Wireless Specifications

Wi-Fi Provisioning Framework Specification

WR-SP-WiFi-MGMT-I09-220621

ISSUED

Notice

DISCLAIMER

This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	WR-SP-WiFi-MGMT-I09-220621			
Document Title:	Wi-Fi Provisioning Framework Specification			
Revision History:	I01 – Released July 29, 2010 I02 – Released October 5, 2010 I03 – Released February 16, 2012 I04 – Released March 11, 2014 I05 – Released December 1, 2014 I06 – Released January 11, 2016 I07 – Released May 12, 2016 I08 – Released December 13, 2016 I09 – Released June 21, 2022			
Date:	June 21, 2022			
Status:	~~Work in Progress~~	~~Draft~~	**Issued**	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	**Public**

Key to Document Status Codes

Work in Progress	An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
Draft	A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A generally public document that has undergone Member and Technology Supplier review, cross-vendor interoperability, and is for Certification testing if applicable. Issued Specifications are subject to the Engineering Change Process.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks

Contents

Figures

Tables

1 SCOPE

1.1 Introduction and Purpose

This specification details the management requirements for the Wireless Fidelity (Wi-Fi) air interface and roaming requirements defined in Wi-Fi Requirements for Cable Modem Gateways specification [WiFi-GW] and WR Roaming Architecture and Interfaces Specification [WiFi-ROAM]. The purpose of this specification is to define object models and over the wire interface definitions to support the management functions of the Wi-Fi requirements. The term management functions relate to the traditional FCAPS (Fault Configuration, Accounting, Performance and Security) areas of management [M.3400].

1.2 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word means that the item is an absolute requirement of this specification.
"CONDITIONAL MUST"	This requirement is a conditional MUST (i.e., it is a requirement only if the feature(s) to which it applies is implemented).
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 REFERENCES

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

All references are subject to revision, and parties to agreement based on this specification are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

[802.11]	IEEE 802.11: Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2012.
[802.11a]	IEEE 802.11a: High-speed Physical Layer in the 5 GHz Band, 1999.
[802.11ac]	IEEE 802.11ac: Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz, December 2013.
[802.11ax]	IEEE 802.11ax: Amendment 1: Enhancements for High-Efficiency WLAN, February 2021.
[802.11b]	IEEE 802.11b: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, 1999.
[802.11g]	IEEE 802.11g: Further Higher Data Rate Extension in the 2.4 GHz Band, 2003.
[802.11i]	IEEE 802.11i: Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.
[802.11n]	IEEE 802.11n: Amendment 5: Enhancement for Higher Throughput, 2009.
[802.1Q]	IEEE 802.1Q: Media Access Control (MAC) bridges and Virtual Bridged Local Area Networks, 2011.
[802.1X]	IEEE 802.1X: Port-Based Network Access Control, 2010.
[CLAB-WIFI-MIB]	CableLabs Wireless CLAB-WIFI-MIB SNMP2 MIB Module, CLAB-WIFI-MIB, http://www.cablelabs.com/MIBs/wireless/
[ISO/IEC 3166-1]	ISO/IEC: 3166-1 Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, 2006.
[MULPIv3.0]	Data-Over-Cable Service Interface Specifications, DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.0-C01-171207, December 7, 2017, Cable Television Laboratories, Inc.
[OSSIv3.0]	Data-Over-Cable Service Interface Specifications, DOCSIS 3.0 Operations Support System Interface Specification, CM-SP-OSSIv3.0- C01-171207, December 7, 2017, Cable Television Laboratories, Inc.
[RFC 2865]	IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), June 2000.
[RFC 1035]	IETF RFC 1035 Domain names - implementation and specification. P.V. Mockapetris. November 1987.
[RFC 2863]	IETF RFC 2863, The Interfaces Group MIB, June 2000.
[RFC 3986]	IETF RFC 3986, Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee, R. Fielding, L. Masinter, January 2005.
[RFC 4282]	IETF RFC 4282, The Network Access Identifier. B. Aboba, M. Beadles, J. Arkko, P. Eronen, December 2005.
[RFC 5580]	IETF RFC 5580, Carrying Location Objects in RADIUS and Diameter, August 2009.

[sRouter] CableLabs Access Network Independent, Standalone Router Specification, CL-SP-sRouter-I03-200715, July 15, 2020, Cable Television Laboratories, Inc.

[TR-069] TR-069 CPE WAN Management Protocol v1.1, Issue 1, Amendment 6 Corrigendum 1, June 2020.

[TR-181i2] TR-181 Device Data Model for TR-069, Issue 2, Amendment 14, November 2020, Broadband Forum Technical Report.

[TR-369] Broadband Forum TR-369: User Services Platform (USP), Issue 1 Amendment 1 Corrigendum 2.

[WFA] Hotspot 2.0 (Release 2) Technical Specification, Version 1.0.0, August 2014, WiFi Alliance.

2.2 Informative References

This specification uses the following informative references.

[802.11d] IEEE 802.11d: Amendment 3: Specification for operation in additional regulatory domains, 2001.

[802.11e] IEEE 802.11e: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, 2005.

[802.11h] IEEE 802.11h: Amendment 5: Spectrum and Transmit Power Management Extensions in the 5Gz band in Europe, 2003.

[802.11k] IEEE 802.11k: Amendment 1: Radio Resource Measurement of Wireless LANs, 2008.

[eDOCSIS] eDOCSIS Specification, CM-SP-eDOCSIS-I30-190213, February 13, 2019, Cable Television Laboratories, Inc.

[eRouter] IPv4 and IPv6 eRouter Specification, CM-SP-eRouter-121-220209, February 9, 2022, Cable Television Laboratories, Inc.

[HTTP Bulk Data] HTTP Bulk Data Collection - https://www.broadband-forum.org/download/TR-369.pdf

[M.3400] ITU-T Recommendation M.3400: TMN AND Network Maintenance: International Transmission Systems, Telephone Circuits, Telegraphy, Facsimile and Leased Circuits, TMN management functions, 02/2000.

[RFC 2578] IETF RFC 2578/ STD0058, Structure of Management Information Version 2 (SMIv2), April 1999.

[RFC 2898] IETF RFC 2898, PKCS #5: Password-Based Cryptography Specification Version 2.0, September 2000.

[RFC 4122] IETF RFC 4122, A Universally Unique IDentifier (UUID) URN Namespace, July 2005.

[RFC 4639] IETF RFC 4639, Cable Device Management Information Base for Data-Over-Cable Service Interface Specification (DOCSIS) Compliant Cable Modems and Cable Modem Termination Systems, December 2006.

[RFC 6838] IETF RFC 6838 Media Type Specifications and Registration Procedures. N. Freed, J. Klensin, T. Hansen. January 2013

[TR181-Ext] http://www.cablelabs.com/namespaces/Wireless/TR181Ext/

[WiFi-GW] Wi-Fi Requirements for Cable Modem Gateways, WR-SP-WiFi-GW-I05-150515, May 15, 2015, Cable Television Laboratories, Inc.

[WiFi-ROAM] Wi-Fi Roaming Architecture and Interfaces Specification, PKT-SP-WiFi-ROAM-I04-141201, December 1, 2014, Cable Television Laboratories, Inc.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; http://www.cablelabs.com
- Broadband Forum, 48377 Fremont Blvd, Suite 117 Fremont, CA 94538, Phone: +1.510.492.4020, Fax: +1.510.492.4001, http://www.broadband-forum.org
- Institute of Electrical and Electronics Engineers, (IEEE), http://www.ieee.org/web/standards/home/index.html
- International Organization for Standardization (ISO), Phone:+41-22-749 01-11; Fax :+41 22-733-34-30, http://www.iso.org/iso
- Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA; Phone: +1-510-492-4080, Fax: +1-510-492-4001.
- ITU Recommendations, International Telecommunication Union, Place des Nations, CH-1211, Geneva 20, Switzerland; Phone +41-22-730-51-11; Fax +41-22-733-7256; http://www.itu.int
- Wi-Fi Alliance, 3925 West Braker Lane, Austin, TX 78759 USA, Phone: +1 (512) 305-0790, Fax: +1 (512) 305-0791, http://www.wi-fi.org

3 TERMS AND DEFINITIONS

This specification uses the following terms.

CWMP	The CPE WAN Management Protocol (as defined in [TR-069]) is a standardized protocol for managing, monitoring, upgrading, and controlling connected devices.
D-ONU	DPoE-capable ONU that complies with all the DPoE specifications.
eRouter	An eSAFE device that is implemented in conjunction with the DOCSIS Embedded Cable Modem.
FCAPS	A set of principles for managing networks and systems, wherein each letter represents one principle. F is for Fault, C is for Configuration, A is for Accounting, P is for Performance, S is for Security.
Hotspot 2.0	Wi-Fi Alliance (WFA) Hotspot 2.0 solution based on IEEE 802.11-u (now incorporated in [802.11] and WFA extensions.
interworking	A service that supports use of an IEEE 802.11 network with non-IEEE 802.11 networks. Functions of the interworking service assist non-access-point (non-AP) stations (STAs) in discovering and selecting IEEE 802.11 networks, in using quality-of-service (QoS) settings for transmissions, in accessing emergency services, and in connecting to subscription service providers (SSPs).
management information base	A database of device configuration and performance information which is acted upon by SNMP.
management protocol	Allows a host to query modules for network-related statistics and error conditions.
multi-operator	Common agreements, requirements and operations amongst operators to support roaming.
Passpoint	Passpoint is a trademark of the Wi-Fi Alliance. It is used in this document synonymously with Hotspot 2.0.
private SSID	An SSID reserved for subscriber private use on the home LAN and may be configurable by the subscriber. Access is typically managed by the subscriber.
public SSID	A Service Provider (SP) configured SSID with client access managed by the SP typically used for applications such as home hotspot.
private SSID	An SSID reserved for subscriber private use on the home LAN and may be configurable by the subscriber. Access is typically managed by the subscriber.
public SSID	A Service Provider (SP) configured SSID with client access managed by the SP typically used for applications such as home hotspot.
roaming	The use of a home network subscription to gain access to a partner network.
sRouter	A Stand-alone Router device that is functionally equivalent to the eRouter except it is operationally independent of the access network. The sRouter is provisioned and managed by the MSO.
service element	A Service Element represents a piece of service functionality that is exposed by a USP Agent, usually represented by one or more data model Objects
standalone Wi-Fi gateway	An integrated sRouter and Wireless Access Point provisioned and managed independently of the access network.
SRV	An SRV record or Service record is a category of data in the Internet Domain Name System specifying information on available services.
TR-069	Term used to refer to the CPE WAN management protocol suite defined in [TR-069]
TR-369	User Services Platmorm (USP) - a major expansion of the TR-069 management protocols and data models.
TR-369 CPE	Term used to refer to the CPE managed using the User Service Platform (USP) specification defined in [TR-369]
USP	User Services Platform (as defined in [TR-369]) is a standardized protocol for managing, monitoring, upgrading, and controlling connected devices
USP Agent	A USP Agent is a USP Endpoint that exposes Service Elements to one or more USP Controllers
USP Controller	A USP Controller is a USP Endpoint that manipulates Service Elements through one or more USP Agents
USP Endpoint	A USP Endpoint is a termination point for a USP Message
USP Message	A USP Message refers to the contents of a USP layer communication including exactly one USP Message header and at most one USP Message body
Wi-Fi GW	Wireless Fidelity Gateway – an integrated embedded Cable Modem, eRouter, and Wireless Access Point

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations.

AP	access point
BSSID	basic service set identifier
CM	cable modem
CRUD	create, read, update, delete
CWMP	CPE WAN Management Protocol
D-ONU	DPoE-capable Optical Network Unit
DOCSIS	Data-Over-Cable Service Interface Specifications
DSCP	differentiated services code points
eDOCSIS	embedded DOCSIS
FCAPS	fault, configuration, accounting, performance and security
GI	guard interval
GW	gateway
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
LED	light emitting diode
MIB	management information base
RRM	radio resource manager
SNMP	Simple Network Management Protocol
SRV	service record
SSID	service set identifier
U-APSD	unscheduled automatic power save delivery
UL	Underwriters Laboratory
USP	user services platform
WDS	wireless distribution system
WEP	wired equivalent privacy
Wi-Fi	wireless fidelity
Wi-Fi AP	wireless fidelity access point
Wi-Fi GW	wireless fidelity gateway
WMM	Wi-Fi multimedia
WPA	Wi-Fi protected access

5 OVERVIEW

The Wi-Fi specification suite defines two types of wireless access gateways—-the Wi-Fi Gateway and the Stand-alone Wi-Fi Gateway. The Wi-Fi Gateway integrates a Wi-Fi air interface access with the cable network (i.e., cable modem) and a router. The Stand-alone Wi-Fi Gateway is decoupled from the access network (e.g., DOCSIS) by removing the cable modem. This specification provides the provisioning and management frameworks for both the Wi-Fi Gateway and Stand-alone Wi-Fi Gateway devices. The Wi-Fi Gateway interface and routing functionality is described in the CableLabs eRouter Specifications. The Standalone Gateway interface and routing functionality is defined in a separate Stand-alone Router specification [sRouter] and based on the eRouter document. The TR-069 CWMP requirements apply to the eRouter and the sRouter gateways. The TR-369 USP requirements apply only to the eRouter gateway.

This specification is focused on management requirements for Wi-Fi interface. The management features include user activation of the AP, user access via the AP, user selection of the network name, Service Set Identifier (SSID), user activation of Security settings, MSO activation of the AP, MSO configuration of an SSID for public usage, and MSO configuration of security on AP. Performance report requirements are driven by operator needs and features widely available in the Wi-Fi industry.

APs can report multiple performance parameters based on the signal strength received from a device, packets sent/received, user authentication, SSID, and QoS. These are required to be monitored for health of the AP, status of the Wi-Fi environment and to provide usage statistics to management entities. TR-x69 and/or SNMP protocols are used to communicate parameters.

The Wi-Fi Gateway AP is often configured through a CM configuration file using the TLV202 family of TLVs defined in the eDOCSIS specification [eDOCSIS]. Additionally, the Wi-Fi Gateways support SNMP, TR-069, and TR-369 management protocols for configuration and management purposes on device initialization and after the device has become operational. This specification does not address range extenders with integrated Wi-Fi Gateway. The Stand-alone Wi-Fi Gateway is configured through a combination of DHCP options and the applicable management protocol—TR-x69 and optionally SNMP. In the Stand-alone Wi-Fi Gateway, the AP is configured and managed via the Operator-Facing Interface, using TR-069 and optionally, SNMP.

This specification defines the data requirements for the functional areas of operations (Fault, Configuration, Accounting, Performance and Security). The provisioning of the Wi-Fi aspects is tied to the provisioning and management process associated with the device hosting the Wi-Fi interfaces. Therefore, this specification considers a generic data model of the management requirements. Unless otherwise specified, the requirements herein apply to both the Wi-Fi Gateway and the Stand-alone Wi-Fi Gateway.

Additional management interfaces using alternative protocols can be derived from the object model as needed.

5.1 Wi-Fi Management Features

The Wi-Fi management features are organized based on the management functional areas as shown in Table 1 below.

Table 1 - Wi-Fi Management Features

Feature	Management Functional Area	Description
Air Interface Configuration	Configuration	802.11 Air interface configuration parameters including Channel, modes of operation, rates, transmission power, etc.
SSID configuration	Configuration	Configuration of SSID domains as sub-interfaces for service separation
Capabilities and Supported Features	Configuration	List of Wi-Fi features support
Access Protection configuration	Configuration	Configuration of Access mechanisms including WEP (Wired Equivalent Privacy, WPA (Wi-Fi Protected Access), and WPA2
Resource And Traffic Priority	Configuration	Assignment of VLANs to SSIDs for traffic prioritization

Feature	Management Functional Area	Description
Device operations	Configuration	Reset Air interface Factory default set Interfaces enabled during outages
Power Saving Status	Configuration, Performance	Configuration and status report of Power Saving
Current transmit power and RSSI (Received Signal Strength Indication)	Performance	Report of Air interface metrics that lead into measure robustness and link quality
Operational Status	Configuration	Active antenna selections Current channel sections Total active associations
Performance Metrics	Performance	Report of Frames and packets counts to measure errors and failed conditions
Logging and Alerting	Fault	The record and reporting of fault conditions
Diagnostic procedures	Fault	Procedures used to collect health status to help diagnose faults
Local CPE access configuration	Configuration	CPE MAC restriction
AAA Radius Client	Security, Accounting	Client capabilities to help support authentication and accounting procedures with a network AAA server
Access Configuration	Security	GUI access and restriction to other groups (SSID domains)
Radio Resource Management	RRM	Wi-Fi GW data items to be read or set by the SON (self-organizing network) controller
Public access and roaming	Public Wi-Fi Management	Configuration of access and roaming mechanisms utilizing home Wi-Fi
Parental Controls	Access Control	Configure Access and authorization of managed devices
WiFi Data Elements	Configuration Performance	Manage multiple Access Point devices

5.1.1 Configuration Management

Cable operators can configure SSIDs to be subscriber or operator managed. The user may be allowed to configure basic wireless settings such as SSID name, security options and passphrase through device admin pages. The operator will maintain exclusive control of any Public SSIDs.

