TECHNICAL REPORT

# TR-196
## Femto Access Point Service Data Model

**Issue: 1 Amendment 1**
**Issue Date: May 2011**

**Notice**

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

This Broadband Forum Technical Report is provided AS IS, WITH ALL FAULTS. ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY:

(A) OF ACCURACY, COMPLETENESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE;
(B) THAT THE CONTENTS OF THIS BROADBAND FORUM TECHNICAL REPORT ARE SUITABLE FOR ANY PURPOSE, EVEN IF THAT PURPOSE IS KNOWN TO THE COPYRIGHT HOLDER;
(C) THAT THE IMPLEMENTATION OF THE CONTENTS OF THE TECHNICAL REPORT WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

By using this Broadband Forum Technical Report, users acknowledge that implementation may require licenses to patents. The Broadband Forum encourages but does not require its members to identify such patents. For a list of declarations made by Broadband Forum member companies, please see http://www.broadband-forum.org. No assurance is given that licenses to patents necessary to implement this Technical Report will be available for license at all or on reasonable and non-discriminatory terms.

ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW (A) ANY LIABILITY (INCLUDING DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES UNDER ANY LEGAL THEORY) ARISING FROM OR RELATED TO THE USE OF OR RELIANCE UPON THIS TECHNICAL REPORT; AND (B) ANY OBLIGATION TO UPDATE OR CORRECT THIS TECHNICAL REPORT.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

  

**Issue History**

| Issue Number | Issue Date | Issue Editor | Changes |
|---|---|---|---|
| Issue 1 | April 2009 | Taka Yoshizawa, Technicolor<br>John Blackford, 2Wire<br>Heather Kirksey, Alcatel-Lucent | Original |
| Issue 1 Amendment 1 | May 2011 | Klaus Wich, Nokia Siemens Networks | Defines FAPService:1.1 with updates to Service Model for 3GPP release 9 and 10. New Theory of operations included. |

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.


| | | |
|---|---|---|
| **Editor** | Klaus Wich | Nokia Siemens Networks |
| **BroadbandHome™ Working Group Chairs** | Greg Bathrick<br>Heather Kirksey | PMC-Sierra<br>Alcatel-Lucent |
| **Vice Chair** | Jason Walls | UNL |
| **Chief Editor** | Michael Hanrahan | Huawei Technologies |
| **Contributors** | Taka Yoshizawa | Technicolor |

**Table of Contents**

**EXECUTIVE SUMMARY ..... 7**

**1 PURPOSE AND SCOPE ..... 9**

1.1 PURPOSE ..... 9
1.2 SCOPE ..... 9

**2 REFERENCES AND TERMINOLOGY ..... 10**

2.1 CONVENTIONS ..... 10
2.2 REFERENCES ..... 11
2.3 DEFINITIONS ..... 12
2.4 ABBREVIATIONS ..... 12

**3 TECHNICAL REPORT IMPACT ..... 14**

3.1 ENERGY EFFICIENCY ..... 14
3.2 IPV6 ..... 14
3.3 SECURITY ..... 14

**4 DATA MODEL DEFINITION ..... 15**

**5 FAPSERVICE PARAMETER DEFINITIONS ..... 17**

**ANNEX A: REQUIRED CPE METHOD IN OPTIONAL RPC MESSAGES ..... 18**

**ANNEX B: VENDOR SPECIFIC TYPE DEFINITIONS ..... 19**

B.1 VENDOR SPECIFIC FILE TYPE ..... 19
B.2 VENDOR SPECIFIC EVENT TYPES ..... 19

**ANNEX C: CONFIGURING THE IPSEC TUNNEL AND QOS ..... 21**

C.1 QUEUING MODEL ..... 21
*C.1.1 Upstream Packet Classification ..... 22*
*C.1.2 Policing ..... 22*
*C.1.3 Queuing and Scheduling ..... 22*
*C.1.4 Tunnel ..... 22*
*C.1.5 Layer3Forwarding ..... 23*
*C.1.6 LocalIPAccess Traffic ..... 23*
C.2 URN DEFINITIONS FOR APP AND FLOW TABLES ..... 24
*C.2.1 ProtocolIdentifier ..... 24*
*C.2.2 FlowType ..... 24*

**APPENDIX I. THEORY OF OPERATION ..... 25**

I.1 INTRODUCTION ..... 25
I.2 MANAGEMENT CONNECTION ESTABLISHMENT ..... 26
I.3 SECGW, FAPGW DISCOVERY AND CONNECTION ESTABLISHMENT ..... 27
I.4 IPSEC TUNNEL STATUS ..... 28
I.5 LOCATION VERIFICATION ..... 29
I.6 SELF-CONFIGURATION ..... 30

  

*I.6.1 General Description* ..... *30*
*I.6.2 General Approach to Self-Configuration* ..... *30*
*I.6.3 General Process Flow* ..... *31*
*I.6.4 Use of "Active Notification"* ..... *31*
*I.6.5 Default Values* ..... *32*
*I.6.6 Discovery of Device Capabilities and Activation of Self-Configuration* ..... *32*
*I.6.7 Deactivation of Self-Configuration* ..... *33*
*I.6.8 Self-Configuration Operation* ..... *34*
I.7 RADIO ENVIRONMENT MEASUREMENT (REM) PROCESS ..... 35
*I.7.1 Execution of REM* ..... *35*
*I.7.2 Configuration of Periodic Measurement* ..... *36*
*I.7.3 Configuration of Selective Measurement* ..... *36*
*I.7.4 Storage and Retrieval the Measurement Result* ..... *37*
I.8 NEIGHBOR LIST CONFIGURATION ..... 38
*I.8.1 Fixed-configuration* ..... *38*
*I.8.2 Self-configuration* ..... *39*
I.9 STATE MANAGEMENT ..... 40
I.10 FAULT MANAGEMENT ..... 41
*I.10.1 Introduction* ..... *41*
*I.10.2 Expedited Event* ..... *44*
*I.10.3 Queued Event* ..... *44*
*I.10.4 Logged Event* ..... *45*

  

## List of Figures

Figure 1 – General Overall View of the Femtocell System ..... 15
Figure 2 – Services.FAPServices.{i}. Structure ..... 16
Figure 3 – Queuing Model for an Internet Gateway Device Supporting FAPService ..... 22
Figure 4 – FAP to ACS connections ..... 26
Figure 5 – SecGW, FAPGW connection establishment ..... 27
Figure 6 – Location information ..... 29
Figure 7 – General process flow of self-configuration ..... 31
Figure 8 – Discovery of device capabilities and activation of self-configuration ..... 33
Figure 9 – Deactivation of self-configuration ..... 33
Figure 10 – Self-configuration operation – object relationship ..... 34
Figure 11 – REM Periodic Configuration ..... 36
Figure 12 – REM Selective Measurement Configuration ..... 36
Figure 13 – Retrieval of REM Result ..... 37
Figure 14 – Neighbor List – Fixed-configuration ..... 38
Figure 15 – State Management ..... 40
Figure 16 – Expedited Event Handling ..... 44
Figure 17 – Queued Event Handling ..... 45
Figure 18 – Logged Event Handling ..... 45

## List of Tables

Table 1 – FAPService Data Model Versions ..... 17
Table 2 – Vendor Specific Event Types ..... 20
Table 3 – IPSec Tunnel selection Decision ..... 27
Table 4 – IKE SA Status ..... 28
Table 5 – Example Parameters for Active Notification ..... 32
Table 6 – *ScanStatus* Definition ..... 37
Table 7 – *MustInclude* Definition ..... 40
Table 8 – SM parameter Definition ..... 41
Table 9 – FM Object Definition ..... 41
Table 10 – FM Object Usage ..... 43

  

**Executive Summary**

TR-196 defines the service data model for the Femto Access Point Service. Femto Access Point (FAP), or "Femtocell" in general, is a terminology for a new type of CPE device emerging in the mobile industry. In other words, it is a small-scale cellular base station designed specifically for indoor coverage. As such, it communicates to the user's mobile handset over the standard-based radio interface using licensed spectrum and further connects to the mobile network infrastructure over the fixed broadband connection.

There are two types of FAP devices: 1) standalone and 2) integrated. The standalone FAP is a device that is connected to a physically separate RGW via an Ethernet cable, while the integrated FAP is a device that has FAP and RGW functionalities combined into a single CPE device.

The notable benefits of Femtocell include the followings:

- Improved in-building signal coverage and quality
- Offloading the macro base stations from indoor users
- Introduction of 3G coverage and service to users irrespective of the presence or absence of the 3G macrocell coverage in the surrounding area
- Enables the introduction of traffic-intensive services that require high data rate
- Enables the introduction of new "Femtozone" applications and services

There are several main characteristics that the Femtocell separates itself from the traditional cellular network infrastructure as follows:

1. It is a consumer CPE device that is located at the end-user's premise.
2. The intended coverage and the capacity are orders of magnitude smaller than the traditional macrocells.
3. The number of devices deployed and to be managed is orders of magnitude higher than the traditional macrocell based system.
4. It uses the existing fixed broadband technology, such as xDSL, as the backhaul to the mobile network.

It is important to note that the above characteristics further present the following implications from an Operation and Management perspective:

1. The physical control of the device itself is outside the control of the mobile operator that provides the service. This includes aspects such as the physical state and condition of the device itself, and the location of the device where it may be installed and operated.
2. Since the number of devices to manage is order of magnitude higher than the traditional macrocells, different approach of device management may be required.
3. Maintaining the same level of Quality of Service and Grade of Service with the traditional macrocell based system present challenges to the mobile operators due to the fact that the tight control of the device is neither necessarily guaranteed nor possible. Some of the constraints include the general nature of the existing fixed broadband technology (e.g. xDSL), and the general characteristics of the CPE device (e.g. absence

  

of HW/SW support of redundancy and the concept of availability). This impacts the area such as real-time device operation, management and service availability.

4. From the perspective of mobile operators who provide the FAP service to end users, support and consideration for the multi-vendor interoperable consumer CPE product paradigm is an important aspect that needs to be taken into account for the successful FAP service deployment and acceptance in the market. This includes the needs for inter-operability across multiple vendor products.

The characteristics of the Femtocell service described above illustrates that the management of FAP requires a fundamentally different management approach from the traditional cellular infrastructure network elements. As the remote management protocol specifically designed for consumer CPE devices, TR-069 CWMP naturally fit the FAP remote management.

Further, FAP management based on the standardized Data Model ensures interoperability across multiple vendors. This means:

- From mobile operator perspective, it ensures easier and smoother operations, administration, maintenance and provisioning (OAM&P) by reusing the technology that is already proven in the mass CPE deployment today.
- From vendor perspective, it encourages and promotes the ecosystem across the whole femto industry, and
- From the end user perspective, it allows simple and error-free "plug-and-play" installation.

  

# 1 Purpose and Scope

## 1.1 Purpose

The purpose of this Technical Report is to specify the Data Model for the Femto Access Point (FAP) for remote management purposes using the TR-069 CWMP within the scope defined in the following section.

This Technical Report defines FAPService as the container associated with the remote management of objects for FAP devices. CPE devices making use of a FAPService object MUST adhere to all of the data-hierarchy requirements defined in TR-106 [4]. In the context of TR-106 [4], the FAPService object is a service object.

