"*802.11 as a component*" Available OAM interface specifications

Date: 2015-09-14

Authors:

Name	Affiliations	Phone	email
Max Riegel	Nokia Networks	+49 173 293 8240	maximilian.riegel@nokia.com

Abstract

- **The presentation provides an overview about available specifications of open OAM interfaces for implementations of IEEE 802.11.**

- **In a particular sense all the specifications describe '802.11 as a kind of component'.**

- **The material may provide insights into today's requirements and capabilities, as the presented specifications are all widely deployed.**

IEEE 802.11 Standards Environment
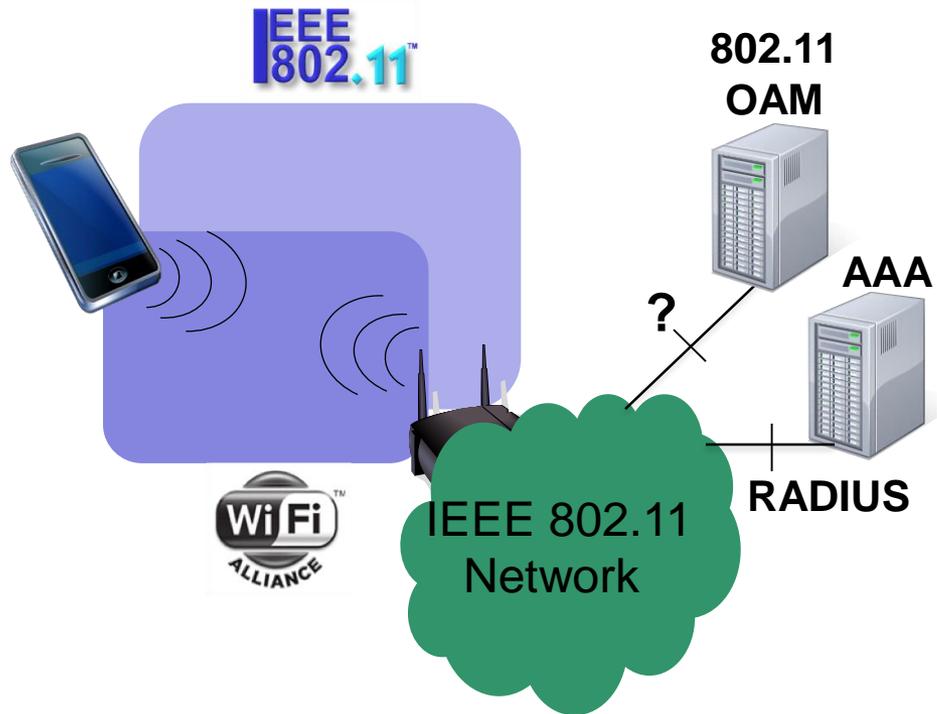
- **IEEE 802.11 defines a radio interface**
- **Wi-Fi Alliance ensures compliance of the radio interface by certification**
- **OAM of the 802.11 radio interface is described by a comprehensive MIB**
- **A couple of organizations developed special variants of OAM interfaces for 802.11**
- **However there is a single solution for AAA: RADIUS**

802.11 OAM

AAA

?

