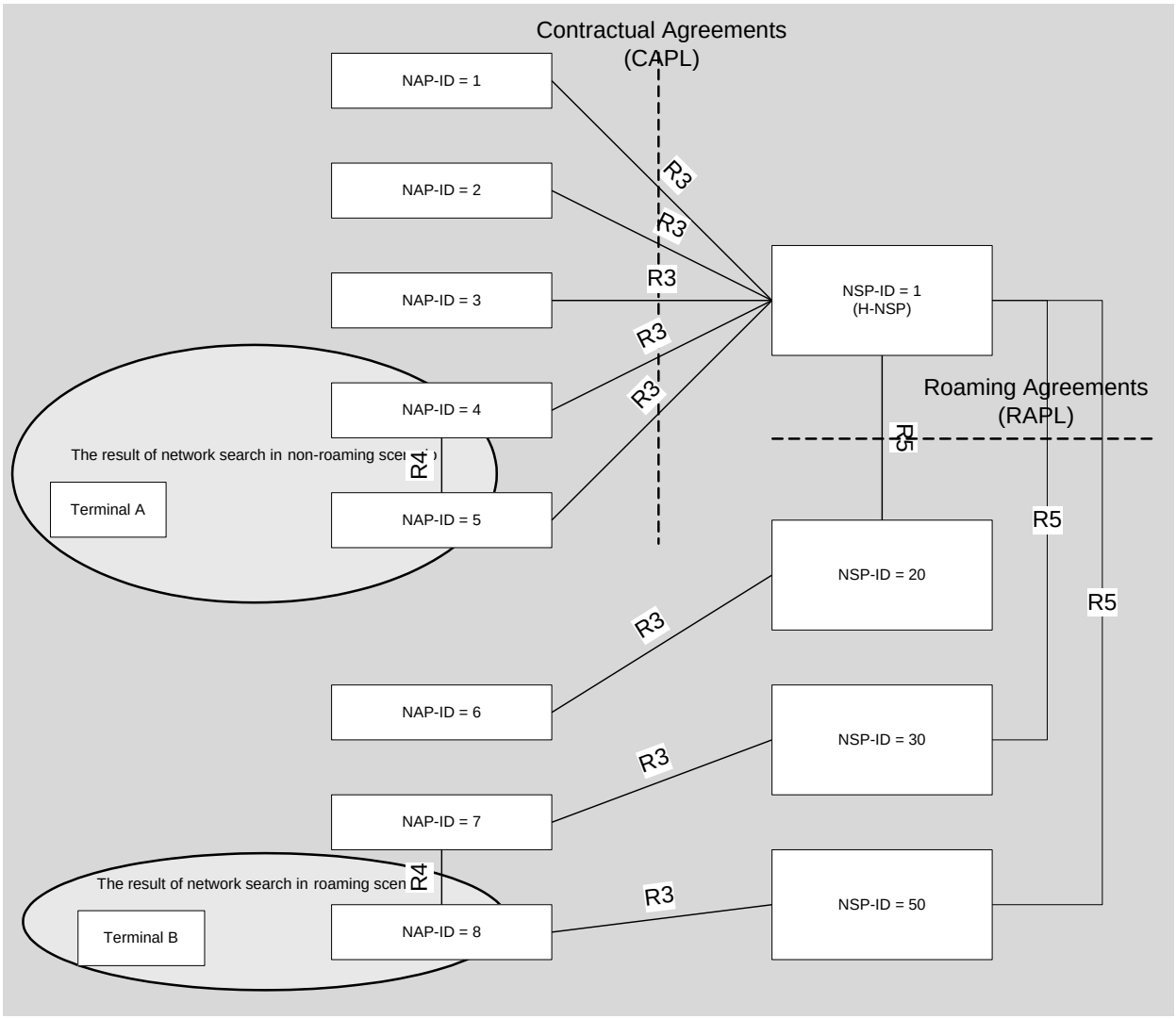


Figure 24 - Network setup

C3.4.1 Non-roaming Scenario with Terminal A:

The result of the network search is

NAP-ID = 4 -> NSP-ID = 1

NAP-ID = 5 -> NSP-ID = 1

The device is not allowed to connect to any of the networks, since the result of the network search did not contain any NAPs, which are listed in CAPL nor have any of the found NAPs, which have direct connection to any of the V-NSPs listed in RAPL.