Operators can manage and configure public and private SSIDs using CM configuration files, TR-x69 or SNMP.

5.1.2 Performance Management

The device configuration is persistent. The Wi-Fi configuration has to be accessible across power cycles. The device will provide an option for the MSO to poll and acquire the performance parameters defined in [TR181-Ext].

5.1.3 Fault Management

The device will provide timely alarms for any internal failures such as radio strength failure or when operating on battery such that not all end devices can be served. The device will maintain the logs on its internal web server page to provide the information related to reboots, configuration changes, intruder detection.

5.1.4 Accounting Management

The device can report usage to an AAA server if it is configured to execute RADIUS accounting client functions.

5.1.5 Security Management

The device needs to support general Wi-Fi security such as WEP, WPA-PSK, WPA2, WPA3 for secure access of the Wi-Fi network. The manufacturer configuration provides default security settings. MAC address based Wi-Fi access configuration may be allowed on the subscriber controlled SSID. This helps the end user to control the devices that are attached to gateway using user defined SSID.

The device will provide the AAA server address to all incoming requests. The incoming requests may be directed to access control web page defined by MSO. This helps the roaming devices to get authenticated on MSO network.

5.1.6 Radio Resource Management

The device can report RRM-related parameters to the SON controller (read parameters), and allow some RRM-related parameters to be set by the SON controller (write parameters).

5.1.7 Public Wi-Fi Management

The gateway may support Community Wi-Fi, which allows unused bandwidth be publicly available to roaming users. The gateway can support Hotspot 2.0 (aka Passpoint) a feature that enables a mobile device owner to seamlessly access multiple Service Provider Wi-Fi networks. Network discovery, registration, provisioning, and access processes are automated to create a seamless user experience when roaming.

5.2 Object Model

The Wi-Fi GW requirements contained in this specification are focused on the wireless access and bridging requirements of [802.11] interfaces. However, there are dependencies and relationships with the features offered by the device supporting the Wi-Fi interface; for example, support of NAT, routing, bridging, tunneling and multiple user domains based on SSIDs. These aspects require visualization and integration of the MAC and IP layer features of the device to transport user data.

5.3 Wi-Fi Management Interfaces

Figure 1 and Figure 2 below show examples of Wi-Fi Management on a device within the context of the Wi-Fi GW management interfaces. In Figure 1, the CM supports Wi-Fi as part of its LAN facing CPE interfaces. In Figure 2, eRouter is the device supporting the Wi-Fi interfaces. Note the nomenclature of provisioning and management interfaces in this section is informative and not defined in [MULPIv3.0] or [eRouter] specifications. The data elements provided by the object model defined in this specification can be provisioned, configured and monitored via the management interfaces listed in Figure 1 and Figure 2 as described on each interface definition below.

Figure 1 shows the management interfaces for the CM (managed device).

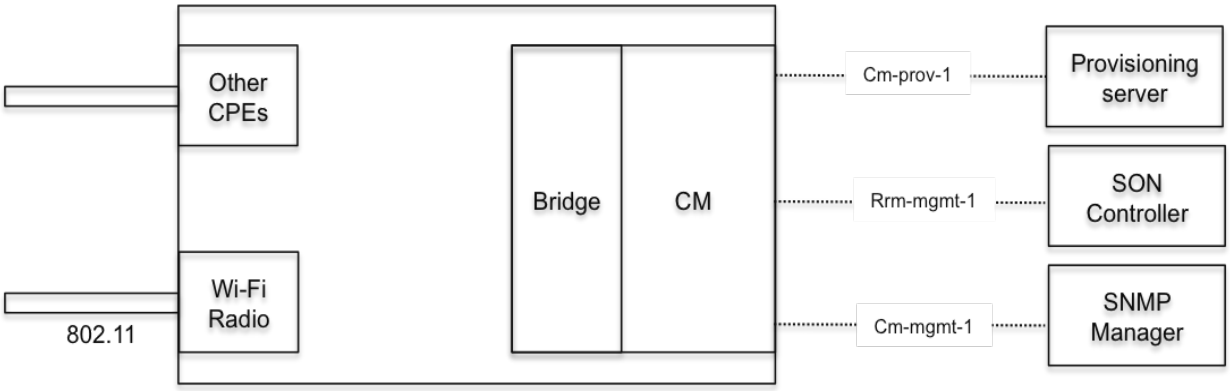

Figure 1 - CM Provisioning and Management Interfaces

5.3.1 Cm-prov-1

This interface provides DHCP and FTP to the CM for provisioning and configuration at initialization. The configuration file provides the attributes to initialize and configure the Wi-Fi interfaces.

5.3.2 Cm-mgmt-1

This interface corresponds to the management interface for operational CMs. Wi-Fi interface attributes and parameters can be monitored and updated through this interface. The implementation is vendor-specific and is not defined in this document.

5.3.3 Rrm-mgmt-1

This interface allows the SON controller to read or set parameters in the Wi-Fi GW that are related to the Wi-Fi RRM.

Figure 2 shows the management interfaces for the eRouter (managed device).

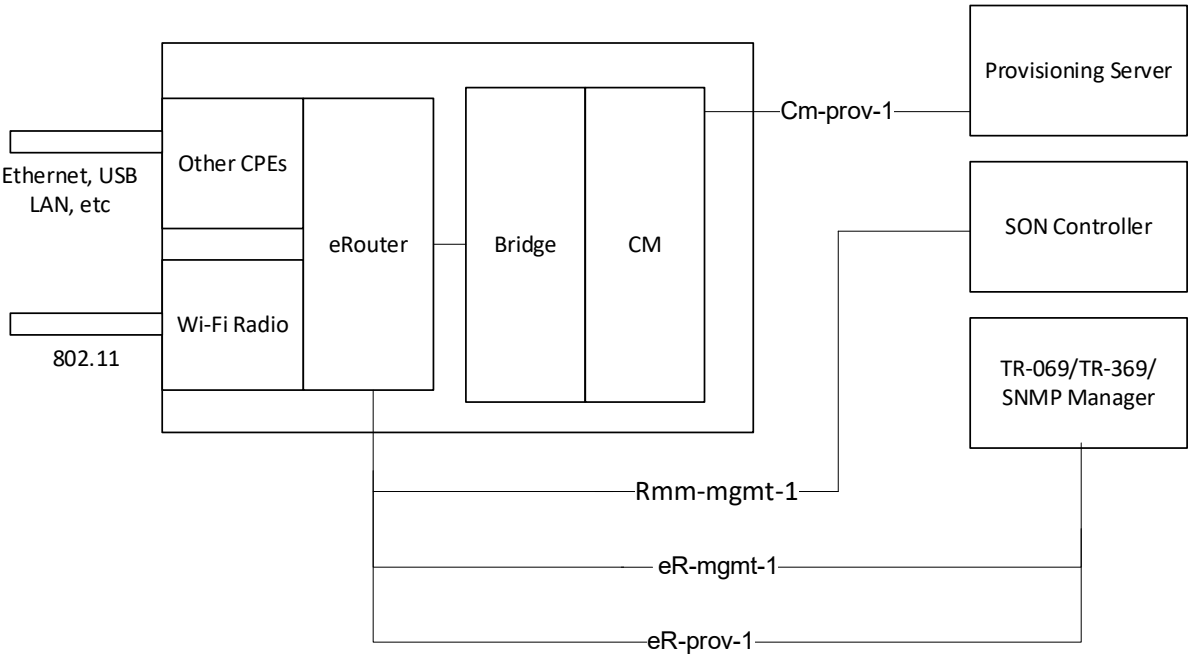

Figure 2 - eRouter Provisioning and Management Interfaces

5.3.4 Cm-prov-1

This is the same interface seen in Figure 1. In the context of eRouter this interface provides a mechanism to pass the eRouter (including Wi-Fi interface parameters) configuration parameters via the CM configuration file to the eRouter device. The DHCP functions are limited to the eCM component. See [eRouter] for details.

5.3.5 eR-prov-1

This interface provides DHCP to the eRouter component.

5.3.6 eR-mgmt-1

This interface corresponds to the management interface for operational eRouter. Wi-Fi interface attributes and parameters can be monitored and updated through this interface.

5.3.7 Rrm-mgmt-1

This interface allows the SON controller to read or set parameters in Wi-Fi Gateway that are related to the Wi-Fi Radio Resource Manager (RRM).

Figure 3 below is an example of Wi-Fi Management of a device within the context of the Stand-alone Wi-Fi Gateway management interfaces. The Stand-alone Router is the device supporting the Wi-Fi interfaces. Note the nomenclature of provisioning and management interfaces in this section is informative. The data elements provided by the object model defined in this specification can be provisioned, configured and monitored via the management interfaces listed in Figure 3.

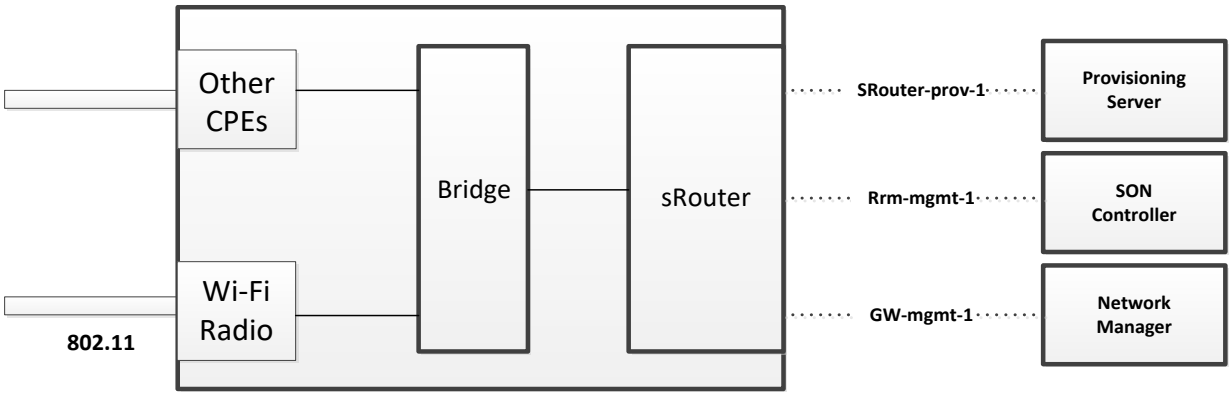

Figure 3 - sRouter Provisioning and Management Interfaces

5.3.8 sRouter-prov-1

This interface provides DHCP for provisioning and configuration at initialization.

5.3.9 Rrm-mgmt-1

This optional interface allows the SON controller to read or set parameters in the Wi-Fi GW that are related to the Wi-Fi RRM.

5.3.10 GW-mgmt-1

This interface corresponds to the management interface for operational sRouter. Wi-Fi interface attributes and parameters can be monitored and updated through this interface.

6 REQUIREMENTS

This section contains normative management requirements on the Wi-Fi GW management interface. Unless otherwise noted, the term "The Gateway" refers to the Wi-Fi Gateway and the Stand-alone Gateway.

6.1 Object Model Requirements

Annex A defines the Wi-Fi GW object model in a protocol independent way. Object definitions for SNMP, TR-069, and TR-369 management protocols are derived or related to the object model in Annex A.

The Gateway MUST support the object model defined in Annex A.

The object model in Annex A is based on [TR-181i2], specifically, the [TR-181i2] Device. Wi-Fi objects provide the basis of the Wi-Fi Physical interface requirements for the Wi-Fi GW. Other aspects of [TR-181i2] such as device level management, other than Wi-Fi physical interfaces, IP networking, and Applications and protocols management are beyond the scope of this specification. Refer to [eRouter] specification for object model requirements at the Gateway level.

6.1.1 IEEE 802.11 MIB Modeling Considerations

The IEEE 802.11 MIB module [802.11] does not provide a view of the configuration elements expected for device level management, but focuses on the lower level protocol primitives needed to configure the MAC and PHY layers. Therefore, the [TR-181i2] model is more appropriate for Wi-Fi management. The optional 802.11 MIB requirements are summarized in Annex A.

6.1.2 Wi-Fi Interface Model

This section details the Wi-Fi interface management requirements to accomplish separation and isolation of user domain traffic. The requirements in this section are driven by cable operator deployment models. The data models leverage design considerations from [TR-181i2]. User domains in Figure 4 below refer to the IP Forwarding layer defined in this model for traffic isolation between SSID domains. The forwarding model is outside the scope of this specification and is detailed in [eRouter] and [sRouter].

For example, a residential user resides in the Residential Domain where LAN hosts (wired and wireless) are in the same network. Public Domain represents Internet with wireless access using an SSID other than the Residential Domain. Similarly, a Roaming Domain supports subscribers from a partner network with a roaming contract. A separate SSID is designated for roaming.

Public, Residential and Roaming Domain subscribers are attached to the same Wi-Fi radio. Thus, an interface hierarchy from layer 1 through layer 3 is needed to accomplish user domain traffic isolation. [TR-181i2] defines SSIDs as logical interfaces on top of the Wi-Fi radio. Traffic marking can be achieved by layering Bridging and VLAN connections on top of SSID interface; traffic isolation is reached by layering IP Interfaces on top of bridges down to the SSID domains accompanied by traffic forwarding rules. The SSID Domain is further modeled in [TR-181i2] as part of Virtual Access Points. The Virtual Access Points are isolated from each other by means of the IP interface and Bridge configuration. See details in [sRouter].

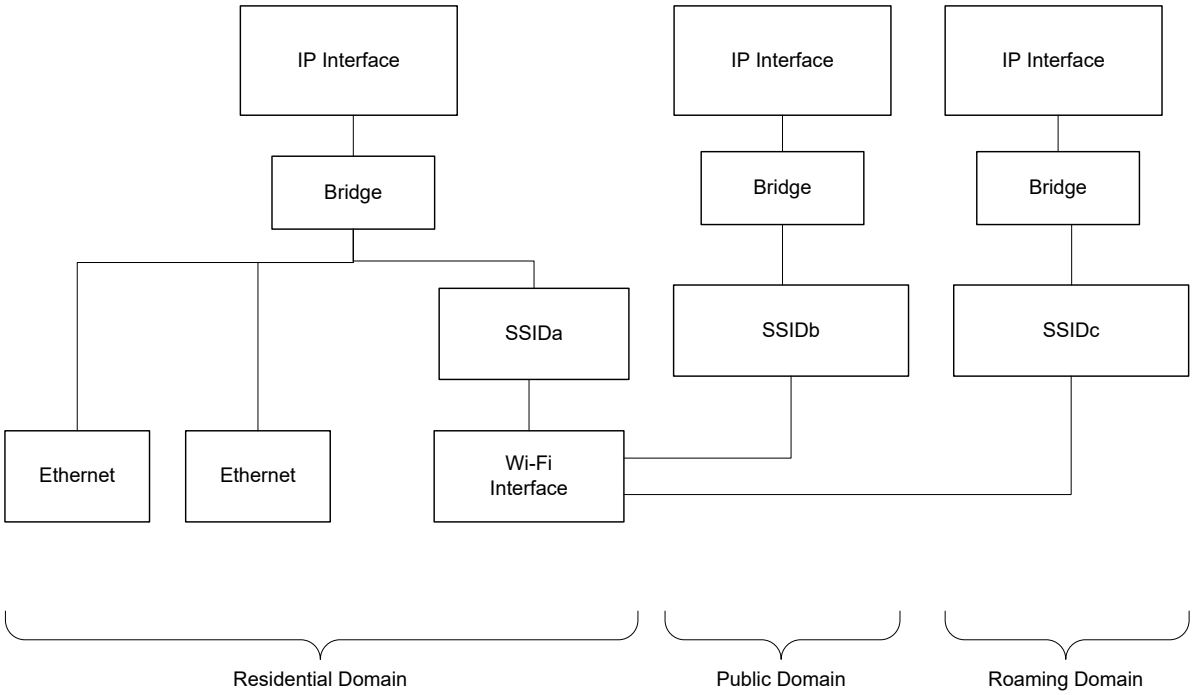

Figure 4 - Example User Domain Interface Model

Figure 4 also shows an example of a user domain configuration. This example is only meant to be representative and is not a requirement. By default Ethernet ports are always associated with the subscriber domain, as part of same domain there is an SSID logical interface (SSIDa). Public and Roaming domain configurations are shown as well.

6.2 Management Interface Protocols Requirements

6.2.1 Requirements for SNMP Protocol

The Gateway requirements reside in a managed device (e.g., [eRouter] or [sRouter]). The Gateway that supports the SNMP interface MUST support the MIB objects listed in Table 2 and defined in [CLAB-WIFI-MIB]. Table 2 shows the mapping between the objects of the object model in and their SNMP MIB objects [CLAB-WIFI-MIB]. If the device implements the functionality represented by an Object Model listed in Table 2, it MUST instantiate the MIB object(s) as defined in this specification.