RADIUS

IEEE 802.11 Network

'OAM' Interface Specifications for 802.11

- **BroadBandForum**
  - Wi-Fi model and attributes of Device Data Model 2 (TR-181) for CPE WAN Management Protocol (TR-069)
- **CableLabs**
  - Wi-Fi Provisioning Framework Specification (WR-SP-WiFi-MGMT)
- **IETF CAPWAP**
  - Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification (RFC5415) and Binding for IEEE 802.11 (RFC5416)
- **LINUX Wireless**
  - mac80211 Wi-Fi driver architecture with cfg80211 kernel configuration module and nl80211 netlink user space interface
- **IETF RADIUS**
  - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)Usage Guidelines (RFC3580), RADIUS Attributes for IEEE 802 Networks (RFC7268) and Carrying Location Objects in RADIUS and Diameter (RFC5580)
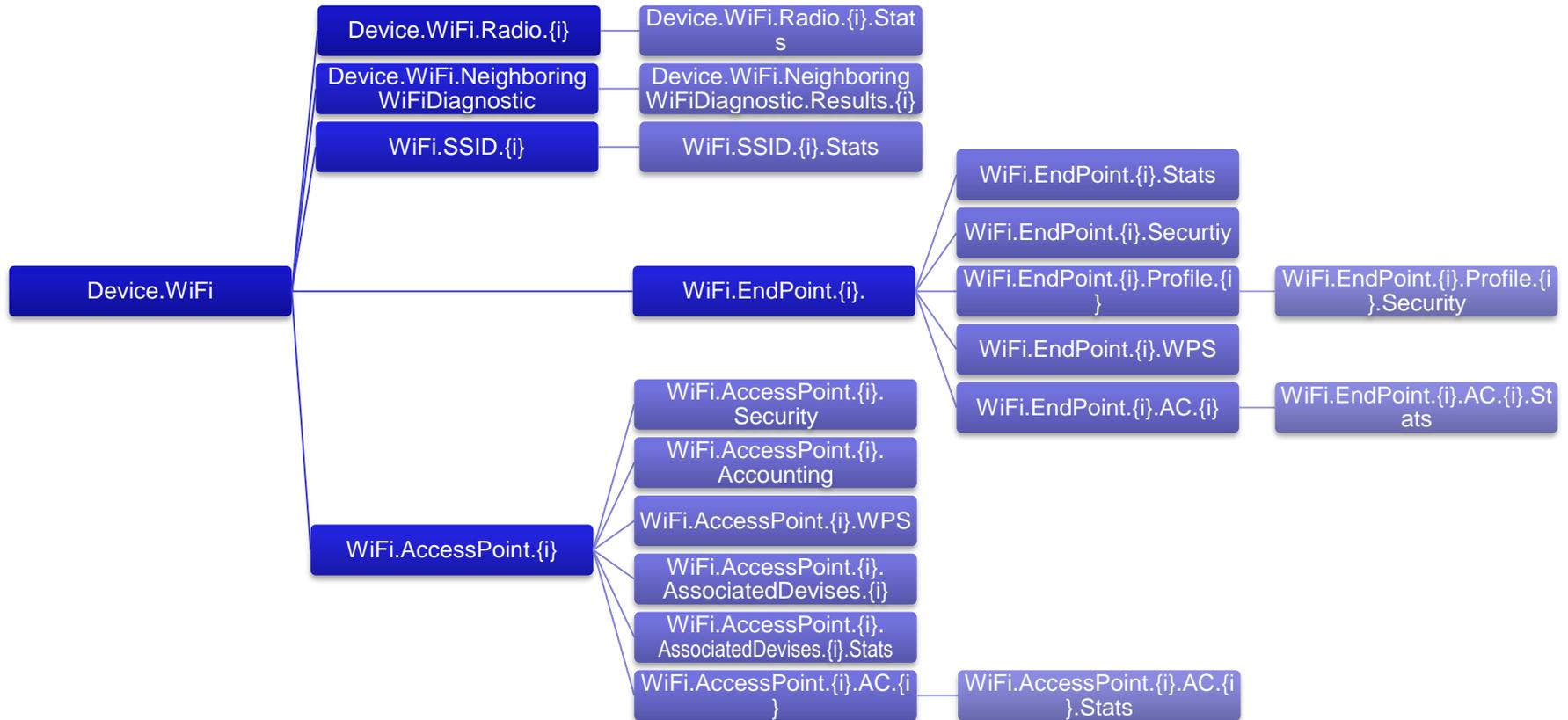
BroadBand Forum CWMP

- **CWMP: CPE WAN Management Protocol aka TR-069**
  - https://www.broadband-forum.org/cwmp.php
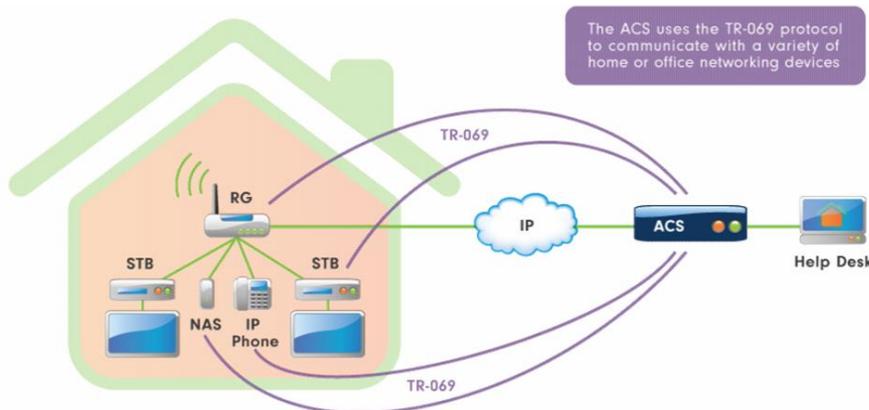
Broadband Forum, MR230, TR-069 deployment scenarios