## 1.2 Scope

The scope of this FAP Data Model is UMTS FDD Home NodeB (i.e. "3G HNB"). However, the structure and organization of the Data Model takes it into consideration in such a way that it can be extended to cover other type(s) of FAP device based on other radio interface technologies, if such a need arises in the future.

In the preceding summary section, two types of FAP devices are described (i.e. standalone and integrated). Both types of devices are anticipated in the market, and both types of devices are expected to use a TR-098 [2] or TR-181 Issue 2 [3] based device.

  

# 2 References and Terminology

## 2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [8].

| | |
|---|---|
| **MUST** | This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification. |
| **MUST NOT** | This phrase means that the definition is an absolute prohibition of the specification. |
| **SHOULD** | This word, or the adjective “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course. |
| **SHOULD NOT** | This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label. |
| **MAY** | This word, or the adjective “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option. |

  

## 2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.
A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

| DOCUMENT | TITLE | SOURCE | YEAR |
|---|---|---|---|
| [1] TR-069 AMENDMENT 3 | *CPE WAN MANAGEMENT PROTOCOL* | Broadband Forum | 2010 |
| [2] TR-098 AMENDMENT 2 | *INTERNET GATEWAY DEVICE DATA MODEL FOR TR-069* | Broadband Forum | 2008 |
| [3] TR-181 ISSUE 2 | *DEVICE DATA MODEL FOR TR-069 (DEVICE:2)* | Broadband Forum | 2010 |
| [4] TR-106 AMENDMENT 5 | *DATA MODEL TEMPLATE FOR TR-069-ENABLED DEVICES* | Broadband Forum | 2010 |
| [5] TS 29.060 | *GENERAL PACKET RADIO SERVICE (GPRS); GPRS TUNNELLING PROTOCOL (GTP) ACROSS THE GN AND GP INTERFACE* | 3GPP | 2011 |
| [6] TS 32.584 | *TELECOMMUNICATIONS MANAGEMENT; HOME NODE B (HNB) OPERATIONS, ADMINISTRATION, MAINTENANCE AND PROVISIONING (OAM&P); XML DEFINITIONS FOR TYPE 1 INTERFACE HNB TO HNB MANAGEMENT SYSTEM (HMS) TELE-COMMUNICATIONS MANAGEMENT; HOME NODE B (HNB) OPERATIONS, ADMINISTRATION, MAINTENANCE AND PROVISIONING (OAM&P); XML DEFINITIONS FOR TYPE 1 INTERFACE HNB TO HNB MANAGEMENT SYSTEM (HMS)* | 3GPP | 2011 |
| [7] TS33.102 | *TECHNICAL SPECIFICATION GROUP SERVICES AND SYSTEM ASPECTS; 3G SECURITY; SECURITY ARCHITECTURE* | 3GPP | 2010 |

| | | | | |
|---|---|---|---|---|
| [8] | RFC 2119 | *KEY WORDS FOR USE IN RFCS TO INDICATE REQUIREMENT LEVELS* | IETF | 1997 |
| [9] | RFC 1305 | *NETWORK TIME PROTOCOL (VERSION 3) SPECIFICATION, IMPLEMENTATION AND ANALYSIS* | IETF | 1992 |
| [10] | RFC 2960 | *STREAM CONTROL TRANSMISSION PROTOCOL* | IETF | 2000 |
| [11] | RFC 3550 | *RTP: A TRANSPORT PROTOCOL FOR REAL-TIME APPLICATIONS* | IETF | 2003 |
| [12] | IEEE-1588 | *STANDARDS FOR A PRECISION CLOCK SYNCHRONIZATION PROTOCOL FOR NETWORKED MEASUREMENT AND CONTROL SYSTEMS,* | IEEE | 2003 |

## 2.3 Definitions

The following terminology is used throughout this Technical Report.

**ACS** Auto-Configuration Server. This is a component in the broadband network responsible for auto-configuration of the CPE for advanced services.

## 2.4 Abbreviations

This Technical Report uses the following abbreviations:

| | |
|---|---|
| 3G | 3rd Generation |
| 3GPP | 3rd Generation Partnership Project |
| ADSL | Asynchronous DSL |
| CM | Configuration Management |
| CN | Core Network |
| CPE | Customer Premises Equipment |
| CWMP | CPE WAN Management Protocol |
| DL | Downlink |
| DSL | Digital Subscriber Line |
| DSCP | DiffServ Code Point |
| FAP | Femto Access Point |
| FAP-GW | FAP Gateway |
| FDD | Frequency Division Duplex |
| FM | Fault Management |

  

| | |
|---|---|
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| GSM | Global System for Mobile |
| GTP-U | GPRS Tunneling Protocol – User Data |
| HNB | Home NodeB |
| IEEE | Institute of Electrical and Electronics Engineers |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPsec | IP security |
| LAC | Location Area Code |
| LAN | Local Area Network |
| NL | Neighbor List |
| NTP | Network Time Protocol |
| O&M | Operation & Maintenance |
| OAM&P | Operation Administration, Maintenance & Provisioning |
| OUI | Organizationally Unique Identifier |
| PCPICH | Primary Common Pilot Channel |
| PLMN | Public Land Mobile Network |
| PPP | Point to Point Protocol |
| PPPoE | PPP over Ethernet |
| QoS | Quality of Service |
| RAC | Routing Area Code |
| REM | Radio Environment Measurement |
| RF | Radio Frequency |
| RFC | Request for Proposal (IETF Document) |
| RFTx | RF transmitter |
| RGW | Residential Gateway |
| RPC | Remote Procedure Call |
| RTP | Real Time Protocol |
| SA | Security Association |
| SCTP | Stream Control Transmission Protocol |
| SecGW | Security Gateway |
| TLS | Transport Layer Security |
| TR | Technical Report |
| UARFCN | UMTS Absolute Radio Frequency Channel Number |
| UE | User Equipment |
| UL | Uplink |
| UMTS | Universal Mobile Telecommunication System |
| URN | Uniform Resource Name |
| xDSL | any kind of DSL (ADSL, VDSL, …) |
| WAN | Wide Area Network |
| WCDMA | Wideband Code Division Multiple Access |
| WG | Working Group |

  

# 3 Technical Report Impact

## 3.1 Energy Efficiency

TR-196 has no impact on Energy Efficiency.

## 3.2 IPv6

TR-196 does not specifically address IPv6, but is intended to support IPv6 addresses as well as IPv4. Enhancements may be required in the future to accommodate full IPv6-based Femtocell service.

## 3.3 Security

The FAP service will be based on the underlying security mechanism between the FAP and the SecGW in the mobile operator's network. The exact description and specification of the security mechanism is found in the 3GPP specification TS33.102 [7] under SA WG3.

  

# 4 Data Model Definition

Figure 1 below shows the general overall view of the Femtocell system. Both standalone and integrated FAP product types are shown.

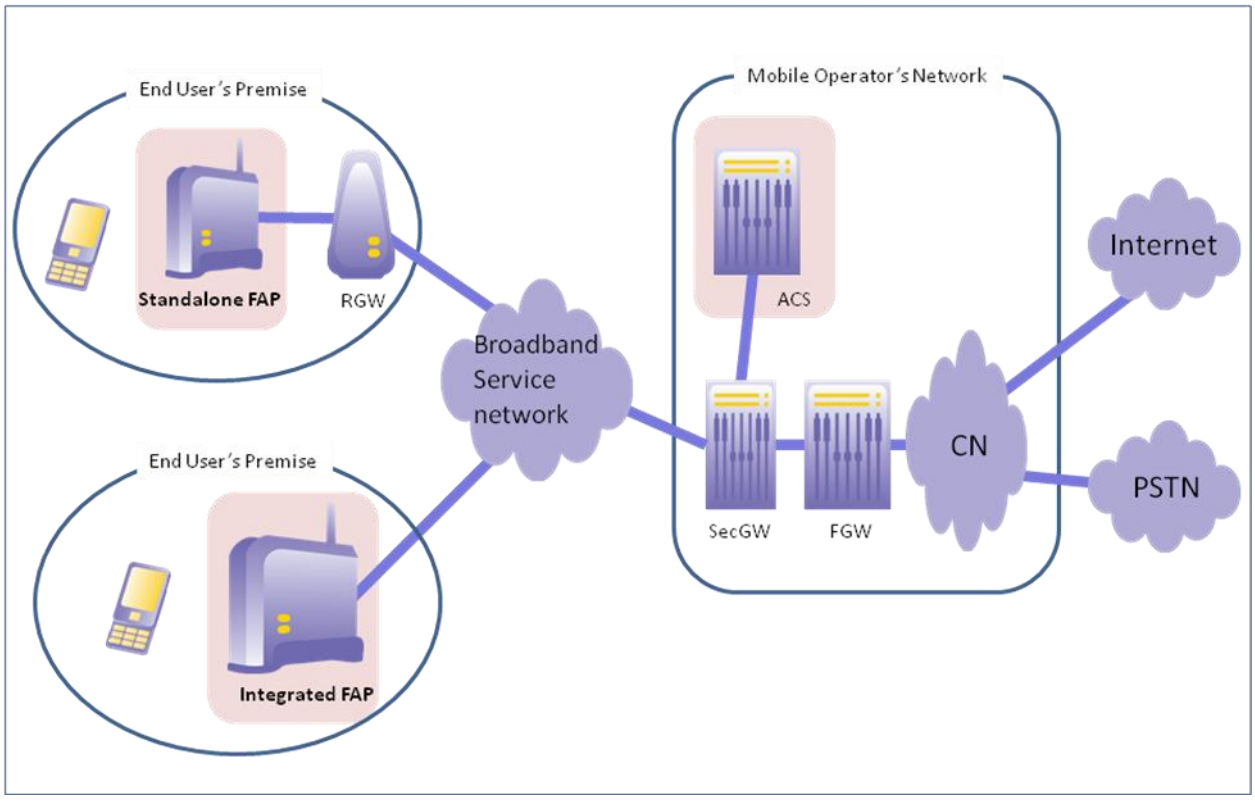


**Figure 1 – General Overall View of the Femtocell System**

Figure 2 below illustrates the internal structure of the FAPService object.