Table 2 - SNMP Object Requirements

Object Model	SNMP MIB Object	Requirement
Based on [TR-181i2] and CableLabs extensions		
DeviceDeviceInfo	clabGWDeviceDeviceInfo	MUST
WiFi	clabWIFIBase	MUST
Radio	clabWIFIRadioTable	MUST
RadioStats	clabWIFIRadioStatsTable	MAY
RadioStats	Counters from ifTable and ifXTable [RFC 2863]	MUST
NeighboringWiFiDiagnostic	clabWIFINeighboringWiFiDiagnostic	SHOULD
NeighboringWiFiDiagnosticResult	clabWIFINeighboringWiFiResultsTable	SHOULD
SSID	clabWIFISSIDTable	MUST
SSIDStats	clabWIFISSIDStatsTable	MUST
AccessPoint	clabWIFIAccessPointTable	MUST

Object Model	SNMP MIB Object	Requirement
AccessPointSecurity	clabWIFIAccessPointsecurityTable	MUST
AccessPointWPS	clabWIFIAccessPointWPSTable	MUST
AssociatedDevice	clabWIFIAssociatedDeviceTable	MUST
EndPoint	Not defined	-
EndPointSecurity	Not defined	-
Profile	Not defined	-
ProfileSecurity	Not defined	-
EndPoint PWS	Not defined	-
InterfaceStack`	IfStackTable [RFC 2863]	-
AC	clabWIFIAccessPointACTable	MUST
ACStats	clabWIFIAccessPointACStatsTable	MUST
Accounting	clabWIFIAccessPointAccountingTable	SHOULD
CableLabs Extensions to [TR-181i2]		
ChannelWiFiDiagnostic	clabWiFiChannelWiFiDiagnostics	SHOULD
ChannelWiFiDiagnosticResult	clabWiFiChannelWiFiDiagnosticsResult	SHOULD
AccessControlFilter	clabWIFICableAccessControlFilter	SHOULD
AccessControlFilterTable	clabWIFICableLabsAccessControlFilterTable	SHOULD
InterworkingService	clabWIFIAccessInterworkingService	CONDITIONAL MUST
Passpoint	clabWIFIPasspointTable	CONDITIONAL MUST
PasspointVenueNames	clabWIFIPasspointVenueNamesTable	CONDITIONAL MUST
PasspointOperatorNames	clabWIFIPasspointOperatorNamesTable	CONDITIONAL MUST
PasspointThreeGPPNetwork	clabWIFIThreePasspointThreeGPPNetworkTable	CONDITIONAL MUST
PasspointDomainNames	clabWIFIPasspointDomainNames	CONDITIONAL MUST
PasspointConsortium	clabWIFIPasspointConsortiumTable	CONDITIONAL MUST
PasspointNAIRealms	clabWIFIPasspointNAIRealmsTable	CONDITIONAL MUST
PasspointNAIRealmsEAPMethods		
PasspointNAIRealmsSupportedEAPListAuth Parameters		
PasspointOSUProviders	clabWIFIPasspointOSUProvidersTable	CONDITIONAL MUST
PasspointOSUProvidersNames		
PasspointOSUProvidersIcons		
PasspointOSUProvidersServiceDescriptions		
PeriodicStats	clabWIFIPeriodicStatsTable	MAY
SSIDPolicy	clabWIFISSIDPolicyTable	MAY
ClientSessions	clabWIFIClientSessionsTable	MAY
ClientStats	clabWIFIClientStatsTable	MAY
RadiusClient	clabWIFIRadiusClientTable	MAY
EventNotif	clabWIFIEventNotif	MAY
	clabWIFIInterfaceStack	MAY
Not in Annex A object model (see InterfaceStack [TR-181i2])	ifStackStatusTable [RFC 2863]	MUST
RadiusSettings	clabWIFIAccessPointRadiusSettingsObjects	MUST

The mapping between the SNMP requirements listed in Annex A and the requirements in [802.11] is not completely one-to-one. Below are a few examples:

- The [TR-181i2] Device.WiFi.Radio object reuses most attributes from the IF-MIB [RFC 2863] ifTable, ifXTable and ifStackStatusTable. However, the attributes are arranged differently in Table 2.
- Interface counters at the PHY layer overlap. In this case, the preferred model of reporting is the conventional [RFC 2863].
- The IF-MIB does not define an interface type for the SSID layer defined in [TR-181i2].
- Extended statistics and roaming authentication are not part of [TR-181i2] requirements. Annex A contain those extensions.

6.2.1.1 Interface Creation and IfTable Relationship

The ifTable defined in [RFC 2863] does not provide a method to create new interfaces or logical interfaces on top of the Physical Wi-Fi interfaces such as SSIDs, Bridges and LAN/WAN IP Interfaces. The [TR-181i2] Device WiFi.SSID, Device.Bridging and Device.IP objects define the artifacts to create logical interfaces and their stack relationships. The Gateway MUST support SSID logical interfaces as defined in [TR-181i2] and relies on the GW router to support stacking Bridges and WAN/LAN IP interfaces to define the SSID service topology.

6.2.1.2 Interface Numbering

This specification defines interface numbering for the purpose of creating deterministic configuration and operation procedures. This is similar to the reserved interface numbers found in [OSSIv3.0].

The Gateway MUST allocate the interfaces numbers indicated in Table 3.

Table 3 - Interface Numbering Requirements

Interface Numbers	Purpose
2XX	IP Interfaces in the LAN side
3XX	IP Interfaces in the WAN Side
1XXYY	Wi-Fi interfaces and SSID interfaces • XX corresponds to the Wi-Fi radio Interface with XX in (0..99). • YY corresponds to the SSID logical interfaces for Wi-Fi radio XX with YY in range 1..99 10000 corresponds to the Wi-Fi Radio with ifAlias = wlan0 10001 corresponds to the Wi-Fi SSID sub-interface 1 on Wi-Fi radio 10000 Interface numbering for devices with more of 100 Radios and/or 99 SSID per radio is vendor specific

Other specifications that reference the Wi-Fi Interface requirements need to observe the interface numbering indicated in Table 3.

6.2.1.3 Interface Naming

This specification uses regular, well defined conventions for interface naming. Interface names are typically used in web portals, console ports, etc. Even though this specification follows the CableLabs interface numbering schema for data models, the equivalent text names are explicitly defined to simplify operations. The Gateway MUST follow the interface naming convention listed in Table 4. The Gateway MUST report the interface name in ifName IF-MIB per [RFC 2863].

Table 4 - Interface Naming Requirements

Interface Name (ifName)	Purpose
lan(n)	IP Interfaces in the LAN side (n) is the one or two digit representation of XX in the interface number 2XX ; e.g., lan0

Interface Name (ifName)	Purpose
wan(n)	IP Interfaces in the WAN Side (n) is the one or two digit representation of XX in the interface number 2XX; e.g., wan0
wlan(n).(m)	Wi-Fi interfaces and sub-interfaces (n) corresponds to the one or two digit representation of XX in the interface number 1XXYY (m) corresponds to the one or two digit representation of YY in the interface number 1XXYY For Wi-Fi Interfaces '.(m)' is omitted. Examples: • wlan0 corresponds to ifIndex 10000 • wlan0.1. corresponds to ifIndex 10001

6.2.1.4 Other Interface Requirements

The Gateway MUST support the ifTable parameters listed in Table 5 as specified in [RFC 2863].

Table 5 - ifTable Parameters

Interface Numbers	ifType	ifDescr	Counters
IP Interfaces in the LAN side	ipForward(142)	LAN IP interface	per [RFC 2863]
IP Interfaces in the WAN Side	ipForward(142)	WAN IP interface	per [RFC 2863]
Wi-Fi interfaces	ieee80211(71)	Wi-Fi Radio Interface	per [RFC 2863]
Wi-Fi sub-interfaces	ieee80211(71)	Wi-Fi SSID sub-interface	per [RFC 2863]

The Gateway MUST support the ifTable and ifXtable counters specified in the Interface MIB [RFC 2863] for the Wi-Fi interfaces and sub-interfaces.

6.2.1.4.1 ifStackTable Requirements

The Gateway MUST report read-only instances of the interface stack represented in [RFC 2863].

6.2.1.4.2 IpNetToPhysicalTable Requirements

The ipNetToPhysicalTable is similar to the requirements in the Host object (see Annex A). The Gateway MUST support the IpNetToPhysicalTable. The Gateway SHOULD support the Host and Host objects defined in Annex A.

6.2.1.4.3 Residential Domain Requirements

The Gateway MUST map by default non-Wi-Fi interfaces (e.g., Ethernet, USB LAN device interfaces) to the Wi-Fi Residential domain. However, the Wi-Fi GW MAY allow the configuration of non-Wi-Fi interfaces other than the Wi-Fi Residential Domain via the LANDevice object defined in Annex A.

6.2.2 Requirements for TR-069

The Gateway MUST support the Device.WiFi objects of [TR-181i2] with the exception of the Device.WiFi.EndPoint objects which are optional.

The Gateway MUST support the TR-069 data object extensions defined in [TR181-Ext] based on Annex A.

6.2.3 Requirements for TR-369

The Gateway MUST support the [TR-181i2]. Device.WiFi objects unless explicitly excluded.Wi-Fi Diagnosis

The Gateway MUST adhere to the recommendations for LED (Light Emitting Diodes) operations for LAN CPEs defined in [OSSIv3.0].

6.2.4 Wi-Fi Object Model Compliance Requirements

This section defines minimal compliance requirements for the object model defined in Annex A. Those compliance requirements are then expressed the proper notation of the corresponding management interface (SNMP as defined in Section 6.2.1, [TR-069] per Section 6.2.2) and [TR-369] per Section xxx.

6.2.4.1 Wi-Fi Radio Relation to SSID and AccessPoint Objects

Section 6.2.1 describes the [TR-181i2] generic model for interfaces association. In particular SSIDs can be associated to any available radio. Further, [TR-181i2] defines the mechanism to configure an AccessPoint object by referencing a particular SSID. This section defines implementation requirements to allow static associations of SSIDs to Radio and AccessPoint objects of Annex A.

The Wi-Fi GW MAY predefine AccessPoint and SSID object instances and reject requests for addition and deletion of existing instances.

The Wi-Fi GW MAY define a Wi-Fi instance which is applied to a specific radio, a set of SSIDs and a set of AccessPoints instances. Within a Wi-Fi instance all SSIDs and AccessPoints instances MAY be statically associated with a unique radio instance. For example, one SSID instance MAY not be associated with two radio instances.

The Wi-Fi GW MAY define a static association of each AccessPoint instance with a single SSID instance.

If multiple SSIDs (AccessPoint) are associated with a single radio, the Gateway MAY use the following AccessPoint parameters from the lowest index of the AccessPoint object instances, and reject the sets to those parameters on the other SSID instances; in case the configuration of those parameters is not supported per SSID/AccessPoint.

- WMMEnable attribute
- UAPSDEnable attribute
- WPS object

Table 6 shows the Management interface implications of the requirements above.

Table 6 - Radio, SSID and AccessPoint Objects Minimal Compliance

Requirement	TR-069 Profiles	SNMP Compliance
No AccessPoint and SSID creation and deletion of Instances	WiFiSSID:1 Profile Device.WiFi.SSID.{i}. requirement = "present"	clabWIFISSIDRowStatus Not Implemented
	WiFi AccessPoint:1 Profile Device.WiFi.AccessPoint.{i}. requirement = "present"	clabWIFIAccessPointWPSRowStatus Not Implemented
SSID static association to Radio	WiFiSSID:1 Profile Device.WiFi.SSID.{i}.LowerLayers requirement = "RO"	clabWIFISSIDLowerLayers RO
AccessPoint static association to SSID	WiFi AccessPoint:1 Profile Device.WiFi.AccessPoint.{i}.SSIDReference requirement = "RO"	clabWIFIAccessPointSSIDReference RO

6.2.4.2 Wi-Fi Objects Reduced Compliance Requirements

The Gateway MUST comply as minimum with the conditions specified in Table 7 for the objects therein listed.

Table 7 - Gateway Object Requirements

Requirement	TR-069 Profiles	SNMP Compliance
SSID RW access	WiFiSSID: 1 Profile Device.WiFi.SSID{i} requirement = RW	clabWIFISSIDTable Requirement = RW
AccessPoint RW access	WiFiAccessPoint: 1 Profile Device.WiFi.AccessPoint{i} requirement = RW	clabWIFIAccessPointTable Requirement = RW
AccessPointSecurity RW	WiFiAccessPoint: 1 Profile Device.WiFi.AccessPoint{i}.Security requirement = RW	clabWIFIAccessPointSecurity Table Requirement = RW

Requirement	TR-069 Profiles	SNMP Compliance
SecurityExtension	CableWiFiExtensions:1 Profile Device.WiFi.AccessPoint(i).Security.X_CABLELABS_COM_SecurityExtension requirement = RW	
WiFiCommitSettings	CableWiFiExtensions:1 Profile X_CABLELABS_COM_WIFICommitSettings requirement = RW	Requirement = per Annex A

Annex A Wi-Fi Interface Model

A.1 Object Model Overview

The object model specified here defines capabilities to manage the Wi-Fi air interface for residential, enterprise and public deployments. The model is driven by operator requirements and leverages aspects from [TR-181i2], 802.11 MIBs per [802.11] and [RFC 2863]. Many definitions are taken directly from [TR-181i2] and [802.11]. Whenever the original specs are vague on functionality or behavior, this specification enhances those definitions.

A.2 Object Model Definitions

A.2.1 Object Model Data Types

There are no data types defined for this object model.

A.2.2 Object Model Class Diagram

The Gateway Object model in [TR-181i2] defines four areas:

- The Radio, corresponds to the physical wireless interface.
- The SSID, defines the Wi-Fi Service Set per [802.11].
- The Access Point, defines the administration of an SSID as an individual access point.
- The End Point, defines the management of stations.

This specification does not model the End Point classes and they are deemed optional. In addition, many of the object diagrams contain only the CableLabs' extensions and therefore should be combined with [TR-181i2] when applicable.

A.2.3 Object Model Description

All objects and object attributes defined in the sections that follow MUST be implemented in conformance with descriptions provided below. In the event of conflict between the description provided in [TR-181i2] and the associated description below, the definition provided in this document is authoritative.

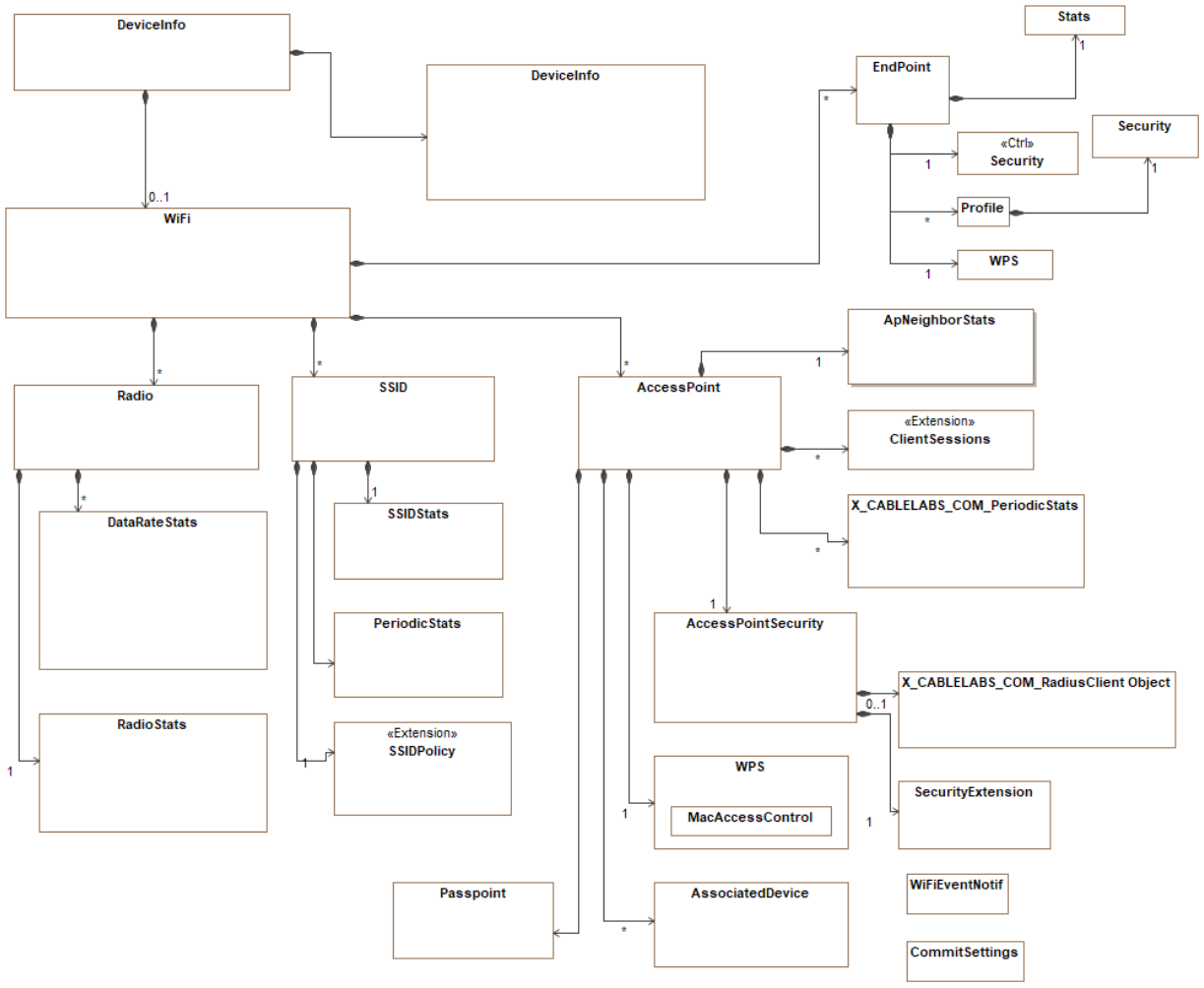

Figure 5 - WiFi Management Object Model

Figure 5 depicts the entire WiFi management object model. Subsequent sections contain the detailed objects and attributes.