  - TR-069 is an soap/HTTP based protocol for transmission of XMLbased descriptions of management models between CPE and ACS
  - TR-069 Data Models are xml documents that are "schema-like", that describe the management objects and parameters used for particular use cases.
- **The CWMP Data Model Schema is specified in TR-106.**
- **TR-181 defines version 2 of the TR-069 Device data model (Device:2) and is applicable to all types of TR-069-enabled devices. It obsoletes both Device:1 and InternetGatewayDevice:1 specifications**

TR-181 Wi-Fi Model

```
Device.WiFi
├── Device.WiFi.Radio.{i} ─── Device.WiFi.Radio.{i}.Stats
├── Device.WiFi.Neighboring WiFiDiagnostic ─── Device.WiFi.Neighboring WiFiDiagnostic.Results.{i}
├── WiFi.SSID.{i} ─── WiFi.SSID.{i}.Stats
├── WiFi.EndPoint.{i}.
│   ├── WiFi.EndPoint.{i}.Stats
│   ├── WiFi.EndPoint.{i}.Securtiy
│   ├── WiFi.EndPoint.{i}.Profile.{i} ─── WiFi.EndPoint.{i}.Profile.{i}.Security
│   ├── WiFi.EndPoint.{i}.WPS
│   └── WiFi.EndPoint.{i}.AC.{i} ─── WiFi.EndPoint.{i}.AC.{i}.Stats
└── WiFi.AccessPoint.{i}
    ├── WiFi.AccessPoint.{i}.Security
    ├── WiFi.AccessPoint.{i}.Accounting
    ├── WiFi.AccessPoint.{i}.WPS
    ├── WiFi.AccessPoint.{i}.AssociatedDevises.{i}
    ├── WiFi.AccessPoint.{i}.AssociatedDevises.{i}.Stats
    └── WiFi.AccessPoint.{i}.AC.{i} ─── WiFi.AccessPoint.{i}.AC.{i}.Stats
```

TR-181 Wi-Fi model summary

- **TR-181 supports two kinds of devices: APs and (nonAP) STAs (Endpoints)**

- **A Wi-Fi device consists out of 1..n radio interfaces, 1..n SSIDs and 1..n AccessPoints or EndPoints**

- **A compact set of IEEE 802.11 specific attributes are provided for configuration**

- **Each of the elements of the Wi-Fi model has a rich set of attributes for monitoring/accounting/statistics.**

CableLabs

CableLabs Wi-Fi MGMT overview

- **WR-SP-WiFi-MGMT-I05-141201.pdf is CableLabs' most relevant specification for OAM of Wi-Fi interfaces.**

- **CableLabs builds management of Wi-Fi on top of TR-069 approaches by**

  - adopting the TR-181 device model for Wi-Fi

  - amending the device model by vendor specific extensions for missing functions

  - defining a compatible SNMP MIB to enable backward-compatibility to the legacy provisioning and management systems in the cable environment

- **CableLabs has currently the most far-reaching Wi-Fi management model for 'residential' deployments**

  - Covering Passpoint™ and reaching out into SON for Wi-Fi

CableLab specific extensions:

- **RadiusClient**
- **Interworking Service**
- **Passpoint**
- **ClientSessions**
- **ClientState**
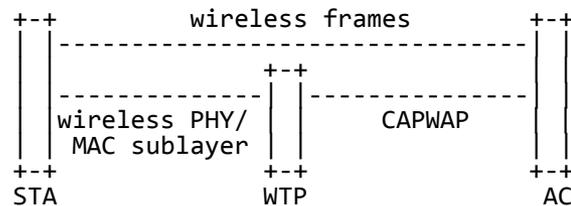- **ApNeighborStats**
- **AccessControlFilter**
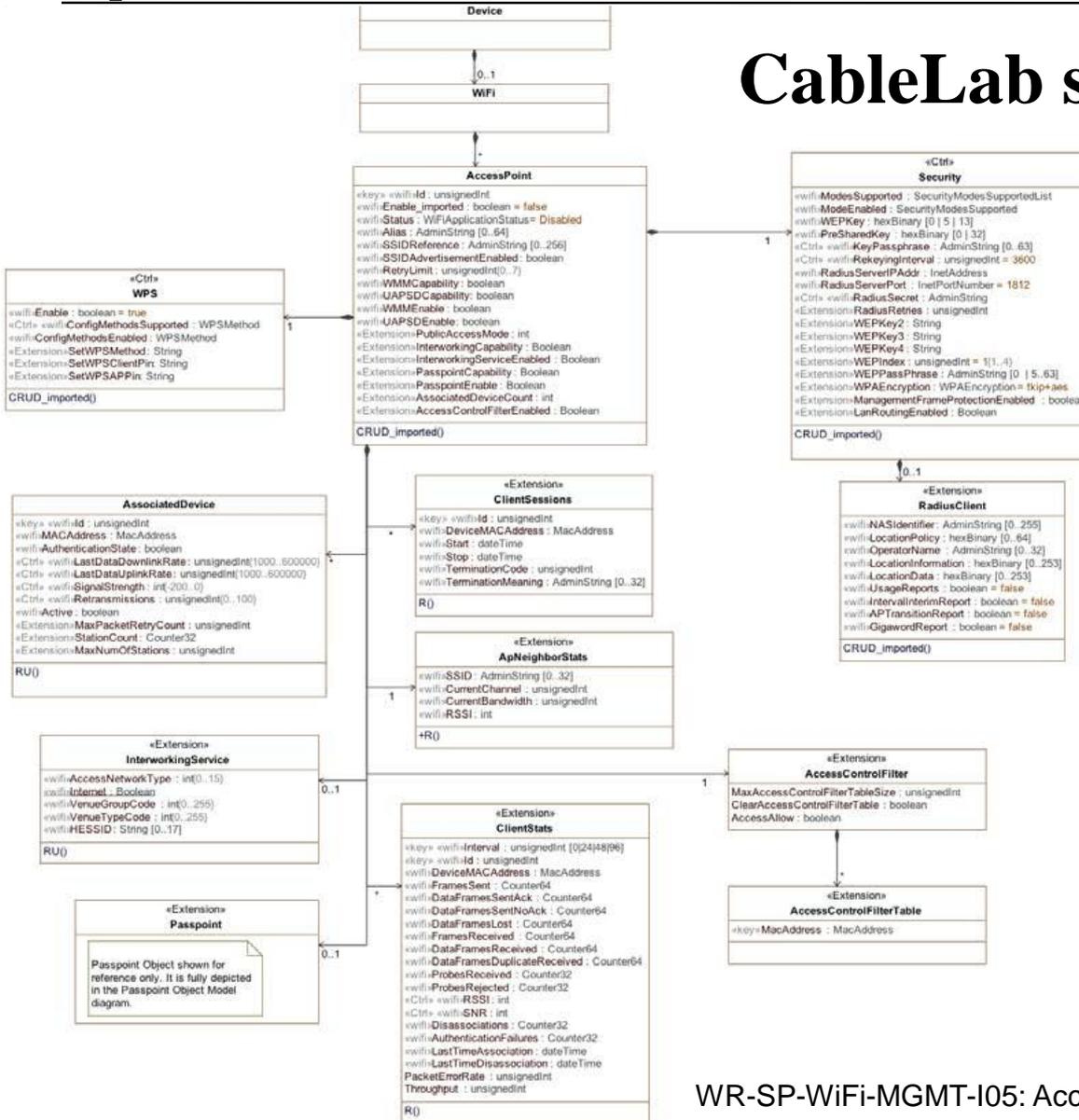
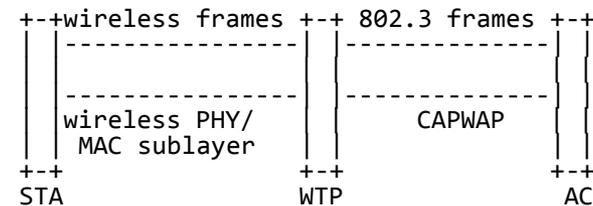WR-SP-WiFi-MGMT-I05: Access Point Object Model Class Diagram

IETF CAPWAP
Control And Provisioning of Wireless Access Points

- **CAPWAP adresses the communication between a wireless termination point (WTP) and an access controller (AC)**

- **Supports different architectural models with various possibilities to locate functions either in WTB or AC**

```
+-+        wireless frames         +-+              +-+wireless frames +-+ 802.3 frames +-+
| |-------------------------------| |              | |---------------| |--------------| |
| |              +-+              | |              | |     +-+       | |      +-+      | |
| |--------------| |--------------| |              | |-----| |-------| |------| |------| |
|wireless PHY/   | |    CAPWAP    | |              |wireless PHY/    | |  CAPWAP | |    | |
| MAC sublayer   | |              | |              | MAC sublayer    | |         | |    | |
+-+              +-+              +-+              +-+               +-+          +-+    +-+
STA              WTP              AC               STA               WTP            AC

Representative CAPWAP Architecture for Split MAC    Representative CAPWAP Architecture for Local MAC
```