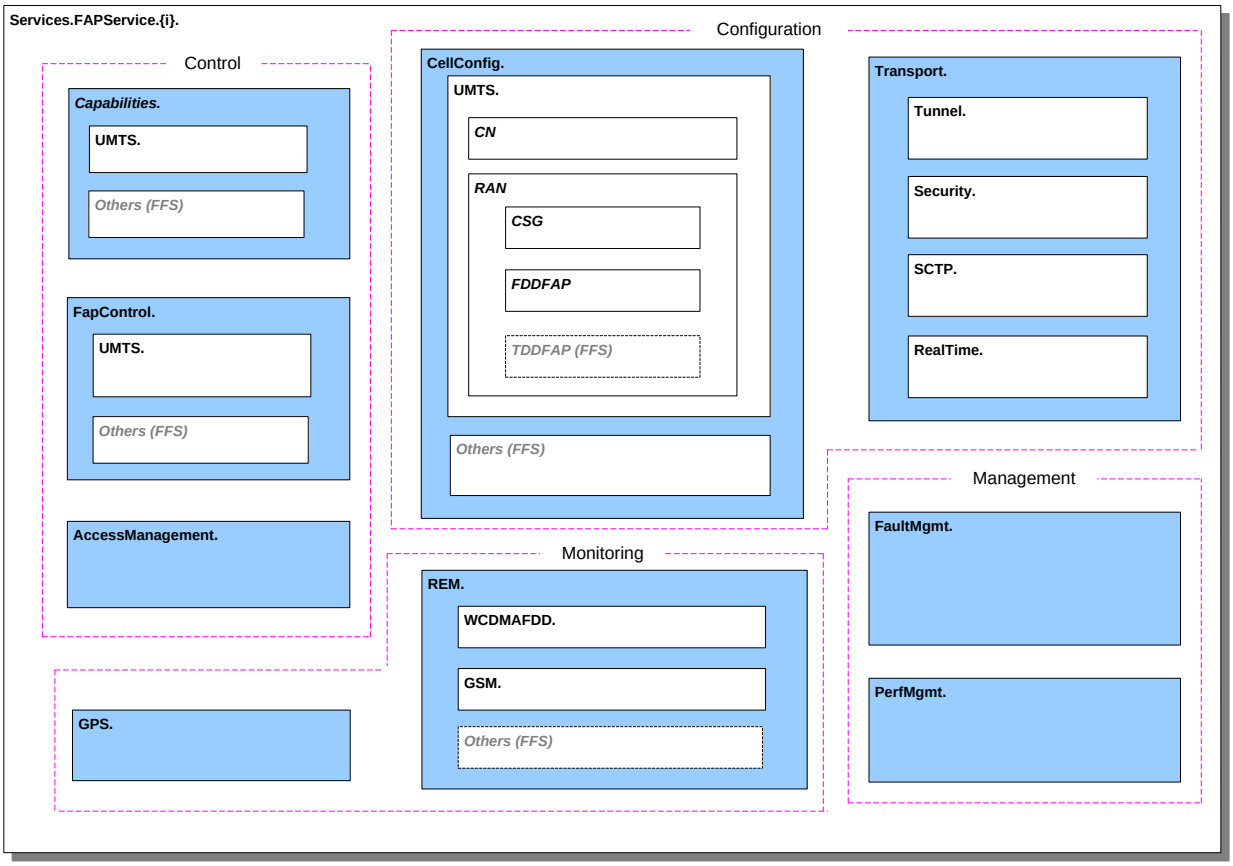


**Figure 2 – Services.FAPServices.{i}. Structure**

# 5 FAPService Parameter Definitions

The normative definition of the FAPService data model is split between several DM Instance documents (see TR-106 [4]). Table 1 lists the data model versions and DM Instances that had been defined at the time of writing. It also indicates the corresponding Technical Reports and gives links to the associated XML and HTML files.

Note that, because new minor versions of the FAPService data model can be defined without re-publishing this Technical Report, the table is not necessarily up-to-date. An up-to-date version of the table can always be found at http://www.broadband-forum.org/cwmp.

**Table 1 – FAPService Data Model Versions**

| Version | DM Instance | Technical Report | XML and HTML[1] |
|---|---|---|---|
| 1.0 | tr-196-1-0.xml | TR-196 | http://broadband-forum.org/cwmp/tr-196-1-0.xml |
| | | | http://broadband-forum.org/cwmp/tr-196-1-0.html |
| 1.1 | tr-196-1-1.xml | TR-196 Amendment 1 | http://broadband-forum.org/cwmp/tr-196-1-1.xml |
| | | | http://broadband-forum.org/cwmp/tr-196-1-1.html |
| | | | http://broadband-forum.org/cwmp/tr-196-1-1-last.html |

Note:

*"The LIPA definition in this version of TR-196, on which this FAPService.AccessManagement.LocalIPAccess object is based, may differ from 3GPP's definition. The implementation and use of the present version's LIPA object may introduce interworking problem when a future data model version incorporates 3GPP's LIPA definition."*

1 The HTML with a name of the form tr-xxx-i-a.html, e.g. tr-196-1-0.html, lists the entire service model. The HTML with a name of the form tr-xxx-i-a-last.html, e.g. tr-196-1-1-last.html, lists only the changes to the service model since the previous version.

  

# Annex A: Required CPE Method in Optional RPC Messages

Section A.4.1/TR-069 [1] describes the optional CPE Methods in RPC messages. By definition, they are optional for individual CPE vendors. However, among them, at least one of them is required for the FAP operation. Therefore, all FAP vendors MUST support the following optional CPE method RPC message:

- Upload

  

# Annex B: Vendor Specific Type Definitions

## B.1 Vendor Specific File Type

The following vendor specific file type is defined for this version of the FAP data model. All FAP vendors that comply with this specification MUST support this file type to be used in the Upload CPE method.

- "X 00256D 3GPP Performance File"

The format is based on the vendor specific file type extension per Section A.4.1.5/TR-069 [1]. By appending "3GPP" in the beginning of the vendor-specific identifier field, it uniquely identifies the file types to be specific for the 3GPP specification per TS 32.584 [6]. The <OUI> field is replaced with the Broadband Forum OUI value of 00256D.

## B.2 Vendor Specific Event Types

Event Type indicates the reason why CPE establishes the TR-069 session with ACS, and is included in the Inform RPC method sent by the CPE. Section 3.7.1.5, Table 7 in TR-069 [1] defines the Event Types. However, some FAP specific scenarios represent a situation where FAP needs to establish a TR-069 session with the ACS due to a reason not covered by the existing Event Types. Because it is most likely inappropriate to re-use any of the existing Event Type for the purpose other than the intended one, two new Event Types are defined specific for TR-196.

The FAP MUST use these newly defined event types in an Inform RPC method when it establishes the TR-069 session with the ACS after one of the following conditions occurred and request for re-provisioning:

1) FAP failed to establish the secure tunnel connection with all of the SecGWs previously provided by the ACS, or

2) FAP failed to establish the Iuh connection with all of the FAP-GWs previously provided by the ACS.

This version of the FAP data model defines the following vendor specific event types. All FAP vendors that comply with this specification MUST support these event types if in the Inform ACS method.

This format is based on the vendor specific event type per Table 7 in TR-069 [1] By appending "3GPP" in the beginning of the vendor-specific identifier field, it uniquely identifies the event to

  

be specific for the 3GPP specification. The <OUI> field is filled with the Broadband Forum OUI value of 00256D.

**Table 2 – Vendor Specific Event Types**

| Event Code | Cumulative Behavior | Explanation | ACS Response for Successful Delivery | Retry/Discard Policy |
|---|---|---|---|---|
| "X 00256D 3GPP Reprovision Required: SecGW" | Single | Indicates that the FAP failed to establish the secure tunnel connection with all of the SecGWs previously provided by the ACS | InformResponse | The CPE MUST NOT ever discard (except on BOOTSTRAP) an undelivered X 00256D 3GPP Reprovision Required: SecGW event. (except on BOOTSTRAP |
| "X 00256D 3GPP Reprovision Required: FAPGW" | Single | Indicates that the FAP failed to establish the Iuh connection with all of the FAP-GWs previously provided by the ACS | InformResponse | The CPE MUST NOT ever discard an undelivered X 00256D 3GPP Reprovision Required: FAPGW event. (except on BOOTSTRAP) |

  

# Annex C: Configuring the IPsec Tunnel and QoS

## C.1 Queuing Model

Figure 3 shows the queuing and bridging model for a CPE supporting the FAPService as defined in this Technical Report. The FAPService utilizes the QueueManagement and Layer3Forwarding framework as defined in the root data model (TR-098 [2] or TR-181 [3]) in order to apply QoS differentiation to packets before and after applying IPsec encapsulation.

The elements of this model are described in the following sections.

Note:

*The queuing model described in this Annex is intended only to clarify the behavior of the related data objects. There is no suggestion that an implementation need be structured to conform to this model.*

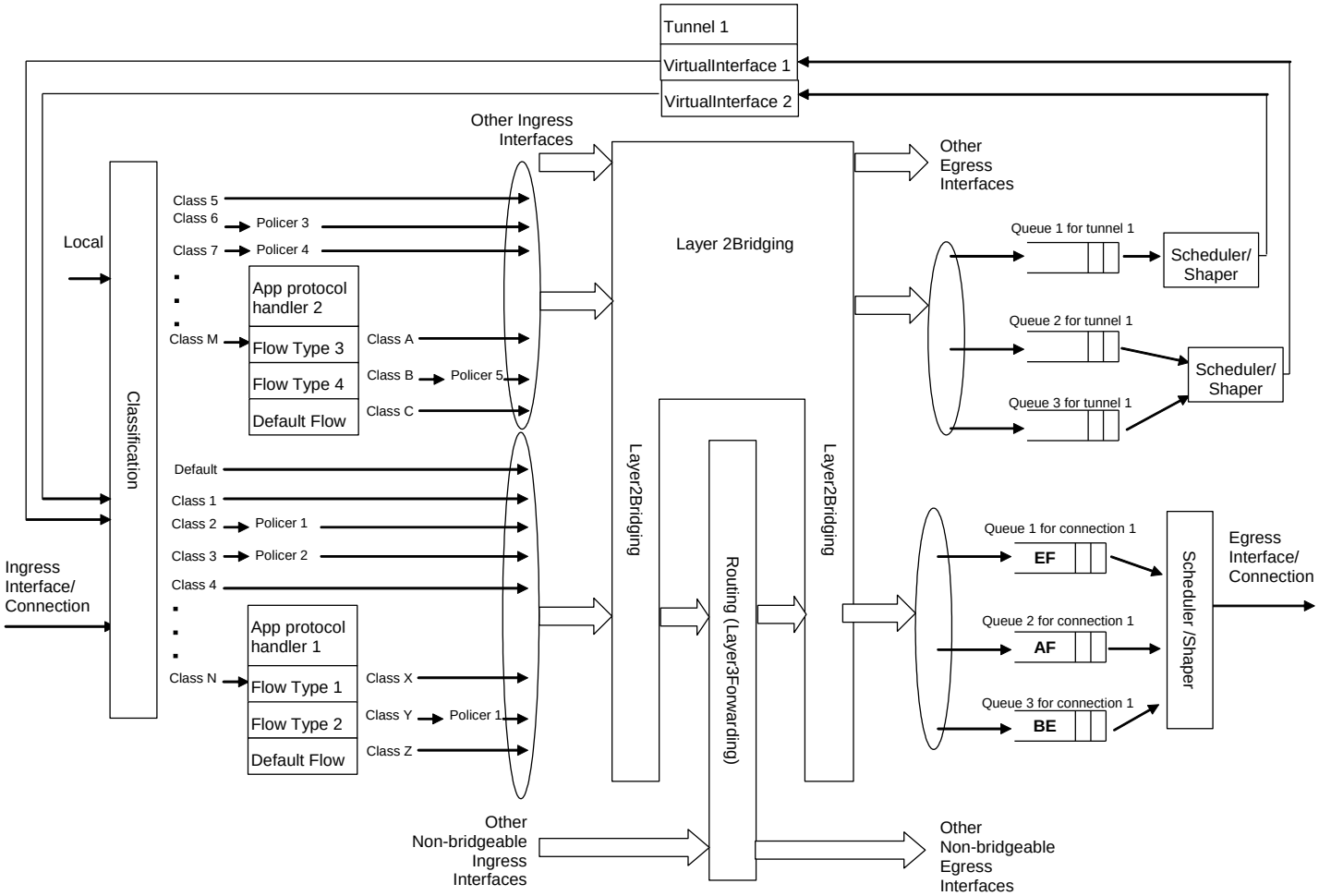


  

**Figure 3 – Queuing Model for an Internet Gateway Device Supporting FAPService**

### C.1.1 Upstream Packet Classification

There is a single classifier object that is used both before and after packets are sent to the VirtualInterface object that represents the IPsec tunnel(s). (As can be seen in the Figure, packets can be viewed as passing twice through the entire QoS management framework.)