A.2.3.1 DeviceInfo Object

This object contains general device information including the WiFi status summary objects.

The DeviceInfo object is defined in [TR-181i2] as Device.DeviceInfo.

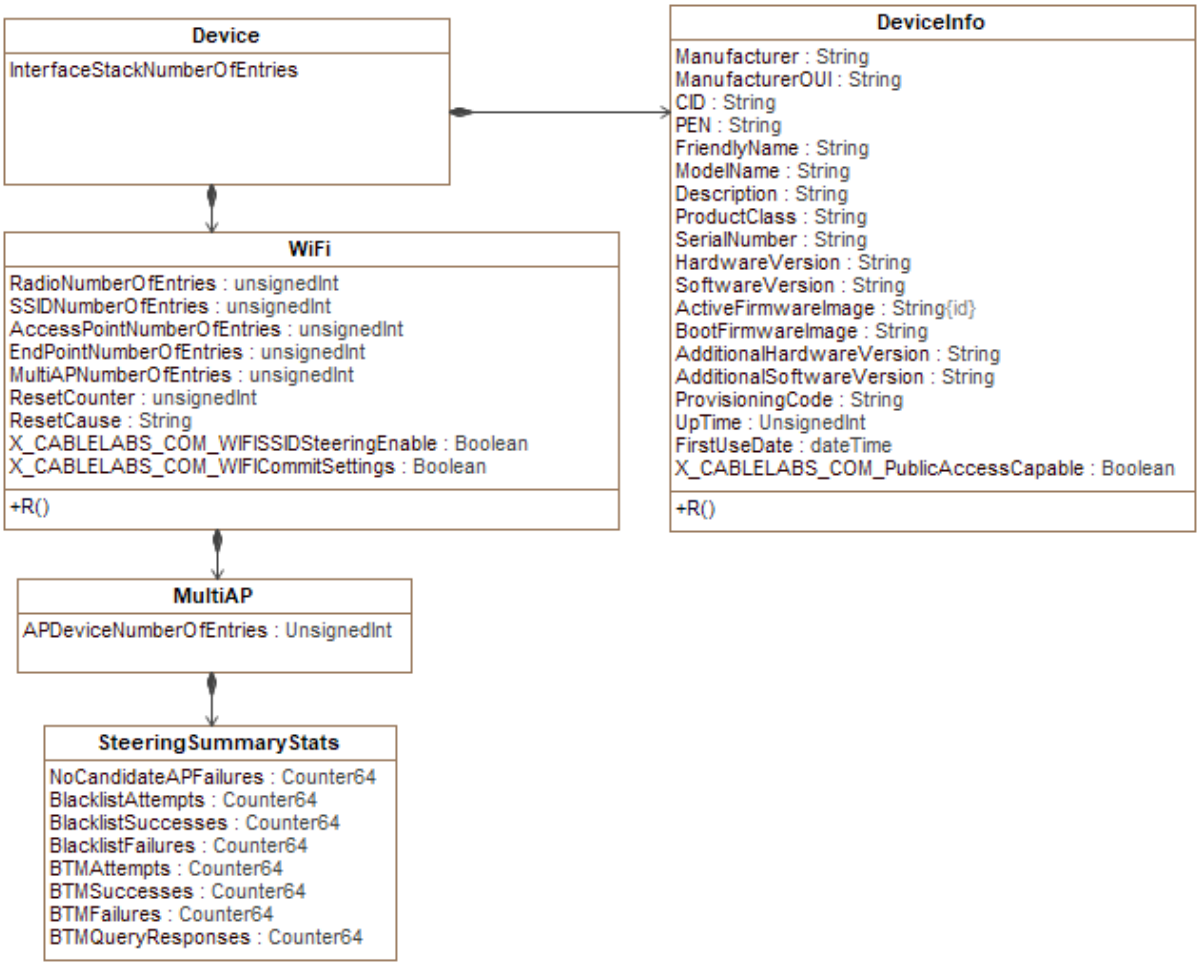

Figure 6 - Device Info

The DeviceInfo object MUST be supported.

Table 8 - Device Info Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Manufacturer	string	RO	SIZE (1..64)			MUST
ManufacturerOUI	string	RO	SIZE (6)			MUST
CID	string	RO	SIZE (6)			MUST
PEN	string	RO	SIZE (10)			MUST
FriendlyName	string	RO	SIZE (32)			MUST
ModelName	string	RO	SIZE (1..64)			MUST
Description	string	RO	SIZE (1..256)			MUST
ProductClass	string	RO	SIZE (1..64)			MUST
SerialNumber	string	RO	SIZE (1..64)			MUST
HardwareVersion	string	RO	SIZE (1..64)			MUST
SoftwareVersion	string	RO	SIZE (1..64)			MUST
ActiveFirmwareImage	string	RO				MUST
BootFirmwareImage	string	RO				MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
AdditionalHardwareVersion	string	RO	SIZE (1..64)			MUST
AdditionalSoftwareVersion	string	RO	SIZE (1..64)			MUST
ProvisioningCode	string	RW	SIZE (1..64)			MUST
UpTime	unsignedInt	RO		seconds		MUST
FirstUseDate	dateTime	RO				MUST
X_CABLELABS_COM_ PublicAccessCapable	boolean	RW	false true		false	MUST

Refer to [TR-181i2] for the definition of the parameters listed in Table 8 above, with the exception of the following CableLabs' extension attribute definitions:

A.2.3.1.1 X_CABLELABS_COM.PublicAccessCapable

This reports Community Public Access capability. This attribute when set to 'true' will indicate that public access is enabled for this device. When set to ‘false’, it indicates public access is disabled for this device.

A.2.3.2 WiFi Object

The WiFi object is based on the Wi-Fi Alliance 802.11 specifications. It defines interface objects, and application objects.

The WiFi object is defined in [TR-181i2] as Device.WiFi.

The WiFi object MUST be supported.

Table 9 - WiFi Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
RadioNumberOfEntries	unsignedInt	RO				MUST
SSIDNumberOfEntries	unsignedInt	RO				MUST
AccessPointNumberOfEntries	unsignedInt	RO				MUST
EndPointNumberOfEntries	unsignedInt	RO				MUST
ResetCounter	unsignedInt	RO				MUST
ResetCause	string	RO	HostReinit(1), Spontaneous Interrupt(2), LossOfPower(3)			MUST
X_CABLELABS_COM_WIFISSID SteeringEnable	boolean	RW	false true		false	MUST
X_CABLELABS_COM_WIFICom mitSettings	boolean	RW	false true		false	MUST

Refer to [TR-181i2] for definitions associated with the parameters listed in Table 9 above, with the exception of the following CableLabs' extension attribute definitions described below:

A.2.3.2.1 WIFICommitSettings

When this attribute is set to 'true', the current Wi-Fi radio interface settings stored in non-volatile memory are discarded, reinitializing the Wi-Fi radio interfaces with a new set of values without requiring a device reboot.

This attribute reports a value of 'false' when the Wi-Fi attributes have been changed, but the changes are not yet active (i.e., not discarded from non-volatile memory and not yet part of the active configuration). Systems that implement immediate commit of the configuration upon change of any attribute will always report this attribute as 'true', and will silently acknowledge SNMP SET-REQUESTS with 'true'.

A.2.3.3 WiFi DataElements Object

This object represents a Wi-Fi network that contains multiple Access Points (Multi-AP). It enables programmatic optimization of a multi-AP network by via a Multi-AP Controller.

Table 10 - MultiAP Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
APDeviceNumberOfEntries	unsignedInt	RO				MUST

A.2.3.3.1 APDeviceNumberOfEntries

Reports the number of entries in the APDevice Table.

A.2.3.4 WiFi MultiAP Steering Summary Stats Object

This object represents a Wi-Fi network that contains multiple Access Points (Multi-AP). It enables programmatic optimization of a multi-AP network via a Multi-AP Controller.

Table 11 - SteeringSummaryStats

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
NoCandidateAPFailures	unsignedLong	RO				MUST
BlacklistAttempts	unsignedLong	RO				MUST
BlacklistSuccesses	unsignedLong	RO				MUST
BlacklistFailures	unsignedLong	RO				MUST
BTMAttempts	unsignedLong	RO				MUST
BTMSuccesses	unsignedLong	RO				MUST
BTMFailures	unsignedLong	RO				MUST
BTMQueryResponses	unsignedLong	RO				MUST

A.2.3.4.1 NoCandidateAPFailures

Reports the number of times Associated Devices should have been steered but weren't because a better candidate AP couldn't be found.

A.2.3.4.2 BlacklistAttempts

Reports the number of times an attempted Blacklist steer was attempted.

A.2.3.4.3 BlacklistSuccesses

Reports the number of times an attempted Blacklist steer succeeded.

A.2.3.4.4 BlacklistFailures

Reports the number of times an attempted Blacklist steer failed.

A.2.3.4.5 BTMAttempts

Reports the number of times a BTM steer was attempted.

A.2.3.4.6 BTMSuccesses

Reports the number of times a BTM steer succeeded.

A.2.3.4.7 BTMFailures

Reports the number of times a BTM steer failed.

A.2.3.4.8 BTMQueryResponses

Reports the Number of asynchronous BTM (BSS Transition Management; 802.11k) Queries for which a BTM Request was issued..

A.2.3.5 Radio Objects

This object represents 802.11 radio(s) in the gateway.

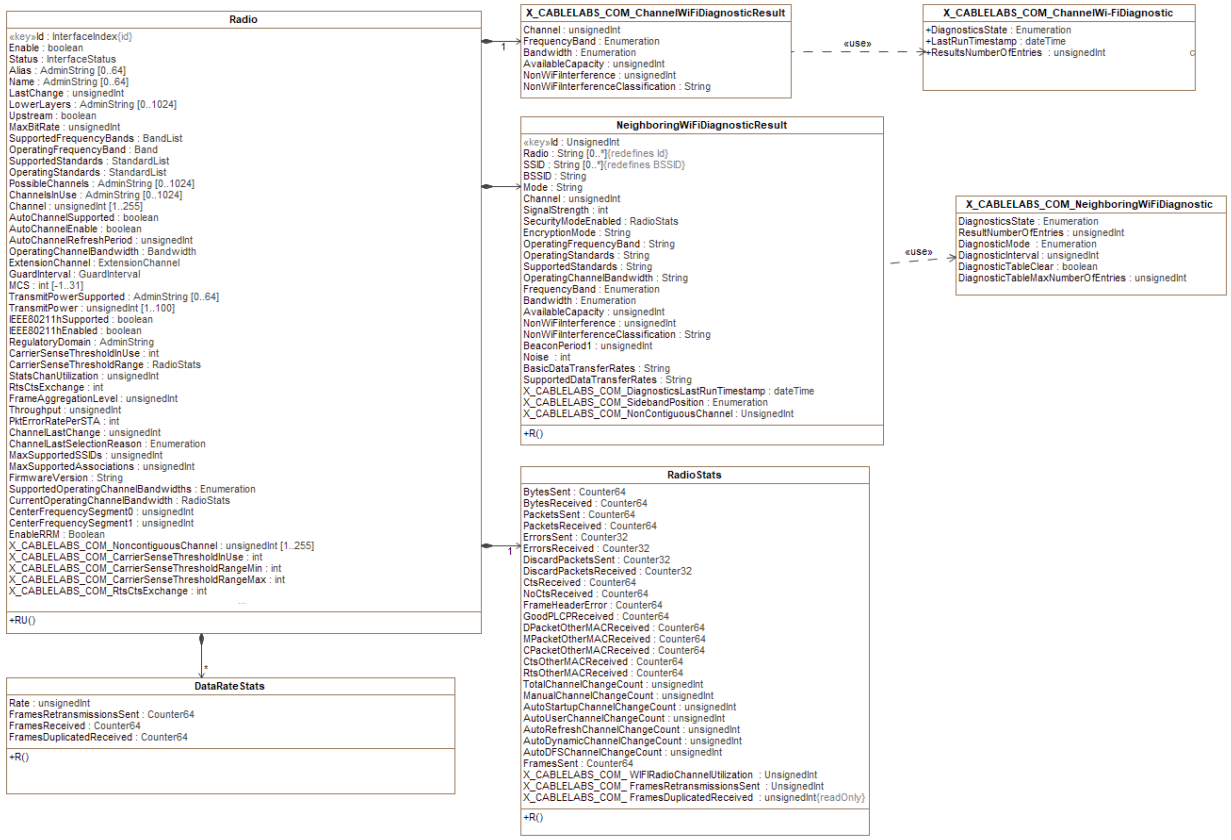

Figure 7 - Radio Object Model Class Diagram

The Radio object is defined in [TR-181i2] as Device.WiFi.Radio{i}.

The Radio object MUST be supported.

Table 12 - Radio Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Id	InterfaceIndex	key				MUST
Enable	boolean	RW				MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Status	enum	RO	up(1), down(2), unknown(4), dormant(5), notPresent(6), lowerLayerDown(7), error(8)			MUST
Alias	string	RW	SIZE (0..64)			MUST
Name	string	RO	SIZE (0..64)			MUST
LastChange	unsignedInt	RO		seconds		MUST
LowerLayers	string	RW	SIZE (0..1024)			MUST
Upstream	boolean	RO	false true			MUST
MaxBitRate	unsignedInt	RO		Mbps		MUST
SupportedFrequencyBands	string	RO	2.4GHz(1), 5GHz(2)	GHz	N/A	MUST
OperatingFrequencyBand	enum	RW	2.4GHz(1), 5GHz(2)	GHz		MUST
SupportedStandards	string	RO	a(1), b(2), g(3), n(4), ac(5)			MUST
OperatingStandards	enum	RO	a(1), b(2), g(3), n(4), ac(5), ax(6)			MUST
PossibleChannels	string	RO	SIZE (0..1024)			MUST
ChannelsInUse	string	RO	SIZE (0..1024)			MUST
Channel	unsignedInt	RW	1..255			MUST
AutoChannelSupported	boolean	RO	false true			MUST
AutoChannelEnable	boolean	RW	false true			MUST
AutoChannelRefreshPeriod	unsignedInt	RW		seconds		MUST
ChannelLastChange	unsignedInt	RO		seconds		MUST
ChannelLastSelectionReason	enum	RO	Manual Auto_Startup Auto_User Auto_Refresh Auto_Dynamic Auto_DFS Unknown			MUST
MaxSupportedSSIDs	unsignedInt-[1:]	RO				MUST
MaxSupportedAssociations	unsignedInt [1:]	RO				MUST
FirmwareVersion	string-(64)	RO				MUST
SupportedOperatingChannel Bandwidths	enum	RO				MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
OperatingChannelBandwidth	enum	RW	20MHz(1), 40MHz(2), 80MHz(3), 160MHz(4), 80+80MHz, auto(5)	MHz	auto	MUST
CurrentOperatingChannel Bandwidth	string					MUST
ExtensionChannel	enum	RW	aboveControlChannel(1), belowControlChannel(2), auto(3)		auto	MUST
GuardInterval	enum	RW	400nsec(1), 800nsec(2), auto(3)		auto	MUST
CenterFrequencySegment0	unsignedInt	RW				
CenterFrequencySegment1	unsignedInt	RW				
MCS	Int	RW	-1..15, 16..31			MUST
TransmitPowerSupported	string	RO	SIZE (0..64)			MUST
TransmitPower	int	RO	-1..100	percent age		MUST
IEEE80211hSupported	boolean	RO	false true			MUST
IEEE80211hEnabled	boolean	RW	false true			MUST
RegulatoryDomain	string	RW	SIZE (3)			MUST
RetryLimit	unsignedInt	RW	0..7			MAY
CCARequest	hexBinary	RW	SIZE (11)			MAY
CCAReport	hexBinary	RO	SIZE (12)			MAY
RPIHistogramRequest	hexBinary	RW	SIZE (11)			MAY
RPIHistogramReport	hexBinary	RO	SIZE (19)			MAY
FragmentationThreshold	unsignedInt	RW		octets		MAY
RTSThreshold	unsignedInt	RW		octets		MAY
LongRetryLimit	unsignedInt	RW				MAY
BeaconPeriod	unsignedInt	RW	1..65535	millisec onds		MUST
DTIMPeriod	unsignedInt	RW	1..255			MUST
PacketAggregationEnable	boolean	RW	false true			MUST
PreambleType	enum	RW	short(1), long(2), auto(3)			MUST
BasicDataTransmitRates	string	RW				MUST
OperationalDataTransmit Rates	string	RW				MUST
SupportedDataTransmitRates	string	RO				MUST
EnableRRM	boolean	RW	false true			MUST
X_CABLELABS_COM_Nonco ntiguousChannel	unsignedInt	RW	1..255			SHOULD
X_CABLELABS_COM_Carrier SenseThresholdInUse	Int	RW		dBm		SHOULD
X_CABLELABS_COM_Carrier SenseThresholdRangeMin	Int	RO		dBm		SHOULD

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
X_CABLELABS_COM_CarrierSenseThresholdRangeMax	Int	RO		dBm		SHOULD
X_CABLELABS_COM_RtsCtsExchange	Int	RW		bytes		SHOULD

Refer to [TR-181i2] for definitions of the parameters listed in Table 12 above, with the exception of the following CableLabs' extension attribute definitions:

A.2.3.5.1 NoncontiguousChannel

This attribute is only applicable to 80+80 MHz channels. It sets the second 80 MHz channel that does not contain the primary channel indicated by the Channel parameter.