C3.4.2 Roaming Scenario with Terminal B:

The result of the network search is

NAP-ID = 8 -> NSP-ID = 50 -> NSP-ID = 1

NAPs listed in CAPL are not found and therefore the device resorts to RAPL. The device is not allowed to connect any of the networks, since the result of the network search did not contain any V-NSPs, which are listed in RAPL.

C4 Channel Plan Usage

This section describes how the NAP based and root channel plan is used in network discovery and selection phases.

C4.1 Example: Network Search – Preferred NAPs Found

Figure 25 and Figure 26 illustrate an example of how the NAP selection is carried out when NAP Based Channel Plan or Root Channel Plan or Full Search is used and preferred NAP is found during the search. The configuration forbids the device to roam and to connect using other NAPs, which are not in the CAPL. The channel plan information is used in network search, when the device is not connected to the network, and it does not have any "Prior Connect Info" record. Please note that values in the channel plan are exemplary.

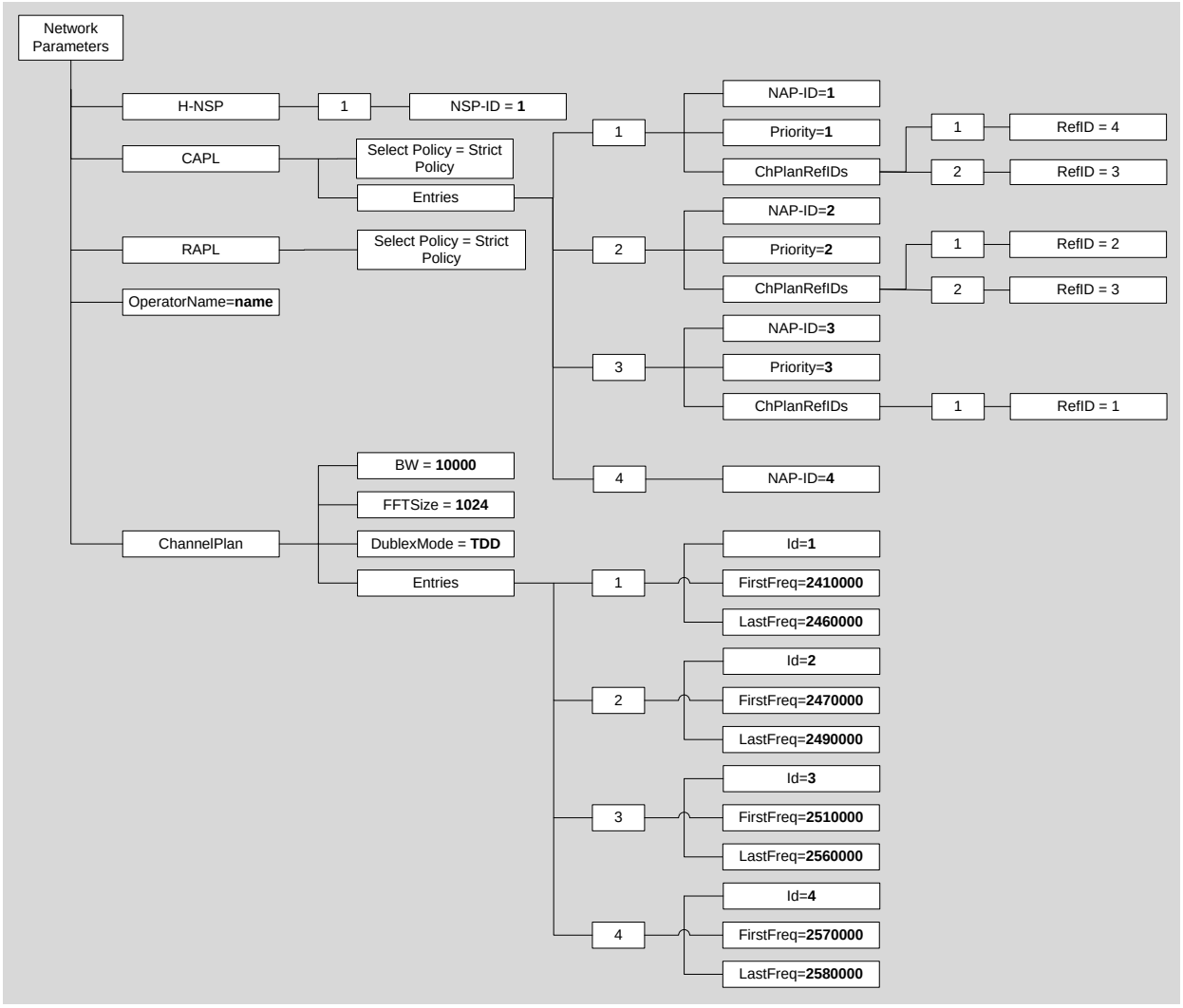


Figure 25 - Example Configuration