The QueueManagement Classification, App and Flow tables are used to select different classes of traffic. For example, UMTS conversational and streaming traffic can be associated with one or two QueueManagement.Queue instances and other UMTS QoS classes can be associated with a 3rd Queue. Classification outcome alternatives are identical to the root data model.

Since the CPE might have LAN interfaces that receive additional traffic, the VirtualInterface can be associated with a 2nd layer of Queues so that the IPsec traffic receives the appropriate QoS with respect to other application traffic. It is also possible to direct all the IPsec packets through a PPPoE interface.

### C.1.2 Policing

Policing is configured as defined in the used root data model. Policing can be performed on FAPService packets both before and after IPsec tunneling.

### C.1.3 Queuing and Scheduling

Queuing and scheduling is configured as for the used root data model, except that a VirtualInterface instance can be used as an egress interface.

In the upstream direction, FAPService packets can first be queued and scheduled before IPsec tunneling. A different set of queues and schedulers can be employed for the packets after they have received the tunneling IP header.

### C.1.4 Tunnel

The policies governing establishment of the IPsec tunnel are provisioned in the Security.CryptoProfile and Security.Secret objects. The CryptoProfile determines which ciphering and hashing algorithms are employed for the tunnel. Each CryptoProfile instance defines a separate tunnel (IKE instance). The Secret objects define credentials to be used to authenticate the tunnel setup. The VirtualInterface object is employed as an egress interface for Queue objects (one or more queues may be associated with a VirtualInterface instance) and ingress interface for Classification objects (encrypted packets can be reclassified to differentiate QoS treatment from packets arriving over LAN interfaces).

  

The IKESA and ChildSA objects provide information about currently established tunnels. This information is not retained beyond the lifetime of the tunnel.

In order to set up tunnel objects, one first configures a Secret or Pkey object. Thereafter one or several CryptoProfile instances are defined (typically one) and associated with an authentication scheme (Pkey and/or Secret) using the AuthMethod parameter. Thereafter one or several VirtualInterface instances are created and associated with a CryptoProfile instance. In order to create two ChildSA pairs with different outer DSCP marking, two VirtualInterface instances are created, both are associated with the same CryptoProfile instance and the MaxChildSA parameter is set to at least 4. (If the MaxChildSA parameter is set equal to 2, there will instead be separate IKE sessions for each VirtualInterface.) DSCP marking policy can be configured for the outside IPsec tunnel header.

The association of a Queue object with a VirtualInterface instance creates a packet processing association for the WAN-facing direction. The device automatically creates the corresponding Layer3Forwarding rule for the reverse direction.

The current version of the data model is intended to support tunneling of traffic to/from the local interface. Support for a more generalized use of the Tunnel object to allow tunneling of traffic to/from LAN interfaces may be added in a future update to the model.

### C.1.5 Layer3Forwarding

Layer3Forwarding is envisioned to be configured on the upstream side of the tunnel object. Implementations and those configuring devices should be careful to avoid associating the Layer3Forwarding object with traffic both before and after the IPsec tunnel, as this could allow undesired packets to traverse the tunnel.

### C.1.6 LocalIPAccess Traffic

This version of the data model uses the FAPService.AccessManagement.LocalIPAccess object to perform local IP breakout to LAN or WAN (depending on destination address). LocalIPAccess packets destined towards local LAN or WAN are extracted from the Iuh packet flow before they hit the QueueManagement Classification object. Similarly, LocalIPAccess return traffic is inserted into the flow such that it never passes through the Classification or Queue objects. The LocalIPAccess packets are inserted into the default queue for egress LAN or WAN interfaces. There is no explicit support in the current data model for configuring QoS or routing for LocalIPAcess packets.

  

## C.2 URN Definitions for App and Flow Tables

The root data models (TR-098 [2], TR-181 [3]) define a set of URNs for the App and Flow tables in the QueueManagement mechanism. An additional set of URNs have been defined to associate traffic arriving over the FAP air interface with the QueueManagement.Classification.{i} object.

### C.2.1 ProtocolIdentifier

The root data models (TR-098 [2], TR-181 [3]) define a set of URNs for the ProtocolIdentifier parameter in the App table of the QueueManagement service. The following set of URNs are additional values that are applicable to the FAPService object.

| URN | Description |
|---|---|
| urn:broadband-forum-org:iuh.control | SCTP as defined in RFC2960 [10] |
| urn.broadband-forum-org:gtp | GTP protocol as defined in 3GPP TS 29.060 [5] |
| urn:broadband-forum-org:iuh.rtp | RTP as defined in RFC3550 [11] or multiplexed RTP |
| urn:broadband-forum-org:time | Network Time Protocol (NTP) as defined in RFC1305 [9] or IEEE1588 Precision Time Protocol (PTP) [12] |

### C.2.2 FlowType

A URN for the FlowType parameter in the Flow table of the QueueManagement service for the GTP protocol as defined in 3GPP TS29.060 [5] is formed as follows:

> For the ProtocolIdentifier urn:broadband-forum-org:gtp, the following QoS-related flow types are defined:
>
> ```
> urn:broadband-forum-org:gtp-conversational
> urn:broadband-forum-org:gtp-streaming
> urn:broadband-forum-org:gtp-interactive
> urn:broadband-forum-org:gtp-besteffort
> ```

  

# Appendix I. Theory of Operation

## I.1 Introduction

This informative appendix describes the "theory of operation" of TR-196 data model. This explains the intended usage of the objects and parameters to achieve the desired operation on the FAP. Note that the actual implementation are influenced by factors external to the TR-069 or TR-196 data model itself – such as operator policy, vendor implementation decision, variations of FAP products, etc. Therefore, variations of implementations will exist and there is no single right answer to accomplish the desired end-goal (i.e. self-configuration). However, objects and parameters in TR-196 are complex enough to warrant some explanations of the intended usage. Under this circumstance, this appendix illustrates, as a guideline, the intended usage of objects and parameters in TR-196 to achieve such goals. It is certainly possible for a FAP vendor to invent and implement mechanisms beyond the existing objects and parameters in TR-196. However, this is outside the scope of this appendix.

Note 1:

*In all of the figures in this appendix, arrows pointing to the ACS indicate the "get" action (GetParameterValues) and arrows pointing away from the ACS indicate the "set" action (SetParameterValues) by the ACS.*

Note 2:

*This theory of operation is based on the data model for UMTS (3G) Femto cells. For other radio protocols the theory has to be adapted.*

Note 3:

*If not specified otherwise, all objects names starting with a dot are relative to the "<rootobject>.Services" object. In all other cases the whole path is specified.*

  

## I.2 Management Connection Establishment

There are two possible scenarios how an UMTS FAP establishes a TR-069 CWMP session with the ACS:

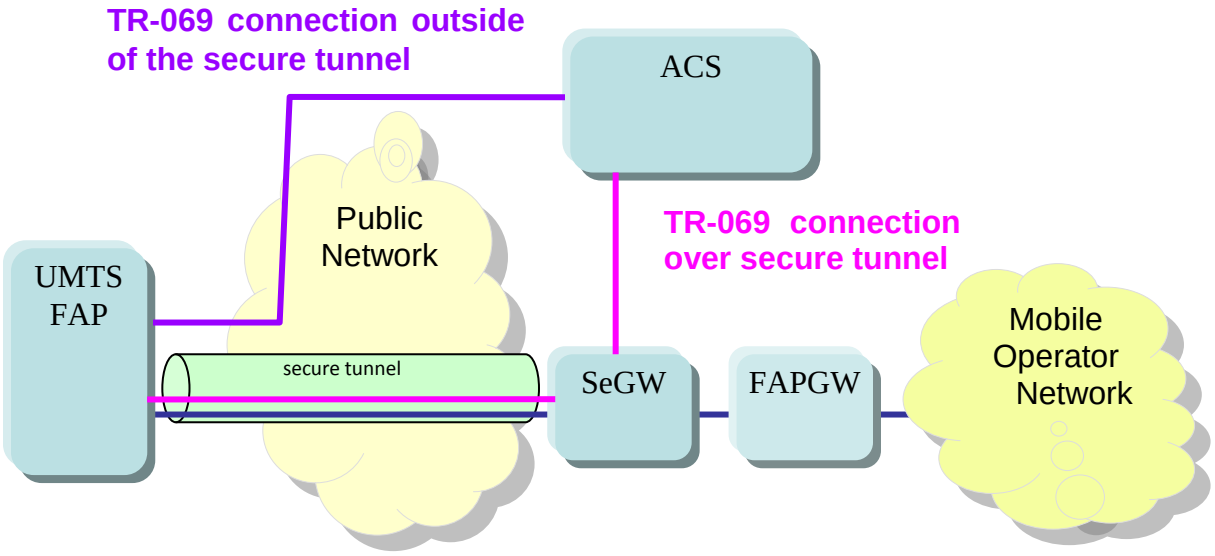


**Figure 4 – FAP to ACS connections**

If the connection is established outside the IPsec tunnel, no specific explanation is needed. TLS/SSL as the TR-069 native method provides the security of the management connection. The <rootobject> already defines the ACS identity, and is expected to exist as the factory-default setting of the FAP:

- ACS identify and associated parameters:
  - <rootobject>.ManagementServer.URL
  - <rootobject>.ManagementServer.Username (if used)
  - <rootobject>.ManagementServer.Password (if used)

If the ACS connection is established through the IPsec tunnel, first the IPsec tunnel needs to be established with the SecGW before the TR-069 session is established with the ACS. In this case, in addition to the parameters listed above, the SecGW identity and associated security parameters are expected to exist as the factory-default setting of the FAP:

- SecGW identity
  - .FAPService.{i}.FAPControl.UMTS.Gateway.SecGWServer1

- Object and subtending sub-objects and parameters necessary to establish the IPsec tunnel under:
  - .FAPService.{i}.Transport.Tunnel.

  

- .FAPService.{i}.Transport.Security.

The FAP's decision whether to use the IPsec tunnel for initial configuration or not depends on the existence of the SecGW parameters in the factory defaults and the parameter <rootobject>.Transport.Tunnel.UseForCWMP. The table shows the possible decisions:

**Table 3 – IPSec Tunnel selection Decision**

| | .FAPService.{i}.**Transport.Tunnel.UseForCWMP** | | |
|---|---|---|---|
| **SecGW parameters** | *Not implemented* | *False* | *True* |
| *Not implemented* | Direct connection | Direct connection | Direct connection |
| *defined* | Use Tunnel | Direct connection | Use Tunnel |

## I.3 SecGW, FAPGW Discovery and Connection Establishment

*Connection Establishment without SecGW:*
Figure 5 below illustrates the process used by the FAP to establish the signaling connection with FAPGW over the IPsec connection with SecGW when the ACS is outside of the IPsec tunnel.