A.2.3.5.2 CarrierSenseThresholdInUse

This attribute indicates the RSSI signal level at which CS/CCA detects a busy condition. This attribute enables APs to increase minimum sensitivity to avoid detecting busy condition from multiple/weak Wi-Fi sources in dense Wi-Fi environments.

A.2.3.5.3 CarrierSenseThresholdRangeMin

This attribute indicates the minimum Carrier Sense Threshold level supported by the radio.

A.2.3.5.4 CarrierSenseThresholdRangeMax

This attribute reports the maximum Carrier Sense Threshold level supported by the radio.

A.2.3.5.5 RtsCtsExchange

This attribute allows configuring the RTS/CTS parameters.

A.2.3.6 RadioStats Object

Packet throughput statistics for this interface.

The RadioStats object is defined in [TR-181i2] as Device.WiFi.Radio{i}.Stats.

The RadioStats object MUST be supported.

StatsCounter64: This data type SHOULD be used for all statistics parameters whose values might become greater than the maximum value that can be represented as an unsignedInt. The maximum value that can be represented as an unsignedLong (i.e. 0xffffffffffffffff) indicates that no data is available for this parameter.

Table 13 - RadioStats Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
BytesSent	unsignedLong	RO		bytes		MUST
BytesReceived	unsignedLong	RO		bytes		MUST
PacketsSent	unsignedLong	RO				MUST
PacketsReceived	unsignedLong	RO				MUST
ErrorsSent	unsignedInt	RO				MUST
ErrorsReceived	unsignedInt	RO				MUST
DiscardPacketsSent	unsignedInt	RO				MAY
DiscardPacketsReceived	unsignedInt	RO				MAY
PLCPErrorCount	unsignedInt	RO				MAY

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
FCSErrorCount	unsignedInt	RO				MAY
InvalidMACCount	unsignedInt	RO				MAY
PacketsOtherReceived	unsignedInt	RO				MAY
Noise	int	RO		dBm		MAY
CtsReceived	unsignedLong	RO	StatsCounter64			MAY
NoCtsReceived	unsignedLong	RO	StatsCounter64			MAY
FrameHeaderError	unsignedLong	RO	StatsCounter64			MAY
GoodPLCPReceived	unsignedLong	RO	StatsCounter64			MAY
DPacketOtherMACReceived	unsignedLong	RO	StatsCounter64			MAY
MPacketOtherMACReceived	unsignedLong	RO	StatsCounter64			MAY
CPacketOtherMACReceived	unsignedLong	RO	StatsCounter64			MAY
CtsOtherMACReceived	unsignedLong	RO	StatsCounter64			MAY
RtsOtherMACReceived	unsignedLong	RO	StatsCounter64			MAY
TotalChannelChangeCount	unsignedInt	RO				MAY
ManualChannelChangeCount	unsignedInt	RO				MAY
AutoStartupChannelChangeCount	unsignedInt	RO				MAY
AutoUserChannelChangeCount	unsignedInt	RO				MAY
AutoRefreshChannelChangeCount	unsignedInt	RO				MAY
AutoDynamicChannelChangeCount	unsignedInt	RO				MAY
AutoDFSChannelChangeCount	unsignedInt	RO				MAY
X_CABLELABS_COM_ WIFIRadioChannelUtilization	unsignedInt	RO				MAY
X_CABLELABS_COM_ FramesRetransmissionsSent	unsignedInt	RO				MAY
X_CABLELABS_COM_ FramesDuplicatedReceived	unsignedInt	RO				MAY

Refer to [TR-181i2] for the definitions of the parameters listed in Table 13 above, with the exception of the following CableLabs' extension attribute definitions:

A.2.3.6.1 X_CABLELABS_COM_WIFIRadioChannelUtilization

This attribute reports Wi-Fi Radio Stats Channel Utilization. The fraction of the time AP senses a busy channel or transmits frames. Provides visibility into channel capacity.

A.2.3.6.2 X_CABLELABS_COM_FramesRetransmissionsSent

This attribute indicates the total number of frames retransmitted out of the interface (marked as duplicated). The value of this counter is not expected to be preserved across CPE device reboots.

A.2.3.6.3 X_CABLELABS_COM_FramesDuplicatedReceived

This attribute indicates the total number of duplicated frames received on this interface. The value of this counter is not expected to be preserved across CPE device reboots.

A.2.3.7 X_CABLELABS_COM_ChannelWiFiDiagnostic Object

The X_CABLELABS_COM_ChannelWiFiDiagnostic object is defined as a CableLabs extension to [TR-181i2] as Device. WiFi.Radio.{i}.X_CABLELABS_COM_ChannelWiFiDiagnostic.

The ChannelWiFiDiagnostic object SHOULD be supported.

Table 14 - X_CABLELABS_COM_ChannelWi-FiDiagnostic Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
DiagnosticsState	enum	RW	none(1), requested(2), complete (3), error(4)			SHOULD
LastRunTimestamp	dateTime	RO				SHOULD
ResultsNumberOfEntries	unsignedInt	RO				SHOULD

A.2.3.7.1 DiagnosticsState

Indicates availability of Wi-Fi SSID data.

A.2.3.7.2 LastRunTimeStamp

Indicates the time stamp of the most recently completed diagnostic routine.

A.2.3.7.3 ResultNumberOfEntries

Number of diagnostic result Entries.

A.2.3.8 X_CABLELABS_COM_ChannelWiFiDiagnosticResult Object

The X_CABLELABS_COM_ChannelWiFiDiagnosticResult object is defined as a CableLabs extension to [TR-181i2] as Device.WiFi.Radio.{i}.X_CABLELABS_COM_ChannelWiFiDiagnosticResult.{i}.

The X_CABLELABS_COM_ChannelWiFiDiagnosticResult object SHOULD be supported.

Table 15 - X_CABLELABS_COM_ChannelWiFiDiagnosticResult Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Channel	unsignedInt	RO				SHOULD
FrequencyBand	enum	RO	2.4GHz(1), 5GHz(2)	GHz		SHOULD
Bandwidth	enum	RO	20MHz(1), 40MHz(2), 80MHz(3), 160MHz(4)	MHz		SHOULD
AvailableCapacity	unsignedInt	RO		percentage		SHOULD
NonWiFiInterference	unsignedInt	RO		percentage		SHOULD
NonWiFiInterferenceClassification	string	RO				SHOULD

A.2.3.8.1 Channel

Channel number for which the current row's statistics refers.

A.2.3.8.2 Frequency Band

Indicates the frequency band at which the radio this SSID instance is operating.

A.2.3.8.3 Bandwidth

Indicates the bandwidth at which the channel is operating.

A.2.3.8.4 AvailableCapacity

Percentage of total channel bandwidth available for use.

A.2.3.8.5 NonWiFiInterference

Percentage of total channel bandwidth occupied by non-Wi-Fi interface.

A.2.3.8.6 NonWiFiInterferenceClassification

Comma-separated list of strings. Each list item is an enumeration of: {Microwave, Bluetooth, Radar, Zigbee, etc.}

A.2.3.9 NeighboringWiFiDiagnostic Object

This object reports neighbor information discovered through channel scans.

The NeighboringWiFiDiagnostic object is defined in [TR-181i2] as Device.WiFi.NeighboringWiFiDiagnostic.

The NeighboringWiFiDiagnostic object SHOULD be supported.

Table 16 - NeighboringWiFiDiagnostic Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
DiagnosticsState	enum	RW	none(1), requested(2), completed(3), error(4)			MUST
ResultNumberOfEntries	unsignedInt	RO				MUST
X_CABLELABS_COM_DiagnosticMode	enum	RW	manual(1), interval(2), stop(3),		manual	SHOULD
X_CABLELABS_COM_DiagnosticInterval	unsignedInt	RW	0..1440	seconds	1440	SHOULD
X_CABLELABS_COM_DiagnosticTableClear	boolean	RW				SHOULD
X_CABLELABS_COM_DiagnosticTableMaxNumberOfEntries	unsignedInt	RW				MUST

Refer to [TR-181i2] for the definitions of the parameters listed in Table 16 above, with the exception of the following CableLabs' extension attribute definitions:

A.2.3.9.1 X_CABLELABS_COM_DiagnosticMode

The user may initiate the following diagnostic modes:

Setting to ‘manual' indicates the test will execute one time only.

Setting to ‘interval’ forces the CPE to execute diagnostics at specific intervals specified in seconds.

Setting to ‘stop’ indicates an active interval-mode diagnostic.

A.2.3.9.2 X_CABLELABS_COM_DiagnosticInterval

The interval, in seconds, between channel scans when DiagnosticMode is set to "Interval".

A.2.3.9.3 X_CABLELABS_COM_DiagnosticTableClear

Clears all entries in the NeighboringWiFiDiagnosticResults table.

A.2.3.9.4 X_CABLELABS_COM_DiagnosticTableMaxNumberOfEntries

Maximum number of entries in the table. When the maximum number plus one is reached, the oldest entry, must be deleted.

A.2.3.10 NeighboringWiFiDiagnosticResult Object

This object reports neighbor information known through channel scans.

The NeighboringWiFiDiagnostic object is defined in [TR-181i2] as Device.WiFi.NeighboringWiFiDiagnostic.Results.{i}.

The NeighboringWiFiDiagnosticResult object SHOULD be supported.

Table 17 - NeighboringWiFiDiagnosticResult Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Radio	string	RO				MUST
SSID	string	RO	SIZE (32)			MUST
BSSID	string	RO	SIZE (17)			MUST
Mode	enum	RO	adhoc(1), infrastructure(2)			MUST
Channel	UnsignedInt	RO	1..255			MUST
SignalStrength	int	RO	-200..0			MUST
SecurityModeEnabled	enum	RO	none (1), wep (2), wpa(3), wpa2(4), wpa-wpa2(5), wpa-enterprise(6), wpa2-enterprise (7), wpa-wpa2-enterprise(8) *wpa3-enterprise(9)*			MUST
EncryptionMode	enum	RO	tkip (1), aes(2)			MUST
OperatingFrequencyBand	enum	RO	2.4GHz(1), 5GHz(2)			MUST
SupportedStandards	string	RO	a(1), b(2), g(3), n(5), ac(6), ax(7)			MUST
OperatingStandards	string	RO				MUST
OperatingChannelBandwidth	enum	RO	20MHz(1), 40MHz(2), 80MHz(3), 160MHz(4), auto(6)			MUST
BeaconPeriod	unsignedInt	RO				MUST
Noise	int	RO	-200..0			MUST
BasicDataTransferRates	string	RO	SIZE (256)			MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
SupportedDataTransferRates	string	RO	SIZE (256)			MAY
DTIMPeriod	unsignedInt	RO		ms		MUST
X_CABLELABS_COM_DiagnosticsLastRunTimestamp	dateTime	RO				
X_CABLELABS_COM_SidebandPosition	enum	RO	upper(1), lower(2)			MUST
X_CABLELABS_COM_NonContiguousChannel	unsignedInt	RW	1..255			MAY

Refer to [TR-181i2] for the definition of the parameters listed in 5 above, with the exception of the following CableLabs' extension attribute definitions:

A.2.3.10.1 X_CABLELABS_COM_DiagnosticsLastRunTimestamp

Date and time representing the last time these diagnostics were run.

A.2.3.10.2 X_CABLELABS_COM_SidebandPosition

The position of the sideband in case the bandwidth of the measured service set is 40 MHz. 1 - upper, 2 - lower.

A.2.3.10.3 X_CABLELABS_COM_NonContiguousChannel

This attribute is only applicable to 80+80MHz channels. It sets the second 80MHz channel that does not contain the primary channel indicated by the Channel attribute.

A.2.3.11 SSID Object

The object describes each SSID and its associated statistics and policy.

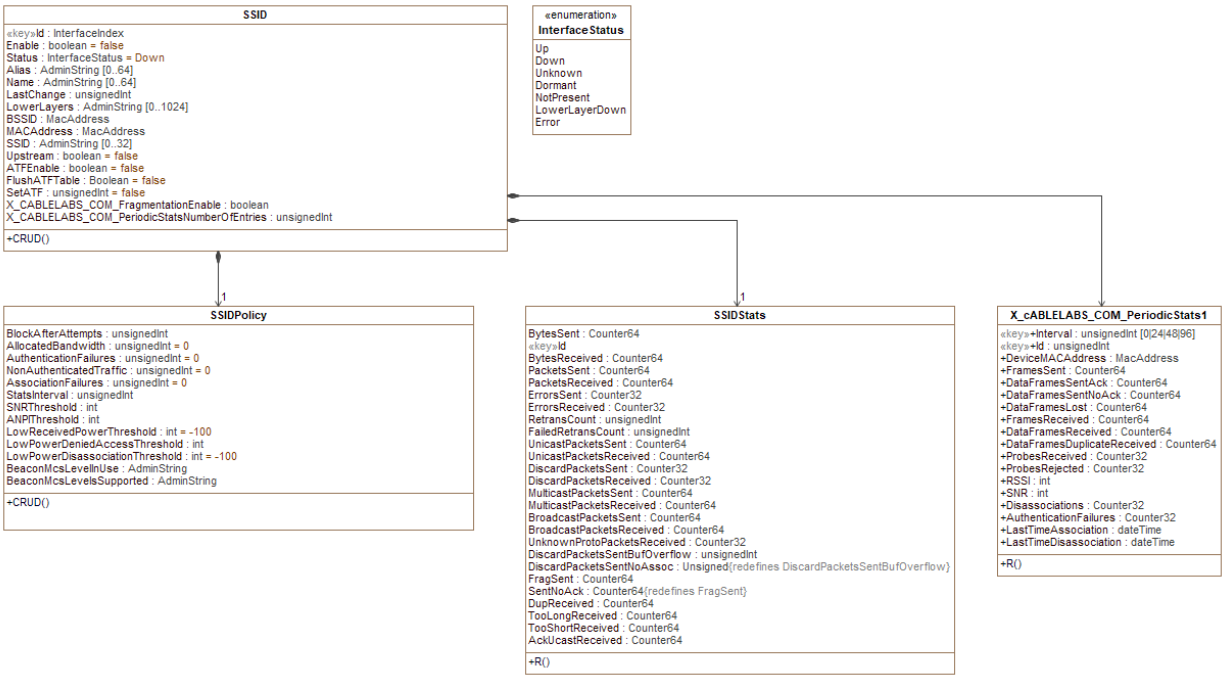

Figure 8 - SSID Object

The SSID object is defined in [TR-181i2] as Device.WiFi.SSID{i}.

The SSID object MUST be supported.