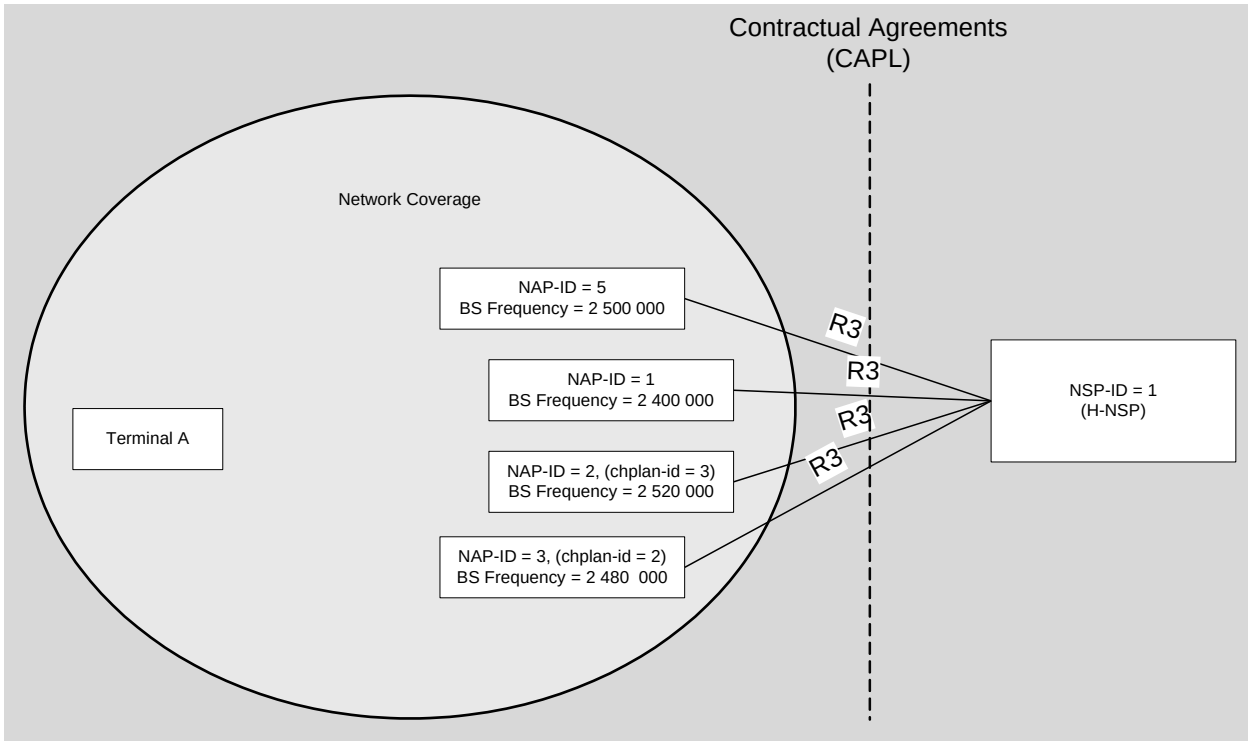


Figure 26 - Network Coverage and Setup

C4.1.1 NAP selection based on NAP Based Channel Plan

Device is allowed to select NAP-ID= 2 even though it is not the most preferred NAP, but it is the highest priority of found NAPs. As NAP-ID=1 is not found from the frequencies of the NAP-ID=1's channel plan entries, the device can ignore the priority of NAP-ID=1.

C4.1.2 NAP selection based on Root Channel Plan

Device is allowed to select NAP-ID= 2 even though it is not the most proferred NAP, but it is the highest priority of found NAPs. As NAP-ID=1 is not found from the frequencies indicated by the Root Channel Plan, the device can ignore the priority of NAP-ID=1.

C4.1.3 NAP selection based on Root Channel Plan, if NAPs in CAPL would not have priorities

The device is allowed to select any of the NAPs from the CAPL. However if the device searches the frequencies in the order given in the Root Channel Plan it first finds NAP-ID=3.

C4.1.4 NAP selection based on full search if channel plan configuration is not provided

Device SHALL select NAP-ID = 1, since it is the most preferred NAP and highest priority of found NAPs.