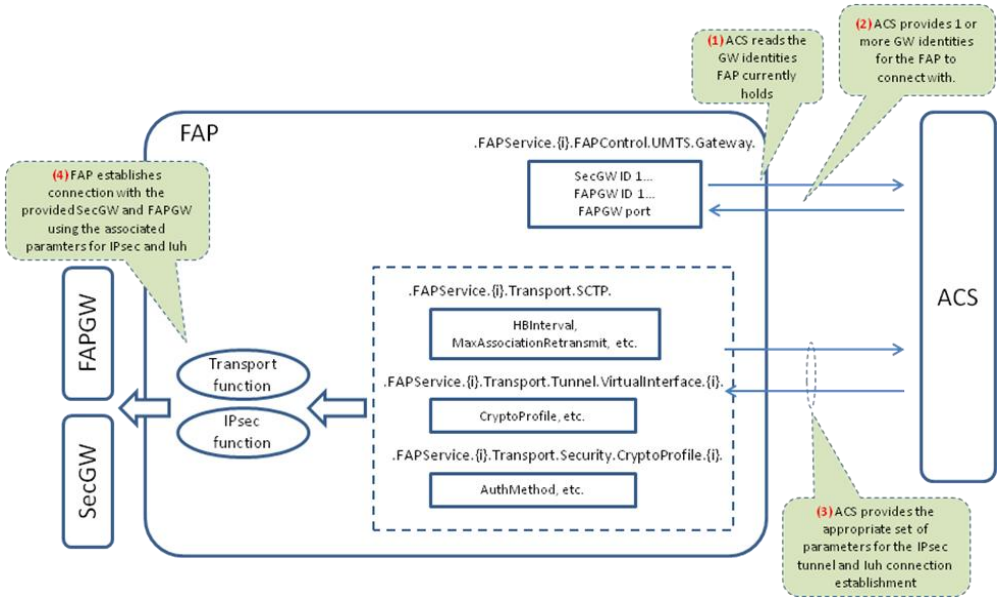


**Figure 5 – SecGW, FAPGW connection establishment**

During this process the FAP is configured with the necessary information about the SecGW.

  

*Connection Establishment with SecGW:*
If the initial TR-069 session with the ACS is established through the IPsec tunnel, then the necessary IPsec related parameters are expected to be already set in the FAP as factory-default. In this case, the ACS can modify the IPsec and SecGW related parameter values anytime if needed.

*Selection of SecGW:*
If the FAP is provided with more than one identity for SecGW, it tries to establish an IPsec tunnel with them in the sequential order they are provided (SecGWID1, 2…). In case the IPsec tunnel is not successfully established, FAP tries the next on the list. After the FAP successfully establishes an IPsec, it moves on to establish signaling connection with the FAPGW similar to the establishment of the SecGW connection.

If ACS decides that the FAP should establish a connection with a SecGW that is different from what it is currently connected, then the ACS can overwrite the SecGW identity. Then the FAP first tears down the existing IPsec tunnel and re-establishes with the new one.

When FAP fails to establish connection with either SecGW or FAPGW for all of the identities provided, then the FAP tries to connect to the ACS directly for re-provisioning of SecGW and/or FAPGW.

## I.4 IPsec Tunnel Status

An IPsec tunnel is established between FAP and SecGW so that FAP and FAP-GW can communicate to each other over the secured connection. Within the FAP the following parameter reflects the status of the SA:

- .FAPService.{i}.Transport.Tunnel.IKESA.{i}.Status

Table 4 below shows the description of the values of this status. If one or more of this multi-instance object pre-exists in FAP, the following description applies to reflect the current status of the IKE SA. If individual multi-instance object is dynamically created/deleted by FAP based on the IPsec tunnel establishment/tear-down, only a subset of the values may be supported to indicate the current status of the IKE SA.

**Table 4 – IKE SA Status**

| Status | Description |
|---|---|
| *Disabled* | This IKE SA is not active. |
| *Active* | This IKE SA has been successfully created. |
| *Completed* | This existing IKE SA has been terminated/deleted. |
| *Progressing* | This IKE SA is in the process of being created. |
| *Error* | This value MAY be used by the CPE to indicate a locally defined error condition. OPTIONAL |

  

## I.5 Location Verification

For Location verification one or more of the following type of information is used:

1. REM process using macro cell information
2. GPS
3. Others (e.g. fixed broadband related information)

Figure 6 below shows the list of objects available for this purpose.

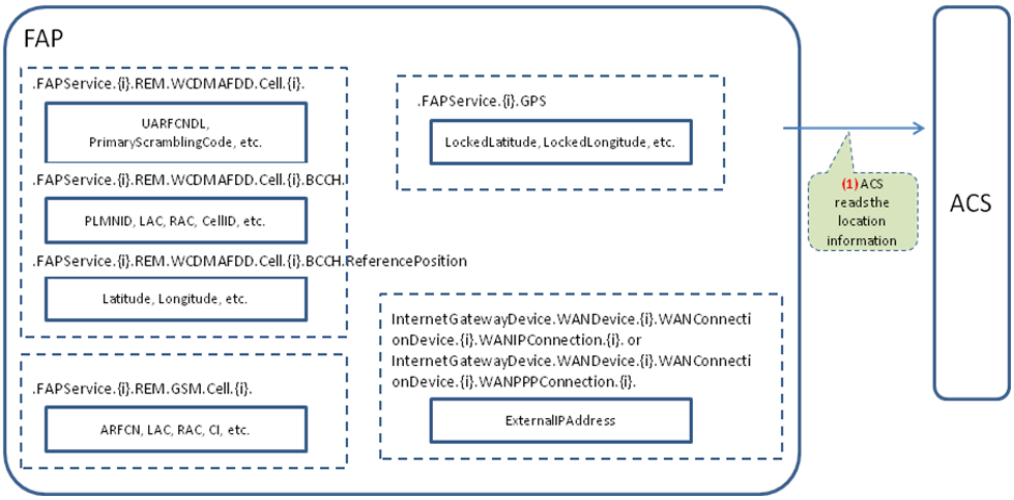


**Figure 6 – Location information**

  

## I.6 Self-Configuration

### I.6.1 General Description

This section describes the self-configuration aspect of the FAP. This topic includes multiple aspects and can mean different things to different people. Even for the same aspect, (e.g. configuration of radio related parameters or neighbor list), it is possible to design more than one way to accomplish the goal. In this respect, even though there is no "right" or "wrong" way in an absolute sense, it is desirable to define a model on which the mechanism is based. To this end, the section illustrates the fundamental concept and approach to the self-configuration.

Note that Radio Environment Measurement (REM) and Neighbor List (NL) configuration require special attention. Therefore, these two topics are discussed separately.

### I.6.2 General Approach to Self-Configuration

Self-configuration is a process in the CM where the FAP determines a specific parameter value among multiple possible choices under the guidance of the ACS as opposed to the latter providing a specific parameter value to the former. The following is the general high-level "theory" of self-configuration of FAP:

1. The ACS acts as the master of the overall self-configuration behavior of the FAP and explicitly instructs the FAP which aspect of the self-configuration it has to perform (or not to perform).
2. FAP behaves under the guidance of the ACS for self-configuration and performs self-configuration for the aspect it is requested to perform within the limitation and boundary set by the ACS.
3. The ACS can provide more than one possible choice of value (or range of values) from which the FAP selects one based on criteria including its local knowledge (e.g. environmental information).
4. The ACS can query the choice made by the FAP and may override the value that the FAP has selected during this process.
5. Once the ACS overrides any specific parameter in the FAP, the FAP accepts the new value unconditionally (as long as the value is valid).

  

### I.6.3 General Process Flow

Figure 7 illustrates an example of the general process flow for the self-configuration. Note that this is a "general" flow and variations exist depending on the exact type of self-configuration. For example, in step (3) in the figure, the ACS provides a list of choices from which the FAP selects. However, in the case of neighbor list configuration, this does not necessarily apply; see the separate section for the self-configuration of the neighbor list.

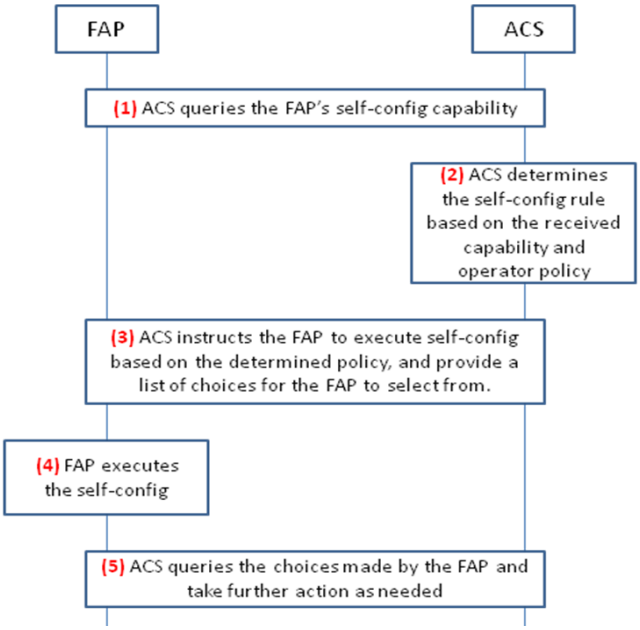


**Figure 7 – General process flow of self-configuration**

### I.6.4 Use of "Active Notification"

In some cases, self-configuration activity can take a period beyond a single TR-069 session. In this case, self-configuration process continues within the FAP independent from the TR-069 session. This implies that a new session needs to be re-established when the FAP is ready to continue with the self-configuration process but no TR-069 session exists at that time.

In this case, one way to facilitate this is to use "active notification." for the self-configured parameters. This is done via setting the "active notification" attribute with an SetParmeterAttributes RPC like described in TR-069[1]. For all parameters with a turned on "active notification" attribute a TR-069 session establishment is triggered when its value changes, and the value change is communicated to the ACS (e.g. self-configuration status change to indicate that the FAP is ready to continue to the next step). This implies that a certain set of parameters needs to have the "notification" attribute to be set appropriately.

  

The example of parameters that can utilize this mechanism includes the followings:

**Table 5 – Example Parameters for Active Notification**

| Parameter | Description |
|---|---|
| .*FAPService*.{i}.REM.WCDMAFDD.ScanStatus | Indicates the current REM status of the UMTS cells (FDD). The change of value from *"InProgress"* to *"Success"* or *"Error_TIMEOUT"* indicates that the FAP has completed the REM process and is ready to proceed to the next step with the FAP. |
| .*FAPService*.{i}.REM.GSM.ScanStatus | Indicates the current REM status of the GSM cells. The change of value from *"InProgress"* to *"Success"* or *"Error_TIMEOUT"* indicates that the FAP has completed the REM process and is ready to proceed to the next step with the FAP. |

### I.6.5 Default Values

There are writable parameters to enable the self-configuration function in the FAP. Typically these writable parameters are set to *"disabled"* when shipped from the factory implying that no self-configuration is allowed until the ACS explicitly sets them to enable them.

This applies to all parameters located under:

- .FAPService.{i}.FAPControl.UMTS.SelfConfig.

### I.6.6 Discovery of Device Capabilities and Activation of Self-Configuration

Figure 8 below shows the activation of self-configuration. The ACS first reads what self-configuration functionalities the FAP supports by reading *…Config* parameters under *.FAPService.{i}.Capabilities.UMTS.SelfConfig*. Based on this information, the ACS enables the appropriate *…ConfigEnable* parameters under *.FAPService.{i}.FAPControl.UMTS.SelfConfig* to activate that specific aspect of the self-configuration. The FAP in turn starts the internal self-configuration function.