Table 18 - SSID Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Id	InterfaceIndex	key				MUST
Enable	Boolean	RW				MUST
Status	enum	RO	up(1), down(2), unknown(4), dormant(5), notPresent(6), lowerLayerDown(7), error(8)			MUST
Alias	string	RO	SIZE (0..64)			MUST
Name	string	RO	SIZE (0..64)			MUST
LastChange	unsignedInt	RO		seconds		MUST
LowerLayers	string	RW	SIZE (0..1024)			MUST
BSSID	MacAddress	RO				MUST
MACAddress	MacAddress	RO				MUST
SSID	string	RW	SIZE (0..32)			MUST
Upstream	boolean	RW				MUST1
ATFEnable	boolean	RW				?
FlushATFTable	boolean	RW				?
SetATF	unsignedInt	RW	[0:100]			?
X_CABLELABS_COM_FragmentationEnable	boolean	RW	false true			MUST
X_CABLELABS_COM_PeriodicStatsNumberOfEntries	unsignedInt	RO				MUST

[R1]: WiFi6

Refer to [TR-181i2] for the definitions of the parameters listed in 5 above, with the exception of the following CableLabs' extension attribute definitions:

A.2.3.11.1 X_CABLELABS_COM_FragmentationEnable

When this attribute is set to 'true' indicates that fragmentation is enabled for this SSID. When set to false, this attribute indicates fragmentation is disabled for this SSID.

A.2.3.11.2 X_CABLELABS_COM_PeriodicStatsNumberOfEntries

The number of periodic statistic entries in the table.

A.2.3.12 SSIDStats Object

Throughput statistics for this interface.

The SSIDstats object is defined in [TR-181i2] as Device.WiFi.SSID{i}.Stats.

The SSIDStats object MUST be supported.

Note: The StatsCounter64 data type SHOULD be used for all statistics parameters whose values might become greater than the maximum value that can be represented as an unsignedInt. The maximum value that can be represented as an unsignedLong (i.e. 0xffffffffffffffff) indicates that no data is available for this parameter.

Table 19 - SSIDStats Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
BytesSent	unsignedLong	RO		bytes		MUST
BytesReceived	unsignedLong	RO		bytes		MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
PacketsSent	unsignedLong	RO				MUST
PacketsReceived	unsignedLong	RO				MUST
ErrorsSent	unsignedInt	RO				MUST
RetransCount	unsignedInt	RO				MUST
FailedRetransCount	unsignedInt	RO				MUST
RetryCount	unsignedInt	RO				MUST
MultipleRetryCount	unsignedInt	RO				MUST
ACKFailureCount	unsignedInt	RO				MUST
AggregatedPacketCount	unsignedInt	RO				MUST
ErrorsReceived	unsignedInt	RO				MUST
UnicastPacketsSent	unsignedLong	RO				MUST
UnicastPacketsReceived	unsignedLong	RO				MUST
DiscardPacketsSent	unsignedInt	RO				MUST
DiscardPacketsReceived	unsignedInt	RO				MUST
MulticastPacketsSent	unsignedLong	RO				MUST
MulticastPacketsReceived	unsignedLong	RO				MUST
BroadcastPacketsSent	unsignedLong	RO				MUST
BroadcastPacketsReceived	unsignedLong	RO				MUST
UnknownProtoPacketsReceived	unsignedInt	RO				MUST
DiscardPacketsSentBufOverflow	unsignedLong	RO	StatsCounter64			MAY
DiscardPacketsSentNoAssoc	unsignedLong	RO	StatsCounter64			MAY
FragSent	unsignedLong	RO	StatsCounter64			MAY
SentNoAck	unsignedLong	RO	StatsCounter64			MAY
DupReceived	unsignedLong	RO	StatsCounter64			MAY
TooLongReceived	unsignedLong	RO	StatsCounter64			MAY
TooShortReceived	unsignedLong	RO	StatsCounter64			MAY
AckUcastReceived	unsignedLong	RO	StatsCounter64			MAY

A.2.3.13 X_CABLELABS_COM_SSIDPolicy Object

The SSIDPolicy object defines the configuration of policies, behaviors and event thresholds controlled per SSID.

The X_CABLELABS_COM_SSIDPolicy object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.SSID{i}.X_CABLELABS_COM_SSIDPolicy.

The X_CABLELABS_COM_SSIDPolicy object MAY be supported.

Table 20 - X_CABLELABS_COM_SSIDPolicy Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
BlockAfterAttempts	unsignedInt	RW			0	MAY
AllocatedBandwidth	unsignedInt	RW			0	MAY
AuthenticationFailures	unsignedInt	RW			0	MAY
NonAuthenticatedTraffic	unsignedInt	RW			0	MAY
AssociationFailures	unsignedInt	RW			0	MAY
StatsInterval	unsignedInt	RW		minutes	0	MAY
SNRThreshold	int	RW		dB	-100	MAY

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
ANPIThreshold	int	RW		dBm	-100	MAY
LowReceivedPowerThreshold	int	RW		dBm	-100	MAY
LowPowerDeniedAccessThreshold	int	RW		dBm	-100	MAY
LowPowerDisassociationThreshold	int	RW		dBm	-100	MAY
BeaconMcsLevelInUse	string	RW				MAY
BeaconMcsLevelsSupported	string	RO				MAY

A.2.3.13.1 BlockAfterAttempts

This attribute indicates the maximum number of attempts a client is allowed to attempt registration before being denied access. Exceeding this value generates one event. Events from same client should not reoccur more than once an hour. The value zero indicates no connection attempts restrictions.

A.2.3.13.2 AllocatedBandwidth

This attribute indicates the maximum bandwidth reserved for a particular interface. The value zero indicates no limit.

A.2.3.13.3 AuthenticationFailures

This attribute indicates the number of authentication failures a station simultaneously produces to generate the event. Events from same client should not reoccur more than once an hour. A value of zero (0) indicates threshold and events of this type are not generated.

A.2.3.13.4 NonAuthenticatedTraffic

This attribute represents the number of non-authenticated messages received from a station to generate an event. Events from same client should not reoccur more than once an hour. A value of zero (0)) indicates no threshold is set and events of this type are not generated.

A.2.3.13.5 AssociationFailures

This attribute indicates the number of simultaneous association failures from a station to generate an event. Events from same client should not reoccur more than once an hour. A value of zero (0) indicates no threshold is set and events of this type are not generated.

A.2.3.13.6 StatsInterval

This attribute indicates the interval value to collect per-interval statistics. A value of zero (0) indicates no interval and values reported are snapshots at the time of the request.

A.2.3.13.7 SNRThreshold

This attribute indicates the threshold to report SNR. The value -100 indicates no threshold, and events of this type are not generated.

A.2.3.13.8 ANPIThreshold

This attribute indicates the threshold to report the Average Noise plus Interference. The value -100 indicates no threshold, and events of this type are not generated.

A.2.3.13.9 LowReceivedPowerThreshold

This attribute indicates the power level threshold to generate an event whenever the station received power is below the threshold. The value -100 indicates no threshold, and events of this type are not generated.

A.2.3.13.10 LowPowerDeniedAccessThreshold

This attribute indicates the power level threshold to deny client association whenever the station received power is below the threshold. The value -100 indicates no threshold, and events of this type are not generated.

A.2.3.13.11 LowPowerDisassociatedThresold

This attribute indicates the threshold to report Disassociation due to low power. The Wi-Fi GW should refuse associations when the power level is below this RSSI level. The value -100 indicates no threshold, and events of this type are not generated.

A.2.3.13.12 BeaconMcsLevelInUse

This attribute specifies the beacon MCS to be used.

A.2.3.13.13 BeaconMcsLevelsSupported

This attribute specifies all the beacon MCSs supported.

A.2.3.14 X_CABLELABS_COM_PeriodicStats Object

This object contains periodic statistics for an 802.11 SSID on a CPE device. Note that these statistics refer to the link layer, not to the physical layer. This object does not include the total byte and packet statistics, which are, for historical reasons, in the parent object.

The X_CABLELABS_COM_PeriodicStats object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.SSID{i}. X_CABLELABS_COM_PeriodicStats.

The X_CABLELABS_COM_PeriodicStats object MAY be supported.

Table 21 - X_CABLELABS_COM_PeriodicStats Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Interval	unsignedInt	key	0, 1..24, 1..48, 1..96			MAY
Id	unsignedInt	key				MAY
DeviceMACAddress	MacAddress	RO				MAY
FramesSent	unsignedLong	RO				MAY
DataFramesSentAck	unsignedLong	RO				MAY
DataFramesSentNoAck	unsignedLong	RO				MAY
DataFramesLost	unsignedLong	RO				MAY
FramesReceived	unsignedLong	RO				MAY
DataFramesReceived	unsignedLong	RO				MAY
DataFramesDuplicateReceived	unsignedLong	RO				MAY
ProbesReceived	unsignedInt	RO				MAY
ProbesRejected	unsignedInt	RO				MAY
RSSI	int	RO		dBm		MAY
SNR	int	RO		dB		MAY
Disassociations	unsignedInt	RO				MAY
AuthenticationFailures	unsignedInt	RO				MAY
LastTimeAssociation	dateTime	RO				MAY
LastTimeDisassociation	dateTime	RO				MAY

A.2.3.14.1 Interval

This key indicates the Interval where the measurements were accumulated. The interval of measurements is synchronized with the wall clock. The total number of intervals is based on a 24 hour period. At an interval of 15

minutes 96 intervals (1..96) are defined, at 30 minutes, 48 intervals (1..48) and 24 intervals (1..24) for 1 hour measurement interval. Devices with no capabilities to report measurements per interval will report the value 0 for the interval attribute of the unique statistics instance.

A.2.3.14.2 Id

The Id key represents a unique identifier for a client MAC address in a given statistics measurement interval.

A.2.3.14.3 Device MACAddress

The DeviceMACAddress attribute represents the MAC address of an associated client device.

A.2.3.14.4 FramesSent

The FrameSent attribute represents the total number of frames transmitted out of the interface. For conventional 802.11 MAC (a,b,g) this counter corresponds to the total of MSDUs (MAC Service Data Unit) being transmitted. For High Throughput transmissions this corresponds to the A-MSDU (Aggregation MSDU). The value of this counter MAY be reset to zero when the CPE is rebooted.

A.2.3.14.5 DataFramesSentAck

The DataFramesSentAck attribute indicates the total number of MSDU frames marked as duplicates and non-duplicates acknowledged. The value of this counter MAY be reset to zero when the CPE is rebooted.

A.2.3.14.6 DataFramesSentNoAck

The DataFramesSentNoAck attribute represents the total number of MSDU frames retransmitted out of the interface (i.e., marked as duplicate and non-duplicate) and not acknowledged but not including those defined in dataFramesLost. The value of this counter MAY be reset to zero when the CPE is rebooted.

A.2.3.14.7 DataFramesLost

The DataFramesLost attribute represents the total number of MSDU frames retransmitted out of the interface that where not acknowledged and discarded for reaching max number of retransmissions. The value of this counter MAY be reset to zero when the CPE is rebooted.

A.2.3.14.8 FramesReceived

The FramesReceived attribute indicates the total number of frames received by the interface. For conventional 802.11 MAC (a,b,g) this counter corresponds to the total of MSDUs (MAC Service Data Unit) being transmitted. For High Throughput transmissions (n) this corresponds to A-MSDUs (Aggregation MSDU) and MSDUs. The value of this counter MAY be reset to zero when the CPE is rebooted.

A.2.3.14.9 DataFramesReceived

The DataFramesReceived attribute represents the total number of MSDU frames received and marked as non-duplicates. The value of this counter MAY be reset to zero when the CPE is rebooted.

A.2.3.14.10 DataFramesDuplicateReceived

The DataFramesDuplicateReceived attribute indicates the total number of duplicated frames received on this interface. The value of this counter MAY be reset to zero when the CPE is rebooted.

A.2.3.14.11 ProbesReceived

The ProbesReceived attribute indicates the total number of probes received.

A.2.3.14.12 ProbesRejected

The ProbesRejected attribute is the total number of probes rejected.

A.2.3.14.13 RSSI

The Received Signal Strength attribute indicates the energy observed at the antenna receiver for the most recent reception.

A.2.3.14.14 SNR

The signal to Noise Ratio (SNR) attribute represents the strength of the signal compared to receive noise for the most recent reception.

A.2.3.14.15 Disassociations

The Disassociations attribute represents the total number of client disassociations.

A.2.3.14.16 AuthenticationFailures

The AuthenticationFailures attribute indicates the total number of authentication failures.

A.2.3.14.17 LastTimeAssociation

This attribute represents the last time the client was associated.

A.2.3.14.18 LastTimeDisassociation

This attribute represents the last time the client disassociated from the interface. The all zeros value indicates the client is currently associated.

A.2.3.15 AccessPoint Object

This object represents an 802.11 connection from the perspective of a wireless access point.

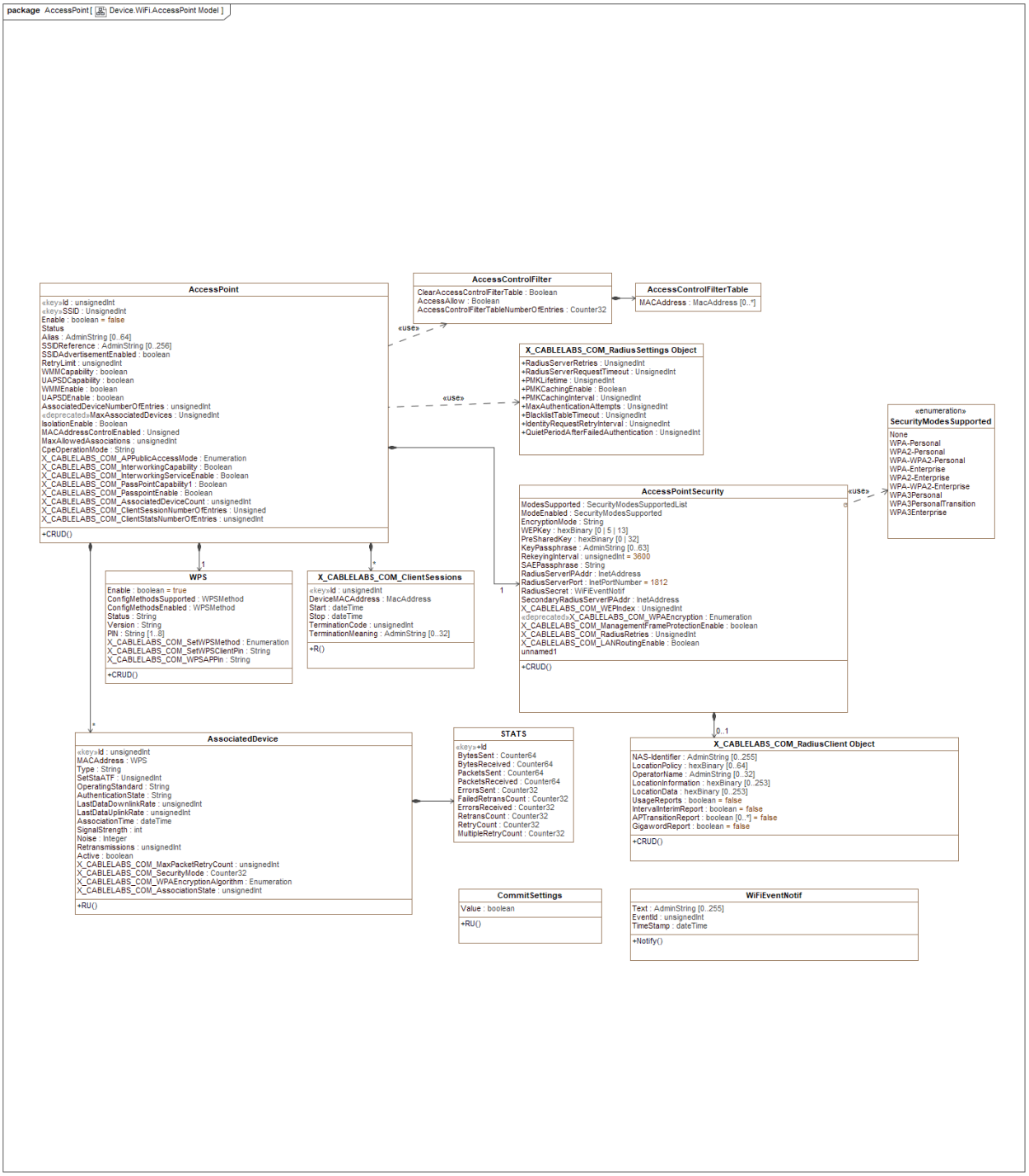

Figure 9 - AccessPoint Object Model Class Diagram

The AccessPoint object is defined in [TR-181i2] as Device.WiFi.AccessPoint{i}.

The AccessPoint object MUST be supported.