- **RFC 5415 defines Control And Provisioning of Wireless Access Points (CAPWAP) Protocol**

- **RFC 5416 provides Binding of CAPWAP for IEEE 802.11**

Applicability

- **Market momentum of CAPWAP was never reached to diminishing benefits of split-MAC implementations**
  - High throughput is easier handled by local MAC solutions
- **Local MAC solutions not really require a complex protocol like CAPWAP**
  - Other protocols like TR-069 (or even ssh) are sufficient
- **802.11 binding in RFC5416 is too hard-coded.**
  - Even tiny extensions have to go through a complete IETF standardization cycle
  - Recent activities in IETF opsawg to amend RFC5416 for more recent 802.11 standards and deployment scenarios
    - RFC7494: IEEE 802.11 Medium Access Control (MAC) Profile for Control and Provisioning of Wireless Access Points (CAPWAP)

LINUX Wireless

LINUX Wi-Fi driver architecture

- **nl80211 has become defacto standard for Wi-Fi configuration in LINUX**
  - Defines a comprehensive list of controls, commands and attributes for Wi-Fi
  - Communicates by netlink (RFC3549) with kernel
- **cfg80211 provides unified interface into kernel drivers**

Wi-Fi OAM specification '*nl80211.h*'

http://git.kernel.org/cgit/linux/kernel/git/linville/wireless.git/tree/include/uapi/linux/nl80211.h?id=HEAD

```
#ifndef __LINUX_NL80211_H
#define __LINUX_NL80211_H
/*
 * 802.11 netlink interface public header
 *
 * Copyright 2006-2010 Johannes Berg <johannes@sipsolutions.net>
 * Copyright 2008 Michael Wu <flamingice@sourmilk.net>
 * Copyright 2008 Luis Carlos Cobo <luisca@cozybit.com>
 * Copyright 2008 Michael Buesch <m@bues.ch>
 * Copyright 2008, 2009 Luis R. Rodriguez <lrodriguez@atheros.com>
 * Copyright 2008 Jouni Malinen <jouni.malinen@atheros.com>
 * Copyright 2008 Colin McCabe <colin@cozybit.com>
 *
 * Permission to use, copy, modify, and/or distribute this software for any
 * purpose with or without fee is hereby granted, provided that the above
 * copyright notice and this permission notice appear in all copies.
 *
 * THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
 * WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
 * MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
 * ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
 * WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
 * ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
 * OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
 *
 */

#include <linux/types.h>

#define NL80211_GENL_NAME "nl80211"

/**
 * DOC: Station handling
 *
 * Stations are added per interface, but a special case exists with VLAN
 * interfaces. When a station is bound to an AP interface, it may be moved
 * into a VLAN identified by a VLAN interface index (%NL80211_ATTR_STA_VLAN).
 * The station is still assumed to belong to the AP interface it was added
 * to.
 *
 * Station handling varies per interface type and depending on the driver's
 * capabilities.
 *
```

nl80211.h defines…

- **120 commands**
- **about 600 attributes and controls**

Potentially nl80211.h is the most comprehensive open OAM interface for 802.11

- **next to the 802.11 MIB**

IETF RADIUS
Remote Authentication Dial-In User Service

- **RADIUS is commonly used for the communication between Access Point and AAA server for user authentication, user authorization and user accounting.**

- **Support of EAPoLAN (IEEE 802.1X), which was introduced to 802.11 by 802.11i, is specified in RFC3580 (IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines).**

- **Further IEEE802 specific attributes are specified by RFC7268 (RADIUS Attributes for IEEE 802 Networks) to support interworking with external networks and enhanced security modes.**

- **RFC5580 (Carrying Location Objects in RADIUS and Diameter) allows also 802.11 to convey location information over the AAA infrastructure.**

Conclusion

- **There are severaly specifications for open OAM interfaces into an IEEE802.11 radio interface.**
  - Created in various places in the communication industry according to deployment needs
- **None of them seems to be sufficient to cover all current and future deployment cases.**
  - Ease of amending the OAM interface specification seems to be highly important to allow for timely deployment of new 802.11 features and functions.
    - Apparently some of the current specifications do better than others
- **Is there really need to start something new from scratch?**

Steps forward

- **Further work on the assessment of existing OAM specification for 802.11 would benefit from input from experts:**

- **Are there other specifications?**

- **Guidance for comparison of specifications?**

- **Is there a recommended structure for listing/grouping capabilities?**

  - e.g. CableLabs Access Point Management Object Model

- **Is there any prior art on comparative assessment of 802.11 management models?**