C4.2 Example: Network Search – Flexible CAPL

Figure 27 and Figure 28 illustrate an example of how the NAP selection is carried out when NAP Based Channel Plan, Root Channel Plan or full network search is used and the NAP Selection Policy in CAPL is set to Partially Flexible Policy or Fully Flexible Policy. The configuration forbids the device to roam. The channel plan information is used in network search, when the device is not connected to the network, and it does not have any "Prior Connect Info" record. Please note that values in the channel plan are exemplary.

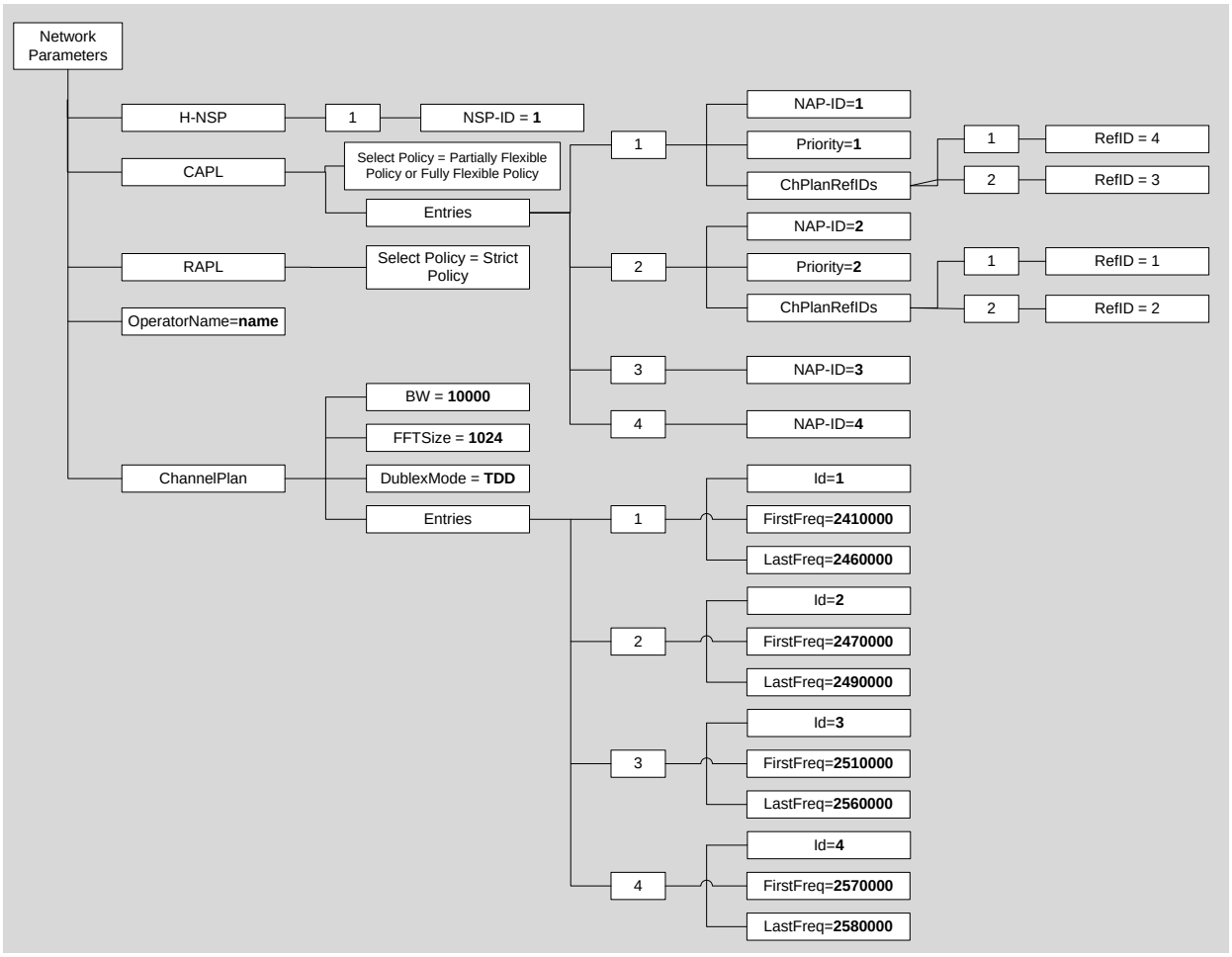


Figure 27 - Example Configuration

C4.2.1 NAPs Not Found From the Channel Plan

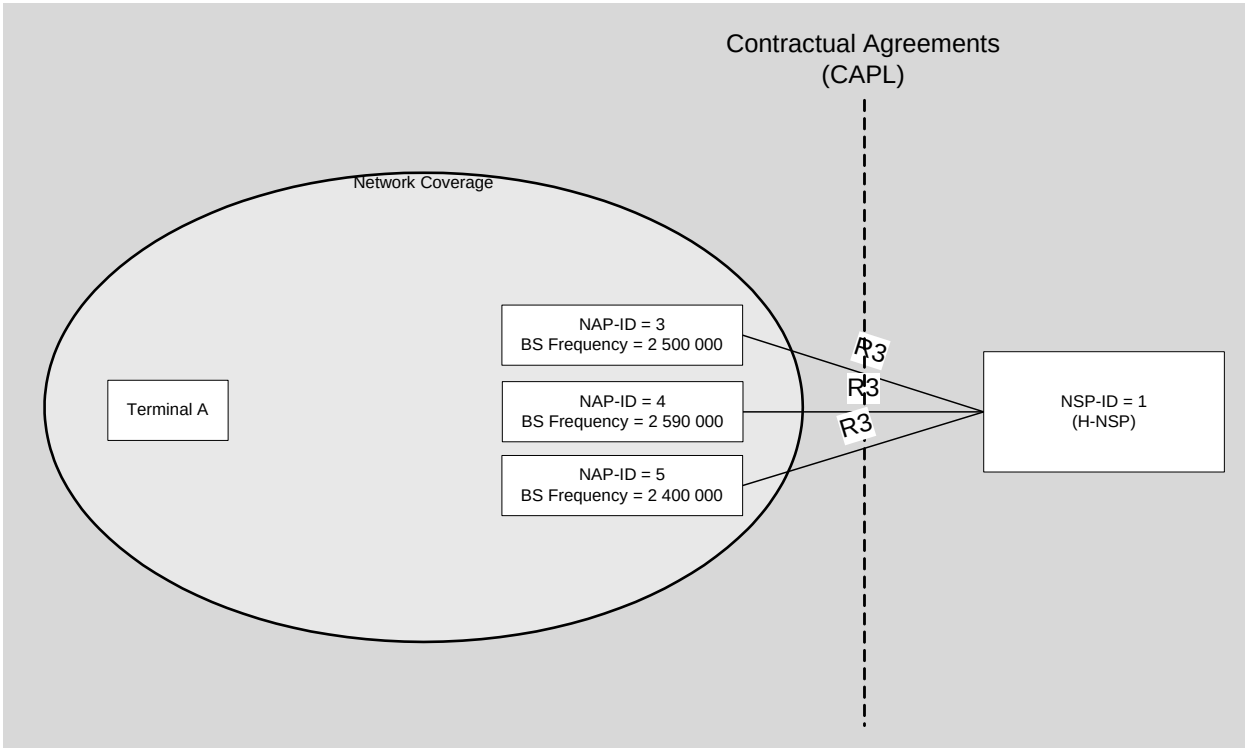


Figure 28 - Network Coverage and Setup

NAP Selection when NAP Selection Policy is set to Partially Flexible Policy

Device is allowed to select either NAP-ID=3 or NAP-ID=4, because NAPs with priority are not found and NAP Selection Policy is set to Partially Flexible Policy which means that the device SHALL respect NAPs in CAPL before selecting other NAP which is connected to the H-NSP. In other words the device is not allowed to select NAP-ID=5. It is implementation specific which one is selected.

NAP selection when NAP Selection Policy is set to Partially Flexible Policy

Device is allowed to select either NAP-ID=3, NAP-ID=4 or NAP-ID=5, because NAPs, which do not have priority, in CAPL are handled with same priority as NAPs which are not in the CAPL. It is implementation specific which one is selected.

ANNEX D. Ensuring Management Authority Control of MOs

To ensure that a MO or specific node cannot be added or altered by an unauthorized management authority (e.g., a rogue service provider), DM provides an ACL mechanism to prevent this from happening.

An ACL is a node property that lists the only management servers allowed to add, replace and/or get the value of the nodes in the data structure.

Exact details on how the ACL property is formatted and how it behaves are included within the OMA DM Tree and Description specification [DMTND].

In addition, ACLs MAY be used by management authorities to lock out whole areas of the DM data structure, to either ensure that SLAs are met, or the device is totally secured from malicious/unsecured management (e.g. such a requirement MAY apply to government-provisioned devices). To accomplish this, it is recommended that these ACLs are provisioned as embedded management operations during the bootstrap via factory provisioning or via the UICC (e.g., in the case of dual mode devices).

1
2
3
4