Table 22 - AccessPoint Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Id	unsignedInt	key				MUST
Enable	boolean	RW	false true		false	MUST
Status	enum	RO	disabled(1), enabled(2), error_misconfigured(3), error(4)			MUST
Alias	string	RW	SIZE (0..64)			MUST
SSIDReference	string	RW	SIZE (0..256)			MUST
SSIDAdvertisementEnabled	boolean	RW				MUST
RetryLimit	unsignedInt	RW	0…7			MUST
WMMCapability	boolean	RO				MUST
UAPSDCapability	boolean	RO				MUST
WMMEnable	boolean	RW				MUST
UAPSDEnable	boolean	RW				MUST
AssociatedDeviceNumberOfEntries	unsignedInt	RO				MUST
MaxAssociatedDevices	unsignedInt	RW				OBSOLETE[1]
IsolationEnable	boolean	RW				MUST
MACAddressControlEnabled	boolean	RW				MUST
AllowedMACAddress	MACAddress	RW				MUST
MaxAllowedAssociations1	unsignedInt	RW				MUST
CpeOperationMode	string	RW	router(1), bridge/extender(2)		router	MUST
X_CABLELABS_COM_APPublicAccessMode	enum	RW	private(1), public(2)			MUST
X_CABLELABS_COM_InterworkingCapability	boolean	RO	false true			CONDITIONAL MUST
X_CABLELABS_COM_InterworkingServiceEnable	boolean	RW	false true			CONDITIONAL MUST
X_CABLELABS_COM_PassPointCapability	boolean	RO	false true			CONDITIONAL MUST
X_CABLELABS_COM_PasspointEnable	boolean	RW	false true			CONDITIONAL MUST
X_CABLELABS_COM_AssociatedDeviceCount	unsignedInt	RO				DEPRECATED
X_CABLELABS_COM_ClientSessionNumberOfEntries	unsignedInt	RO				MUST
X_CABLELABS_COM_ClientStatsNumberOfEntries	unsignedInt	RO				MUST

Refer to [TR-181i2] for the definition of the parameters listed in Table 22 above, with the exception of the following CableLabs' extension attribute definitions:

A.2.3.15.1 X_CABLELABS_COM_APPublicAccessMode

Configure as private or public (public only if community Wi-Fi enabled on device.deviceinfo).

A.2.3.15.2 X_CABLELABS_COM_InterworkingCapability

Declare support for Interworking with external networks.

[1] Replaced by MaxAllowedAssociations

A.2.3.15.3 X_CABLELABS_COM_InterworkingServiceEnable

Enable/disable Interworking. Enables or disables capability of the access point to interwork with external network. When enabled, the access point includes Interworking IE in the beacon frames.

A.2.3.15.4 X_CABLELABS_COM_PasspointCapability

Declare Passpoint support.

A.2.3.15.5 X_CABLELABS_COM_PasspointEnable

Enable/disable Passpoint.

A.2.3.15.6 X_CABLELABS_COM_AssociatedDeviceCount

Total number of active devices associated at any point in time. DEPRECATED: Use AssociatedDeviceNumberOfEntries instead.

A.2.3.15.7 X_CABLELABS_COM_ClientSessionNumberOfEntries

The number of client session entries.

A.2.3.15.8 X_CABLELABS_COM_ClientStatsNumberOfEntries

The number of client statistic entries.

A.2.3.16 X_CABLELABS_COM_AccessControlFilter

The X_CABLELABS_COM.AccessControlFilter object is defined as a CableLabs extension to [TR-181i2] as Device.WiFi.AccessPoint{i}.X_CABLELABS_COM_AccessControlFilter.

Support for the X_CABLELABS_COM.AccessControlFilter object is a CONDITIONAL MUST.

Table 23 - X_CABLELABS_COM_AccessControlFilter Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
ClearAccessControlFilterTable	boolean	RW	false true		false	MUST
AccessAllow	boolean	RW	false true		false	MUST
AccessControlFilterTableNumberOfEntries	unsignedInt	RO				MUST

Please refer to [TR-181i2] for the definition of the parameters listed in Table 23 above except as specified below.

A.2.3.16.1 ClearAccessControlFilterTable

When set to ‘true’, this attribute clears the CPE MAC address entries from the Access Control Filter Table residing in non-volatile memory..

A.2.3.16.2 AccessAllow

This attribute indicates if access is allowed for this MACAddress. A value of 'true' indicates access is allowed, whereas, a value of 'false' indicates that access is denied.

A.2.3.16.3 AccessControlFilterTableNumberOfEntries

This attribute represents the number of access control filter entries.

A.2.3.17 AccessControlFilterTable

This object defines parameters used for filtering by MAC address.

The AccessControlFilter object is defined as a CableLabs extension to [TR-181i2] as Device.WiFi.AccessPoint{i}. X_CABLELABS_COM_AccessPointControlFilter.AccessControlFilterTable.{i}.

The AccessControlFilterTable object MUST be supported.

The AccessControlFilterTable object MUST reside in non-volatile memory.

Table 24 - AccessPointAccessControlFilterTable

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
MACAddress	MACAddress	RW	SIZE (17)			MUST

A.2.3.17.1 MACAddress

MACAddress is the key used in the AccessPointAccessControlFilterTable to represent the CPE MAC address of a device to be allowed or disallowed access on the WiFi radio interface.

A.2.3.18 AccessPointSecurity

This object contains security parameters that apply to a CPE acting as an access point.

The AccessPointSecurity object is defined in [TR-181i2] as Device.WiFi.AccessPoint{i}.Security.

The device MUST support the AccessPointSecurity object if.

Table 25 - AccessPointSecurity Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Reset	boolean	RW	false true			MUST
ModesSupported	string	RO	none(1), wep64(2) DEPRECATED, wep128(3) DEPRECATED, wpaPersonal(4), wpa2Personal(5), wpaWPA2Personal(6), wpaEnterprise(7), wpa2Enterprise(8), wpaWpa2Enterprise(9), wpa3Personal (10), wpa3PersonalTransition (11), pa3Enterprise (12)			MUST
ModeEnabled	enum	RW	none(1), wep64(2) DEPRECATED, wep128(3) DEPRECATED, wpaPersonal(4), wpa2Personal(5), wpaWPA2Personal(6), wpaEnterprise(7), wpa2Enterprise(8), wpaWpa2Enterprise(9), wpa3Personal (10), wpa3PersonalTransition (11), wpa3Enterprise (12)			MUST
EncryptionMode	string	RW	tkip (1), aes (2)			MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
WEPKey	hexBinary	RW	SIZE (5)			DEPRECATED
PreSharedKey	hexBinary	RW	SIZE (32)			MUST
KeyPassphrase	string	RW	SIZE (8..63)			MUST
RekeyingInterval	unsignedInt	RW		seconds	3600	MUST
SAEPassphrase	string	RW				MUST
RadiusServerIPAddr	IPAddress	RW				MUST
SecondaryRadiusServerIPAddr	IPAddress	RW				MUST
RadiusServerPort	unsignedInt	RW			1812	MUST
SecondaryRadiusServerPort	unsignedInt	RW				MUST
RadiusSecret	string	RW				MUST
SecondaryRadiusSecret	string	RW				MUST
MFPConfig	string	RW	disabled (1), optional (2), required (3)		disabled	MUST
X_CABLELABS_COM_WEPKey2	hexBinary	RW	SIZE (5,13)			DEPRECATED
X_CABLELABS_COM_WEPKey3	hexBinary	RW	SIZE (5,13)			DEPRECATED
X_CABLELABS_COM_WEPKey4	hexBinary	RW	SIZE (5,13)			DEPRECATED
X_CABLELABS_COM_WEPIndex	unsignedInt	RW	1..4			DEPRECATED
X_CABLELABS_COM_WEPPassPhrase	string	RW	SIZE (0, 5,13)			DEPRECATED
X_CABLELABS_COM_WPAEncryption	enum	RW	aes(1), tkip+aes(2)		tkip+aes	DEPRECATED
X_CABLELABS_COM_ManagementFrameProtectionEnable	boolean	RW	False true			MUST
X_CABLELABS_COM_RadiusRetries	unsignedInt	RW				MUST
X_CABLELABS_COM_LANRoutingEnable	boolean	RW	False true			MUST

Please refer to [TR-181i2] for the definitions of the parameters listed in Table 25 except for those listed below.

A.2.3.18.1 X_CABLELABS_COM_WEPKey2

This attribute defines the WEP key 2 expressed as a hexadecimal string. DEPRECATED: WEP should no longer be used.

A.2.3.18.2 X_CABLELABS_COM_WEPKey3

This attribute defines the WEP key 3 expressed as a hexadecimal string. DEPRECATED: WEP should no longer be used.

A.2.3.18.3 X_CABLELABS_COM_WEPKey4

This attribute defines the WEP key 4 expressed as a hexadecimal string. DEPRECATED: WEP should no longer be used.

A.2.3.18.4 X_CABLELABS_COM_WEPIndex

This attribute defines the selected WEP key. DEPRECATED: WEP should no longer be used.

A.2.3.18.5 X_CABLELABS_COM_WEPPassPhrase

This attribute defines a human readable password to derive the WEP keys, following a well-known key generation algorithm for the purpose. When this attribute is a zero-length string, WEP keys are used directly. Otherwise, the

values of the WEP keys cannot be changed directly and an error is returned on write. DEPRECATED: WEP should no longer be used.

A.2.3.18.6 X_CABLELABS_COM_WPAEncryption

This attribute defines the encryption algorithm used for WPA. DEPRECATED: Use EncryptionMode instead.

A.2.3.18.7 X_CABLELABS_COM_ManagementFrameProtectionEnable

This attribute determines if the Management Frame Protection mechanism that provides security for the management messages passed between access point (AP) and Client stations is enabled or disabled.

A.2.3.18.8 X_CABLELABS_COM_RadiusRetries

This attribute indicates the failover retry count that increments when the Radius server cannot be reached.

A.2.3.18.9 X_CABLELABS_COM_LANRoutingEnable

This attribute indicates LAN routing is enabled. A value of 'true' indicates LAN Routing is enabled, whereas a value of 'false' indicates LAN routing is disabled.

A.2.3.19 AccessPointWPS Object

This object contains parameters related to Wi-Fi Protected Setup for this access point.

The AccessPointWPS object is defined in [TR-181i2] as Device.WiFi.AccessPoint{i}.WPS.

The AccessPointWPS object MUST be supported.

Table 26 - AccessPointWPS Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Enable	boolean	RW	false true			MUST
ConfigMethodsSupported	enum	RO	USBFlashDrive(1), Ethernet(2), Label(3), Display(4), ExternalNFCToken(5), IntegratedNFCToken(6), NFCInterface(7), PIN(8), PushButton(9), PhysicalPushButton(10), PhysicalDisplay(11), VirtualPushButton(12), VirtualDisplay(13)			MUST
ConfigMethodsEnabled	enum	RW	SBFlashDrive(1), Ethernet(2), Label(3), Display(4), ExternalNFCToken(5), IntegratedNFCToken(6), NFCInterface(7), PIN(8), PushButton(9), PhysicalPushButton(10), PhysicalDisplay(11), VirtualPushButton(12), VirtualDisplay(13)			MUST
InitiateWPSPB()	data model cmd	RW	ASYNC; no input args			MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
<= Status	enum output arg	RO	success(1), error_not_ready(2), error_timeout(3), error_other(4)			MUST
X_CABLELABS_COM_SetWPSMethod	enum	RW	USBFlashDrive(1) Ethernet(2) Label(3) Display(4) ExternalNFCToken(5) IntegratedNFCToken(6) NFCInterface(7) PIN(8) PushButton(9)			DEPRECATED
X_CABLELABS_COM_SetWPSClientPin	string	RW				MUST
X_CABLELABS_COM_WPSAPPin	string	RO				MUST

Please refer to [TR-181i2] for the definitions of the parameters listed in Table 26 above except as noted below.

A.2.3.19.1 X_CABLELABS_COM_SetWPSMethod

This attribute is used to set and report the BSS WPS Method (Soft or physical). DEPRECATED: Use ConfigMethodsEnabled instead.

A.2.3.19.2 X_CABLELABS_COM_SetWPSClientPin

This attribute is used to set the BSS WPS Client Pin.

A.2.3.19.3 X_CABLELABS_COM_WPSAPPin

This attribute is used to set the BSS WPS AP Pin.

A.2.3.20 AssociatedDevice Object

A table of the devices currently associated with the access point.

The AssociatedDevice object is defined in [TR-181i2] as Device.WiFi.AccessPoint{i}.AssociatedDevice{i}.

The AssociatedDevice object MUST be supported.

Table 27 - AssociatedDevice Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Id	unsignedInt	key				MUST
MACAddress	MacAddress	RO				MUST
Type	string	RO				MUST
SetStaATF	unsignedInt	RW	1..100	Percentage		MUST
OperatingStandard	string	RO	a (1), b (2), c (3), g (4), n (5), ac (6), ax (7)			MUST
AuthenticationState	Boolean	RO				MUST
LastDataDownlinkRate	unsignedInt	RO	1000..600000	kbps		MUST
LastDataUplinkRate	unsignedInt	RO	1000..600000	kbps		MUST
AssociationTime	dateTime	RO				MUST
SignalStrength	int	RO	-200..0	dBm		MUST
Noise	int	RO	-200..0			MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Retransmissions	unsignedInt	RO	0..100	packets		MUST
Active	Boolean	RO				MUST
X_CABLELABS_COM_MaxPacketRetryCount	unsignedInt	RW		packets		MUST
X_CABLELABS_COM_SecurityMode	enum	RO	none(1), wep64(2), wep128(3), wpaPersonal(4), wpa2Personal(5), wpaWPA2Personal(6), wpaEnterprise(7), wpa2Enterprise(8), wpaWpa2Enterprise(9), wpa3Personal (10), wpa3PersonalTransition (11), wpa3Enterprise (12)			MUST
X_CABLELABS_COM_WPAEncryptionAlgorithm	enum	RO	TKIP(1), AES(2)			DEPRECATED
X_CABLELABS_COM_AssociationState	enum	RO	connected(1), clientDisassociated(2), forcedDisassociationAuth(3), forcedDisassociationTimeout(4), forcedDisassociationNetMode(5), forcedDisassociationSnr(6), other(7)			MUST

Please refer to [TR-181i2] for the definitions of the parameters listed in Table 27 with the exception of the following attribute definitions:

A.2.3.20.1 X_CABLELABS_COM_MaxPacketRetryCount

Indicates the number of packets to be retransmitted to have an upper limit.

A.2.3.20.2 X_CABLELABS_COM_SecurityMode

Reports security mode for associated device.

A.2.3.20.3 X_CABLELABS_COM_WPAEncryptionAlgorithm

This attribute reports the encryption algorithm used for the associated device.

A.2.3.20.4 X_CABLELABS_COM_AssociationState

This attribute reports the status of any known devices that are or have been associated if the CPE tracks device history after disassociation.

A.2.3.21 X_CABLELABS_COM_ClientSessions Object

The ClientSessions object represents the current and closed sessions (association connections). When the maximum number of instances is reached, the oldest closed session instance is replaced by a newly created client association.

The X_CABLELABS_COM_ClientSessions object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint{i}.X_CABLELABS_COM_ClientSessions.{i}.

The X_CABLELABS_COM_ClientSessions object MUST be supported.

Table 28 - X_CABLELABS_COM_ClientSessions Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Id	unsignedInt	key				MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
DeviceMACAddress	MACAddress	RO				MUST
Start	dateTime	RO				MUST
Stop	dateTime	RO				MUST
TerminationCode	unsignedInt	RO				MUST
TerminationMeaning	string	RO	SIZE (0..32)			MUST

A.2.3.21.1 Id

The Id key identifies a single client MAC Address in the Client Sessions table.

A.2.3.21.2 DeviceMACAddress

This attribute indicates the MAC address of an associated client device.

A.2.3.21.3 Start

This attribute indicates the time when the session started.

A.2.3.21.4 Stop

This attribute indicates the time when the session ended. When the session is active, the value reported is all zeros.

A.2.3.21.5 TerminationCode

This attribute indicates the Reason Code or the Status Code that lead to ending the association of the station. Reason Code and Status Code overlap. The context of the type of termination is provided by the TerminationMeaning attribute. The value zero indicates the session is active.

A.2.3.21.6 TerminationMeaning

This attribute indicates the meaning of the Reason Code or Status Code for the ended session. The zero-length string is used when the instance corresponds to an active session.

A.2.3.22 X_CABLELABS_COM_ClientStats Object

The ClientStats object contains accumulative statistics for each client station served by the Wi-Fi GW. A station is reported only after it is associated for the first time.

The X_CABLELABS_COM_ClientStats object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint{i}.X_CABLELABS_COM_ClientStats.{i}.

The X_CABLELABS_COM_ClientStats object MUST be supported.

Table 29 - X_CABLELABS_COM_ClientStats Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Interval	unsignedInt	key	0, 1..24, 1..48, 1..96			MUST
Id	unsignedInt	key				MUST
DeviceMACAddress	MACAddress	RO				MUST
FramesSent	unsignedLong	RO				MUST
DataFramesSentAck	unsignedLong	RO				MUST
DataFramesSentNoAck	unsignedLong	RO				MUST
DataFramesLost	unsignedLong	RO				MUST
FramesReceived	unsignedLong	RO				MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
DataFramesReceived	unsignedLong	RO				MUST
DataFramesDuplicateReceived	unsignedLong	RO				MUST
ProbesReceived	unsignedInt	RO				MUST
ProbesRejected	unsignedInt	RO				MUST
RSSI	int	RO		dBm		MUST
SNR	int	RO		dB		MUST
Disassociations	unsignedInt	RO				MUST
AuthenticationFailures	unsignedInt	RO				MUST
LastTimeAssociation	dateTime	RO				MUST
LastTimeDisassociation	dateTime	RO				MUST
Throughput	unsignedInt	RO		Kbps		MUST
PktErrorRatePerSTA	unsignedInt	RO		10-5 Errors		MUST

A.2.3.22.1 Interval

This attribute indicates when the measurements were accumulated. The interval of measurements is synchronized with the wall clock. The total number of intervals is based on a 24 hour period. At an interval of 15 minutes 96 intervals (1..96) are defined, at 30 minutes, 48 intervals (1..48) and 24 intervals (1..24) for 1 hour measurement interval. Devices with no capable to report measurements per interval will report the value 0 for the interval attribute.