  

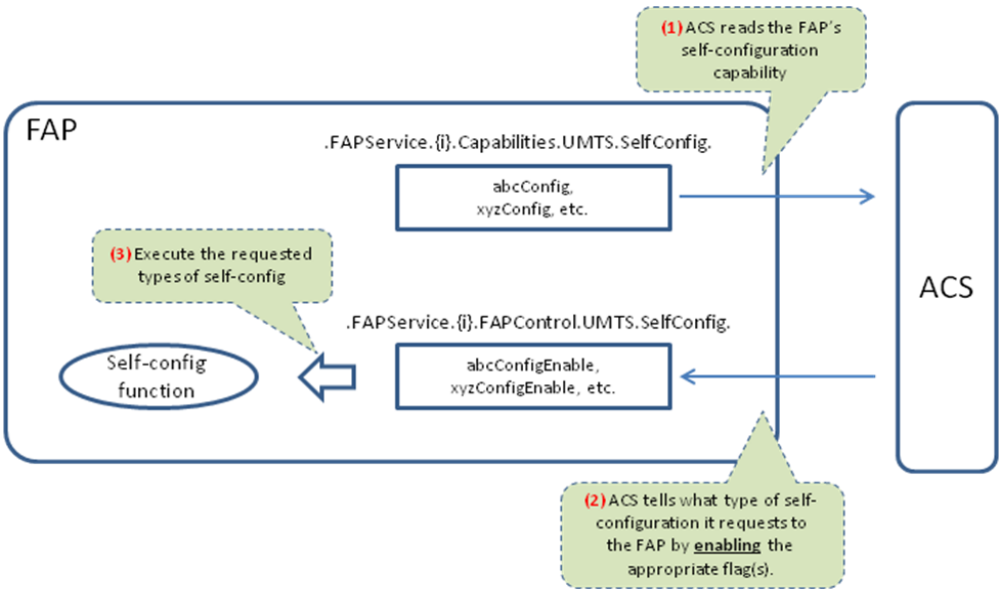


**Figure 8 – Discovery of device capabilities and activation of self-configuration**

### I.6.7 Deactivation of Self-Configuration

Deactivation of self-configuration is done in the following way as shown in Figure **9** below. The ACS disables the appropriate *…ConfigEnable* parameter under *.FAPService.{i}.FAPControl.UMTS.SelfConfig* to de-activate that specific aspect of the self-configuration. FAP in turn stops the internal self-configuration function.

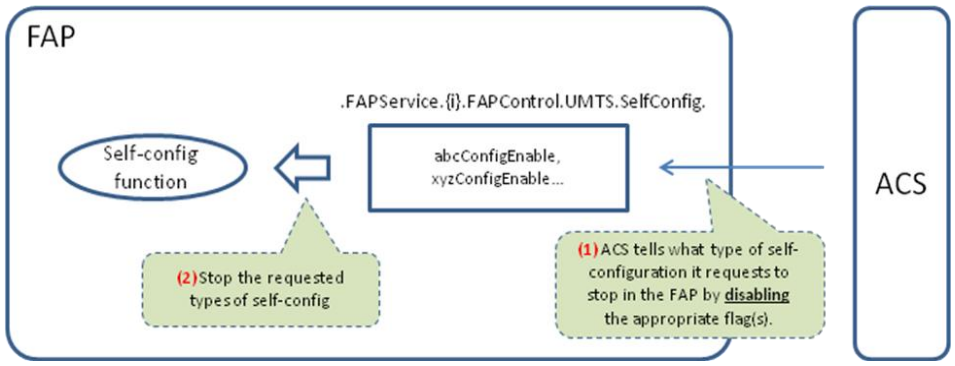


**Figure 9 – Deactivation of self-configuration**

  

### I.6.8 Self-Configuration Operation

There are two types of self-configuration operation. The first type applies to individual parameter and the second type applies to a group of parameters. In Figure 10 below shows these as two horizontal groups. In addition, the figure also displays the relationship of objects and parameters to illustrate the process or flow of events with four columns moving from left to right.

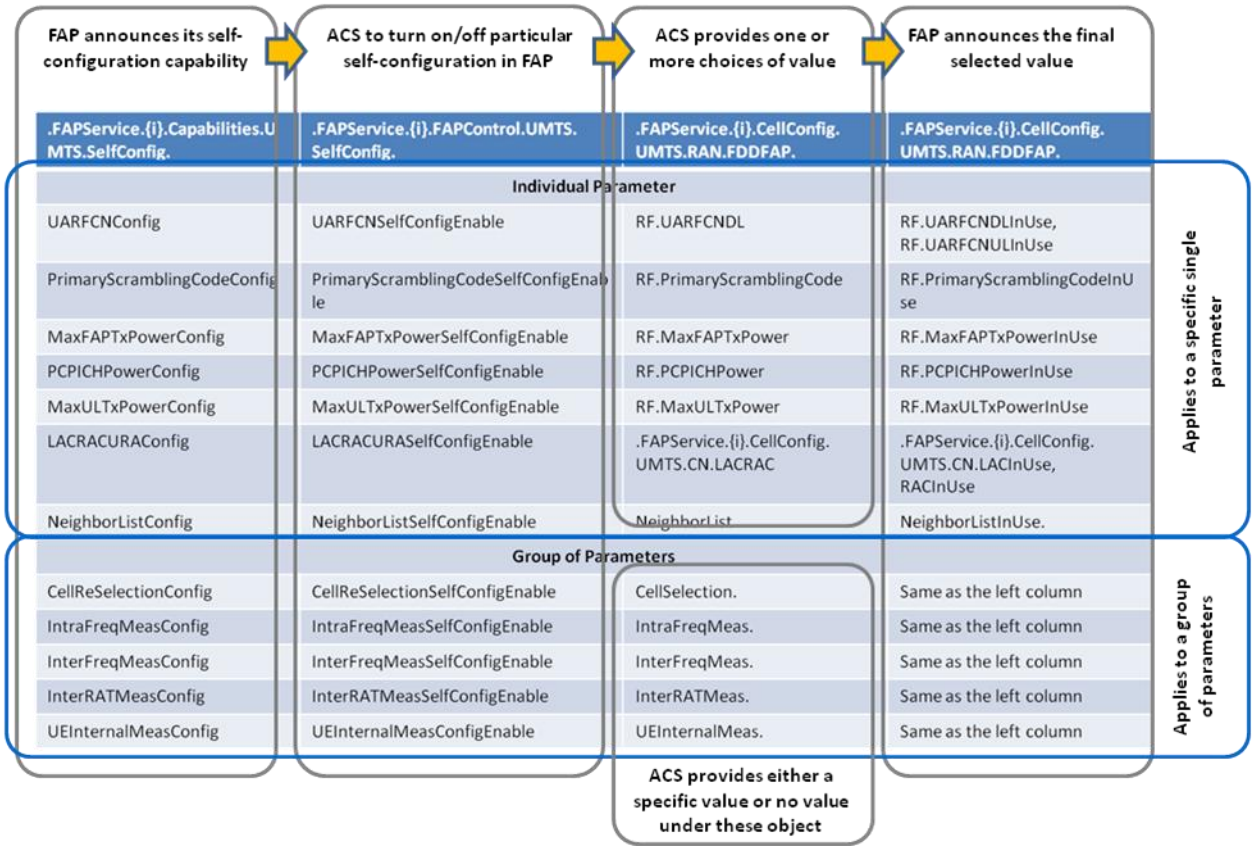


**Figure 10 – Self-configuration operation – object relationship**

For the first type that applies to the individual parameter (the upper horizontal group in the figure), the self-configuration operation is simple – the respective …ConfigEnable flag turns on or off the self-configuration of that particular parameter (e.g. UARFCN).

For the second type that applies to a group of parameters (the lower horizontal group in the figure), the self-configuration operation works as follows:

1. If the ACS explicitly provides a value to a particular parameter in the group during configuration, the FAP takes it as is and considers that self-configuration action of that parameter is not requested.

2. If the ACS does not explicitly provide a value to a particular parameter in the group during the configuration, the FAP considers it as a request by the ACS that those "missing" parameters require self-configuration. The FAP initiates the self-configuration action for those "missing" parameters.

  

## I.7 Radio Environment Measurement (REM) Process

There are three main purposes for the REM process and they are functionally separated:

1. Location verification
   The surrounding cell information (e.g. macro cells) can be used as a "fingerprint" of the area the FAP is located in order for the O&M system to verify its location against the location the FAP owner subscribed the service with (e.g. street address of the owner). The previous section that discusses location verification covers this.

2. Neighbor list (NL) configuration
   The scanning of the DL information (physical radio level information and broadcast information) is gathered from the nearby cells to build the neighbor list. This is a part of the FAP configuration so that it can broadcast appropriate set of NL to the UEs. The next section will cover this.

3. Parameter value selection
   The scanning of the DL information (both physical radio level and broadcast information) from the nearby cells is useful for the parameter selection process within the FAP. If the FAP is provided with a choice of multiple values or range of values, the nearby cell information can be used to avoid collision or to minimize interference in the area. Some of the examples are as follows:
   - Primary Scrambling Code
   - Maximum FAP Transmit Power
   - Maximum UL Transmit Power
   - PCPICH Power
   - LAC, RAC

This section discusses the general aspect of the REM process to facilitate these two purposes.

### I.7.1 Execution of REM

The REM process is expected to be executed at the following timings:

- Very first (i.e. "out-of-the-box") initialization
- Subsequent initialization (i.e. reboot/reset)
- At periodic interval during the normal operation

  

### I.7.2 Configuration of Periodic Measurement

The ACS configures the periodic interval of the REM process by setting one or more of the parameters shown in Figure 11 below.

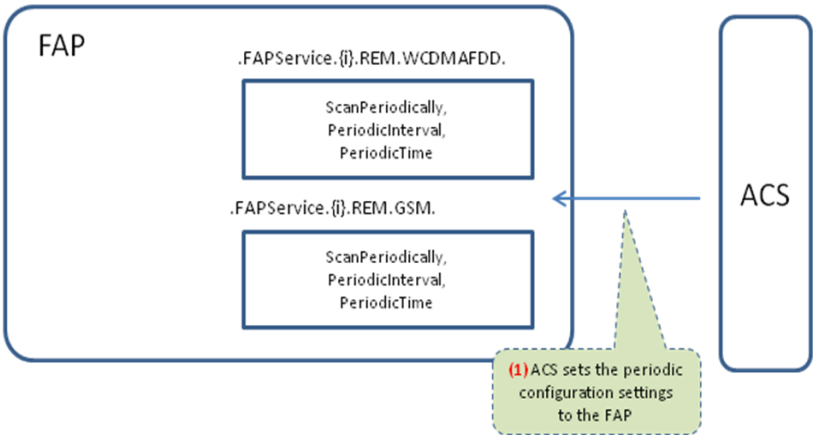


**Figure 11 – REM Periodic Configuration**

### I.7.3 Configuration of Selective Measurement

The REM activity can be setup so that only a selected subset of the possible measurements is to be done. This helps to optionally speed up the REM process in the FAP by possibly ignoring other cell(s) that the system operator chooses not to consider (e.g. cells that belong to other PLMNs, or cells under a specific UARFCN, or other Femto cells). This can be done by using one or more of the following parameters shown in Figure 12 below. Typically, no selective measurement is assumed by the FAP with factory defaults. In other words, all parameter values in Figure 12 are *"<empty>"* when shipped from the factory.

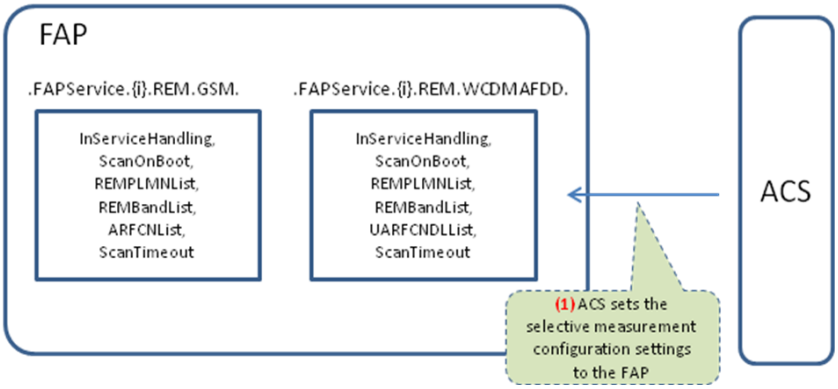


**Figure 12 – REM Selective Measurement Configuration**

### I.7.4 Storage and Retrieval the Measurement Result

Figure 13 below shows the storage and retrieval of the REM information. When the FAP indicates that the information is available (*ScanStatus*), ACS can read the content. See Table 5 for the use of "Active Notification" attribute discussed earlier in this appendix.

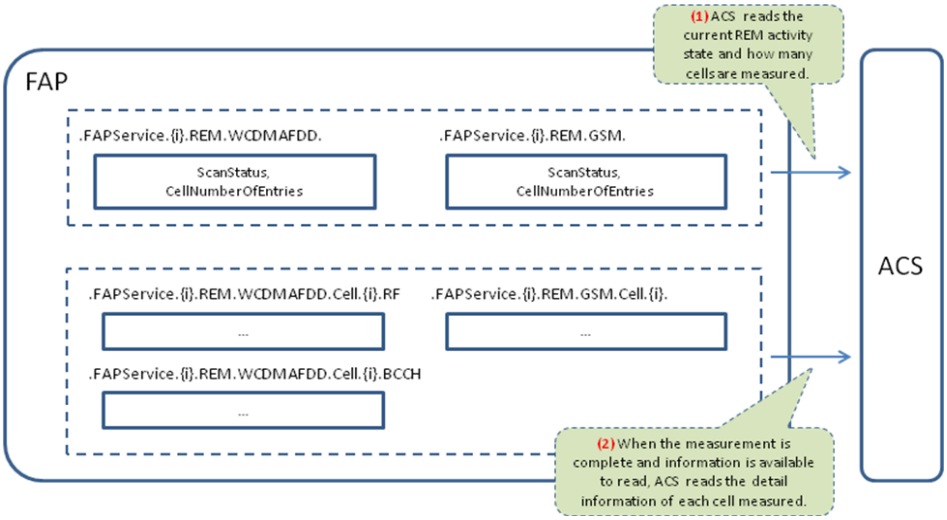


**Figure 13 – Retrieval of REM Result**

Two *ScanStatus* parameters shown in the above figure indicate the current REM status as defined in Table 6 below (this applies to both WCDMA-FDD and GSM cells).

**Table 6 – *ScanStatus* Definition**

| Value | Description |
|---|---|
| *Indeterminate* | REM has not been executed and there are no valid scan results available, or REM has been executed but no neighbor cells have been detected. This is also the initial (default) value (i.e. out-of-the-box state). |
| *InProgress* | REM process is currently in progress and the corresponding *"...Cell.{i}."* objects are not yet ready to be read. |
| *Success* | REM process has completed successfully and corresponding *"...Cell.{i}."* objects are ready to be read. At least one valid entry can be found in the "...Cell.{i}." objects. |
| *Error* | REM process has resulted in error and corresponding *"...Cell.{i}."* objects is either empty or does not contain valid information. |
| *Error_TIMEOUT* | REM process was terminated due to timeout set by the ScanTimeOut parameter. CellNumberOfEntries indicates the number of the valid entries in the corresponding "…Cell.{i}." objects and are ready to be read. |

## I.8 Neighbor List Configuration

There are two methods for the neighbor list configuration:

- Fixed-configuration
- Self-configuration

### I.8.1 Fixed-configuration

In fixed-configuration, the entire neighbor list configuration is provided by the ACS without consideration of the detected neighbors by the FAP as a result of the REM process. In this case, the detected neighbor list from the REM process can be used specifically for the location verification purpose only, but not for the neighbor list configuration purpose. Or ACS can, if so desired, optionally turn-off the entire REM process by setting the *ScanOnBoot* and ScanPeriodically parameters to be *"false."*

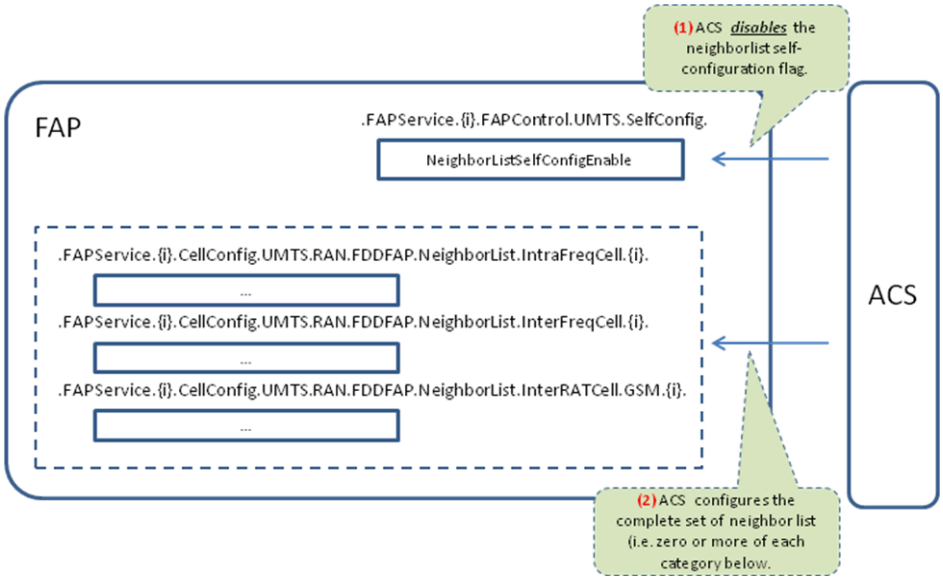


**Figure 14 – Neighbor List – Fixed-configuration**

### I.8.2 Self-configuration

In self-configuration, the result from the REM process is taken into account for the final neighbor list configuration. Based on the REM result, the ACS takes additional step to configure the neighbor list.

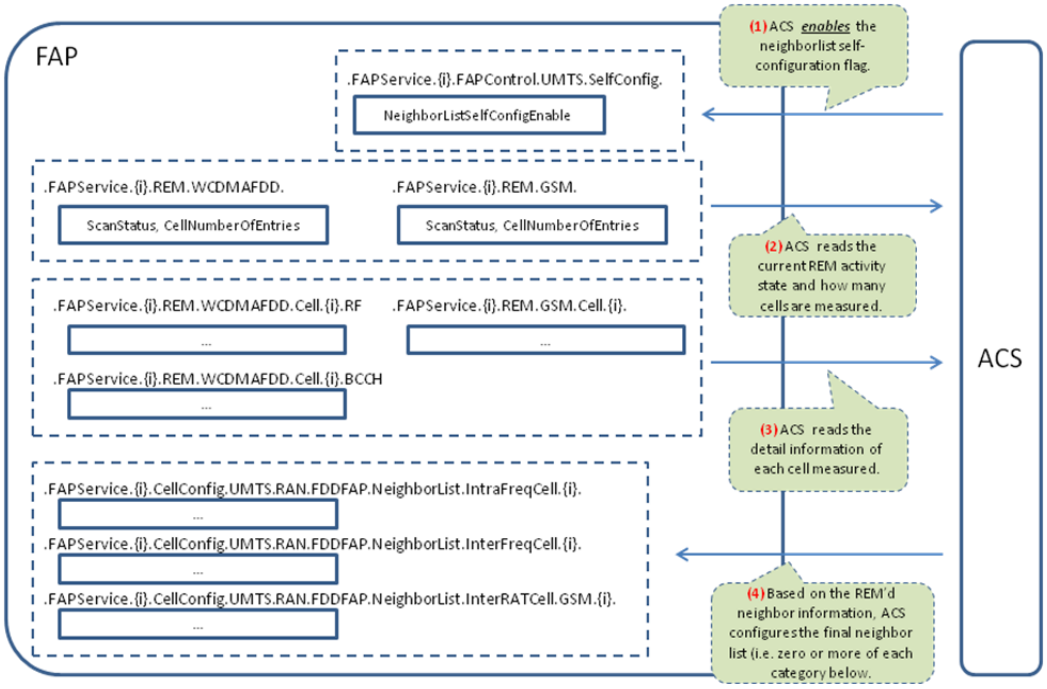


**Figure 11: Neighbor List – Self-configuration**

Upon obtaining the detected neighbor list through the REM process, the ACS has two options to take for each detected neighbor in order to derive the final neighbor list configuration:

1. Keep it.
2. Remove it (ignore it).

In addition, if the ACS wishes to add any cell that is not in the reported neighbor list, it can add it to the final neighbor list.

The decisions made by the ACS mentioned above are communicated to the FAP by *MustInclude* parameter under the following objects:

- .FAPService.{i}.CellConfig.UMTS.RAN.FDDFAP. NeighborList.IntraFreqCell.{i}.
- .FAPService.{i}.CellConfig.UMTS.RAN.FDDFAP. NeighborList.InterFreqCell.{i}.
- .FAPService.{i}.CellConfig.UMTS.RAN.FDDFAP .NeighborList.InterRATCell.GSM.{i}.

Upon receiving the neighbor list in the above object, the FAP obeys the request by the ACS expressed in MustInclude parameter (see next Table).

**Table 7 – *MustInclude* Definition**

| MustInclude value | Description |
|---|---|
| True | ACS requests FAP to include this particular neighbor in the final neighbor list. |
| False | ACS requests FAP to exclude this particular neighbor from the final neighbor list. |

## I.9 State Management

The following Figure 15 shows the State Management.

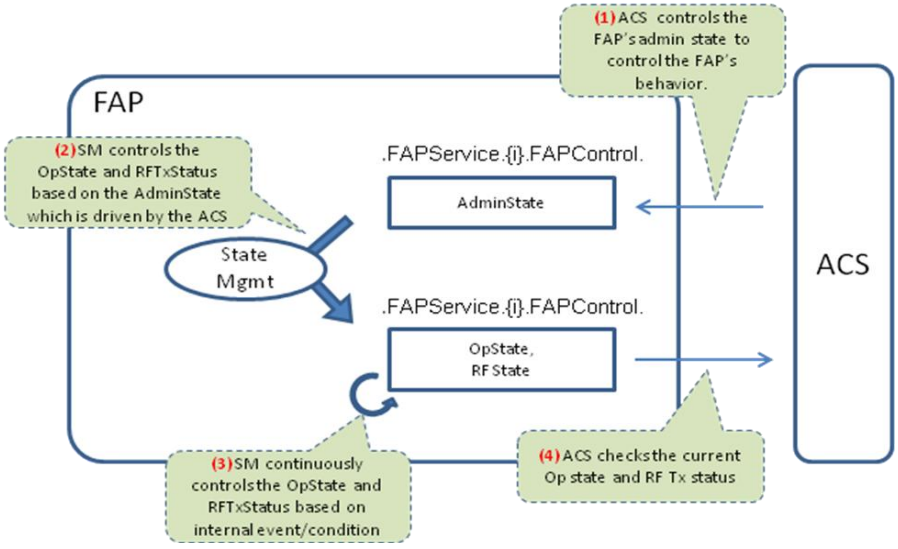


**Figure 15 – State Management**

There are 3 parameters that controls the FAP state and operation.

1. Administrative State (.FAPService.{i}.FAPControl.AdminState)
2. Operational State (.FAPService.{i}.FAPControl.OpState)
3. RF Tx Status (.FAPService.{i}.FAPControl.RFTxStatus)

When the FAP (re-)initializes, it changes the status of these parameters to the following value as default regardless of the current value (see Table 8).

  

**Table 8 – SM parameter Definition**

| Parameter | Default value |
|---|---|
| Administrative State | false (i.e. locked) |
| Operational State | false (i.e. disabled |
| RF Tx Status | false (i.e. RF off) |

## I.10 Fault Management

### I.10.1 Introduction

There are four types of alarm event handling:

| | |
|---|---|
| Expedited Event | alarm event is immediately notified to the ACS with the use of Active Notification mechanism |
| Queued Event | alarm event is notified to the ACS at the next opportunity with the use of Passive Notification mechanism |
| Logged Event | The FAP stores the alarm event locally but does not notify the ACS |
| Disabled Event | The FAP ignores the alarm event and takes no action |

Table 9 shows the multi-instance objects for FM to manage the alarm events.

**Table 9 – FM Object Definition**

| Object name (*FAPService.{i}.FaultMgmt.*) | Table size | Content | Purpose and usage |
|---|---|---|---|
| SupportedAlarm.{i}. | Fixed | Static & fixed content | Defines all alarms that the FAP supports. *ReportedMechanism* defines how the alarm is to be handled within the FAP: *0 – Expedited, 1 – Queued, 2 – Logged, 3 – Disabled*<br>The table size is fixed and its content is static in order to drive the alarm handling behavior in the FAP. |
| ExpeditedEvent.{i}. | Fixed | Dynamically updated | Contains all *"Expedited"* type alarm events since the last FAP initialization. This includes events that are already reported or not yet reported to the ACS. One entry exists for each event. In other words, raising and clearing of the same alarm are two separate entries. As the table size is fixed (vendor defined), new alarm event overwrites the oldest entry in FIFO fashion |

  

| Object name (*FAPService.{i}.FaultMgmt.*) | Table size | Content | Purpose and usage |
|---|---|---|---|
| | | | after the table becomes full. |
| QueuedEvent.{i}. | Fixed | Dynamically updated | Contains all *"Queued"* type alarm events since the last FAP initialization. This includes events that are already reported or not yet reported to the ACS. One entry exist for each event. In other words, raising and clearing of the same alarm are two separate entries.<br>As the table size is fixed (vendor defined), new alarm event overwrites the oldest entry in FIFO fashion after the table becomes full. |
| CurrentAlarm.{i}. | Variable | Dynamically updated | Contains all the currently active alarms (i.e. outstanding alarms that are not yet cleared) since the last FAP initialization. When an outstanding alarm is cleared, that entry is deleted from this table. Therefore, only 1 entry exists for a given unique alarm.<br>ACS can retrieve the content of this table to get the entire view of the currently outstanding alarms.<br>As this is a variable size table, the size changes as alarm event is raised and cleared. |
| HistoryEvent.{i}. | Fixed | Dynamically updated | Contains all alarm events as a historical record keeping purpose. One entry exist for each event. In other words, raising and clearing of the same alarm are two separate entries.<br>ACS can retrieve the content of this table to get the entire chronological history of the alarm events on the FAP.<br>As the table size is fixed (vendor defined), new alarm event overwrites the oldest entry in FIFO fashion after the table becomes full. |

  

Table 10 shows the timing of when an entry to be created/updated/deleted, and the entire table to be cleared.

**Table 10 – FM Object Usage**

| Object name (*FAPService.{i}.FaultMgmt.*) | Timing of a new entry to be created | Timing of an existing entry to be updated | Timing of an existing entry to be deleted | Timing of the entire table to be cleared |
|---|---|---|---|---|
| ExpeditedEvent.{i}. | When a new event of *"Expedited"* type occurs (i.e. raise a new alarm or clear an existing alarm) | Never (i.e. once an entry is made, the content is not changed)<br>The only exception is that when the table is rolling over in a FIFO fashion, the entry will be over-written. | Never (i.e. once created, the content is never deleted) | FAP reboot |
| QueuedEvent.{i}. | When a new event of *"Queued"* type occurs (i.e. raise a new alarm or clear an existing alarm) | Never (i.e. once an entry is made, the content is not changed)<br>The only exception is that when the table is rolling over in a FIFO fashion, the entry will be over-written. | Never (i.e. once created, the content is never deleted) | FAP reboot |
| CurrentAlarm.{i}. | When a new alarm (all types except Disabled events) is raised | When the alarm status changes | When the alarm is cleared | FAP reboot |
| HistoryEvent.{i}. | When a new event of all types except Disabled type occur (i.e. raise a new alarm or clear an existing alarm) | Never (i.e. once an entry is made, the content is not changed)<br>The only exception is that when the table is rolling over in a FIFO fashion, the entry will be over-written. | Never (i.e. once created, the content is never deleted) | Never (i.e. content is maintained across reboot) |

  

### I.10.2 Expedited Event

Figure 16 shows the expedited event handling. All alarms in the *"expedited"* type are stored in *.FAPService.{i}.FaultMgmt.ExpeditedEvent.{i}.* multi-instance object and notified to the ACS using Active Notification mechanism by immediately establishing a TR-069 session with the ACS.

Alarms are also stored in *.FAPService.{i}.FaultMgmt.CurrentAlarm.{i}.* and *.FAPService.{i}.FaultMgmt.HistoryEvent.{i}.*

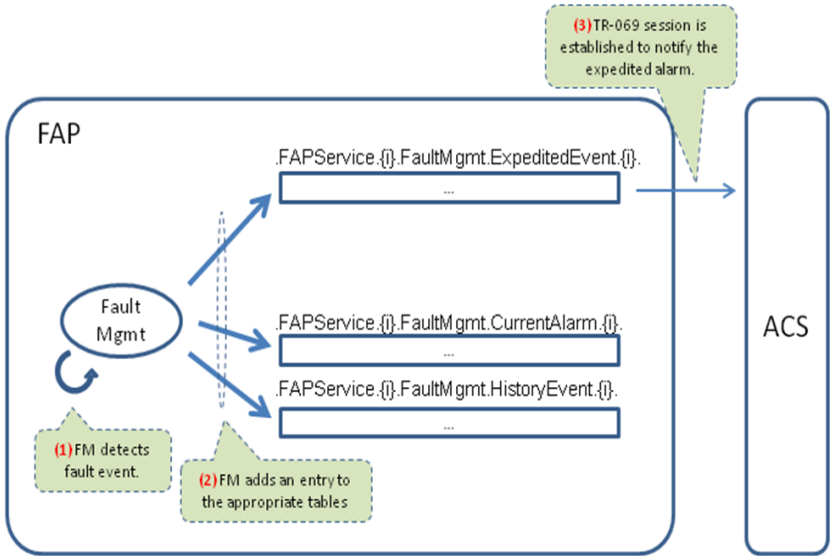


**Figure 16 – Expedited Event Handling**

### I.10.3 Queued Event

Figure 17 shows the queue event handling. All alarms in the "queued" type are stored in. *.FAPService.{i}.FaultMgmtQueuedEvent.*{i}. multi-instance object. It is notified to the ACS using Passive Notification mechanism. In this case, the event is notified to the ACS at the next TR-069 session establishment.

Alarms are also stored in *.FAPService.{i}.FaultMgmt.CurrentAlarm.{i}.* and *.FAPService.{i}.FaultMgmt.HistoryEvent.{i}.*

  

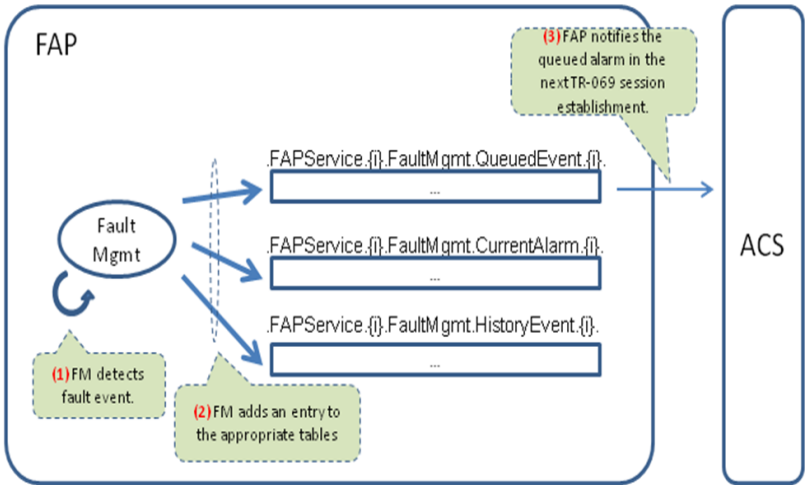


**Figure 17 – Queued Event Handling**

### I.10.4 Logged Event

Figure 18 shows the logged event handling. All alarms in the *"logged"* type are stored only in the *.FAPService.{i}.FaultMgmt.CurrentAlarm.{i}.* and *.FAPService.{i}.FaultMgmt.HistoryEvent.{i}.* Alarms of this type are not reported to the ACS.

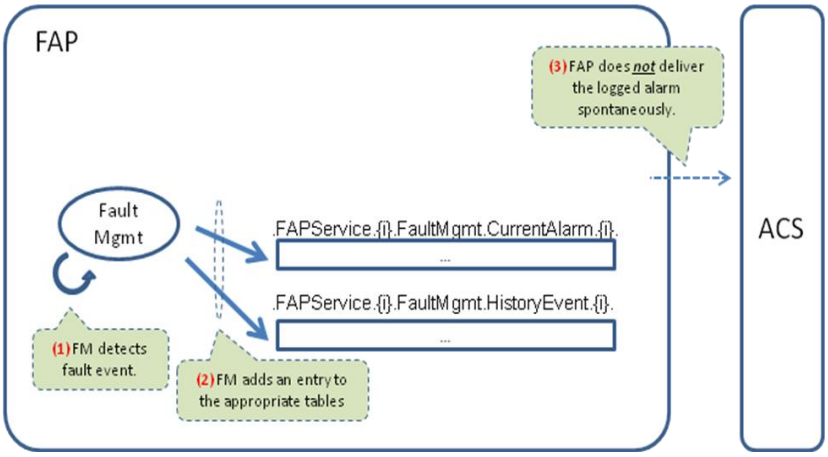


**Figure 18 – Logged Event Handling**

End of Broadband Forum Technical Report TR-196