A.2.3.22.2 Id

The Id key identifies a single client MAC Address.

A.2.3.22.3 DeviceMACAddress

This attribute indicates the MAC address of an associated client device.

A.2.3.22.4 FramesSent

This attribute indicates the total number of frames transmitted out of the interface. For conventional 802.11 MAC ([802.11a], [802.11b], [802.11g], [802.11n], [802.11ac], and [802.11ax]) this counter corresponds to the total of MSDUs being transmitted. For High Throughput transmissions this corresponds to the A-MSDU. The value of this counter may be reset to zero when the CPE is rebooted.

A.2.3.22.5 DataFramesSentAck

This attribute indicates the total number of MSDU frames marked as duplicates and non-duplicates acknowledged. The value of this counter may be reset to zero when the CPE is rebooted.

A.2.3.22.6 DataFramesSentNoAck

This attribute indicates the total number of MSDU frames retransmitted out of the interface (i.e., marked as duplicate and non-duplicate) and not acknowledged, but does not exclude those defined in the DataFramesLost parameter. The value of this counter may be reset to zero when the CPE is rebooted.

A.2.3.22.7 DataFramesLost

This attribute indicates the total number of MSDU frames retransmitted out of the interface that were not acknowledged and discarded for reaching max number of retransmissions. The value of this counter may be reset to zero when the CPE is rebooted.

A.2.3.22.8 FramesReceived

This attribute indicates the total number of frames received by the Wi-Fi interface. For conventional 802.11 MAC ([802.11a], [802.11b], [802.11g], [802.11n], and [802.11ac]) this counter corresponds to the total of MSDUs being transmitted. For High Throughput transmissions (n), this corresponds to A-MSDUs and MSDUs. The value of this counter may be reset to zero when the CPE is rebooted.

A.2.3.22.9 DataFramesReceived

This attribute indicates the total number of MSDU frames received and marked as non-duplicates. The value of this counter may be reset to zero when the CPE is rebooted.

A.2.3.22.10 DataFramesDuplicateReceived

This attribute indicates the total number of duplicated frames received on this interface. The value of this counter may be reset to zero when the CPE is rebooted.

A.2.3.22.11 ProbesReceived

This attribute indicates the total number of probes received.

A.2.3.22.12 ProbesRejected

This attribute indicates the total number of probes rejected.

A.2.3.22.13 RSSI

This attribute indicates the energy observed at the antenna receiver for a current transmission.

A.2.3.22.14 SNR

This attribute indicates the signal strength received from a client compared to the noise received.

A.2.3.22.15 Disassociations

The This attribute indicates the total number of client disassociations.

A.2.3.22.16 AuthenticationFailures

This attribute indicates the total number of authentication failures.

A.2.3.22.17 LastTimeAssociation

This attribute indicates the last time the client was associated.

A.2.3.22.18 LastTimeDisassociation

This attribute indicates the last time the client disassociated from the interface. The all zeros value indicates the client is currently associated.

A.2.3.22.19 Throughput

This attribute indicates the packet throughput expressed in Kbps.

A.2.3.22.20 PktErrorRatePerSTA

This attribute signifies the number of packet errors, represented as 10-5 errors, on a per STA basis.

A.2.3.23 X_CABLEABS_COM_RadiusClient Object

The RadiusClient object is the extension of Radius Client operation for the Access Point 802.1x Authenticator for WPA Enterprise. An instance is relevant when the attribute AccessPointSecurity. ModeEnabled is 'WPA-Enterprise' or 'WPA2-Enterprise' or 'WPA-WPA2-Enterprise'.

The X_CABLELABS_COM_RadiusClient object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.Security.X_CABLELABS_COM_RadiusClient.

The device MUST support the X_CABLELABS_COM_RadiusClient object if….

Table 30 - X_CABLELABS_COM_RadiusClient Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
NAS-Identifier	string	RW	SIZE (0..255)			MAY
LocationPolicy	hexBinary	RW	SIZE (0..64)			MAY
OperatorName	string	RW	SIZE (0..32)			MAY
LocationInformation	hexBinary	RW	SIZE (0..253)			MAY
LocationData	hexBinary	RW	SIZE (0..253)			MAY
UsageReports	boolean	RW	false true		false	MAY
IntervalInterimReport	boolean	RW	false true		false	MAY
APTransitionReport	boolean	RW	false true		false	MAY
GigawordReport	boolean	RW	false true		false	MAY

A.2.3.23.1 NAS-Identifier

This attribute corresponds to the Radius attribute NAS-Identifier used in Access request messages. The device always sends the Radius parameter NAS-IP-Address and will send the NAS-Identifier parameter when this attribute is set to other than the zero-length string. The NAS-Identifier attribute can be used as a hint to indicate the authentication server the SSID domain where user tries to authenticate, i.e., when more than one SSID domains are using the same Radius server instance.

A.2.3.23.2 LocationPolicy

This attribute corresponds to the string value of the RADIUS Basic-Location-Policy-Rules attribute per [RFC 5580].

A.2.3.23.3 OperatorName

This attribute corresponds to the string value of the RADIUS Operator-Name attribute per [RFC 5580].

A.2.3.23.4 LocationInformation

This attribute corresponds to the string value of the RADIUS Location-Information attribute per [RFC 5580].

A.2.3.23.5 LocationData

This attribute corresponds to the string value of the RADIUS LocationData attribute per [RFC 5580].

A.2.3.23.6 UsageReports

This attribute indicates whether the client send usage data ('true') or not ('false').

A.2.3.23.7 IntervalInterimReport

This attribute indicates whether the client sends Interim reports at periodic time intervals. A value of ('true') indicates Interim reports are sent based upon a periodic time interval.

A.2.3.23.8 APTransitionReport

This attribute indicates the client sends Interim reports when the stations transitions to a different Access point when the value is set to ‘true’.

A.2.3.23.9 GigawordReport

This attribute indicates the client sends Interim reports when the 32-bit counters rollover when the value is set to ‘true’.

A.2.3.24 X_CABLELABS_COM_WiFiEventNotif Object

This object represents the Wi-Fi event notification object.

The X_CABLELABS_COM_WiFiEventNotif object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi. X_CABLELABS_COM_WiFiEventNotif.

The X_CABLELABS_COM_WiFiEventNotif object MAY be supported.

Table 31 - X_CABLELABS_COM_WiFiEventNotif Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Text	string	RW	SIZE (0..255)			MAY
EventId	unsignedInt	RW				MAY
TimeStamp	dateTime	RW				MAY

A.2.3.24.1 Text

This attribute represents the Event Message of the event.

A.2.3.24.2 EventId

This attribute represents the identifier of the event.

A.2.3.24.3 TimeStamp

This attribute establishes the Date and Time when the event was generated (not the time when the event was dispatched).

A.2.3.25 X_CABLELABS_COM_InterworkingService Object

Interworking objects in conjunction with Hotspot2.0.

The X_CABLELABS_COM_InterworkingService object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_InterworkingService.

The device MUST support the X_CABLELABS_COM_InterworkingService object if.. MUST.

Table 32 - X_CABLELABS_COM_ InterworkingService Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
AccessNetworkType	int	RW	1..15			MUST
Internet	boolean	RW	false true			MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
VenueGroupCode	int	RW	0..255			MUST
VenueTypeCode	int	RW	3..5			MUST
HESSID	string	RW	SIZE (17)			MUST

A.2.3.25.1 AccessNetworkType

This attribute is used to set the value for the Interworking IE transmitted in the beacons. (refer 8.4.2.94 of [802.11]). Possible values are:

0 - Private network

1 - Private network with guest access

2 - Chargeable public network

3 - Free public network

4 - Personal device network

5 - Emergency services only network

6-13 - Reserved

14 - Test or experimental

A.2.3.25.2 Internet

This attribute, when set to ‘true’, provides connectivity to the Internet; otherwise it is set to ‘false’ indicating that it is unspecified whether the network provides connectivity to the Internet.

A.2.3.25.3 VenueGroupCode

This attribute indicates the Venue Group of the Venue Info Field (refer 8.4.1.34 of [802.11]) where the access point is installed.

1 - Unspecified

2 - Assembly

3 - Business

4 - Educational

5 -Factory and Industrial

6 - Institutional

7 - Mercantile

8 - Storage

9 - Utility and Miscellaneous

10 - Vehicular

11 - Outdoor

12-255 - Reserve

A.2.3.25.4 AccessPoint

This represents the key value. Each row represents common attributes of an Access Point supporting Passpoint 2.0.

A.2.3.25.5 VenueTypeCode

This attribute indicates the Venue Type of the Venue Info Field (refer 8.4.1.34 of [802.11] 2012) where the access point is installed. The possible values are listed in the referenced standard.

A.2.3.25.6 HESSID

This attribute represents Homogeneous Extended Service Set Identifier (HESSID). The HESSID is a globally unique identifier that in conjunction with the WLAN-SSID, may be used to provide network identification for a subscription service provider network.

A.2.3.26 X_CABLELABS_COM_Passpoint Object

This object defines the common attributes to implement Passpoint2.0.

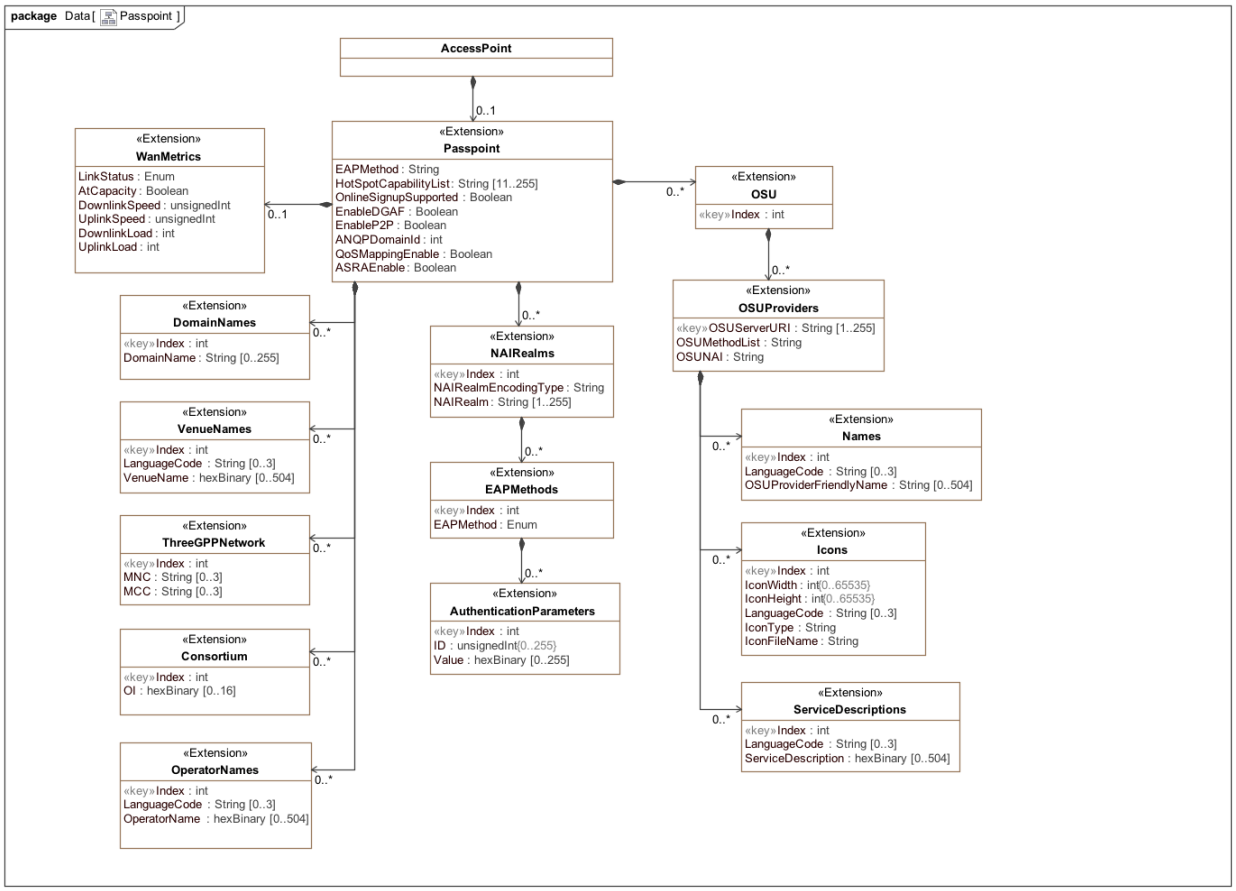

Figure 10 - Passpoint Object Model Class Diagram

The X_CABLELABS_COM_Passpoint object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_Passpoint.

The device MUST support the X_CABLELABS_COM_Passpoint object if...

Table 33 - X_CABLELABS_COM_Passpoint Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
EAPMethod	enum	RO				MUST
HotSpotCapabilityList	string	RO	SIZE (11..255)			MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
OnlineSignupSupported	boolean	RO				MUST
DGAFEnable	boolean	RW	false true			MUST
P2PEnable	boolean	RW	false true			MUST
ANQPDomainID	int	RW	-1..65535			MUST
QoSMappingEnable	boolean	RW	false true			MUST
ASRAEnable	boolean	RW	false true			MUST
ManagementFrameProtectionEnable						MUST
VenueNamesNumberofEntries	unsignedInt	RO				MUST
ThreeGPPNetworkNumberOfEntries	unsignedInt	RO				MUST
ConsortiumNumberOfEntries	unsignedInt	RO				MUST
DomainNamesNumberOfEntries	unsignedInt	RO				MUST
OperatorNamesNumberOfEntries	unsignedInt	RO				MUST
NAIRealmsNumberOfEntries	unsignedInt	RO				MUST
OSUNumberOfEntries	unsignedInt	RO				MUST

A.2.3.26.1 EAPMethod

This attribute represents the EAP method used by this AP. Refer to Device.IEEE8021x.

A.2.3.26.2 HotSpotCapabilityList

This attribute represents the capability list in the table in an exact order. HS Query list (1), HS Capability list (2), Operator Friendly Name (3), WAN Metrics (4), Connection Capability (5), NAI Home Realm Query (6), Operating Class Indication (7), OSU Providers list (8), Reserved (9), Icon Request (10), Icon Binary File (11). Each Octet corresponds to a capability by relative position as follows: 0-not supported, 1-supported.

A.2.3.26.3 OnlineSignupSupported

This attribute indicates whether online signup is supported as indicated by a value of 'true' or 'false'.

A.2.3.26.4 DGAFEnable

This attribute represents the Downstream Forwarding of Group-Addressed Frames (DGAF). This attribute is enabled with a value of 'true' and disabled with a value of 'false.

A.2.3.26.5 P2PEnable

This attribute represents if the Point to Point cross connect is enabled or disabled using a value of 'true' or 'false'.

A.2.3.26.6 ANQPDomainID

This attribute indicates a 16-bit field included in Beacon and Probe response frames transmitted by the AP. All APs in the same ESS sharing a common, nonzero value of ANQP Domain ID shall have identical ANQP information for the ANQP elements and Hotspot 2.0 vendor-specific ANQP elements. APs having their ANQP Domain ID field set to a value of zero have unique ANQP information in one or more of their ANQP elements or Hotspot 2.0 vendor-specific ANQP elements, or have not been implemented with means of knowing whether their ANQP information is unique. APs having their ANQP Domain ID field set to -1 should not include ANQP Domain ID field in the HS2.0 indication element.

A.2.3.26.7 QoSMappingEnable

This attribute represents the QoS mapping for Interworking Services is enabled 'true' or not 'false'.

A.2.3.26.8 ASRAEnable

This attribute, the Additional Step Required for Access (ASRA) is enabled with a value of 'true' and disabled with a value of 'false'.

A.2.3.26.9 VenueNamesNumberOfEntries

This attribute represents the number of venue name entries.

A.2.3.26.10 ThreeGPPNetworkNumberOfEntries

This attribute represents the number of 3GPP network entries.

A.2.3.26.11 ConsortiumNumberOfEntries

This attribute indicates the number of consortium entries.

A.2.3.26.12 OSUNumberOfEntries

This attribute indicates the number of OSU entries.

A.2.3.26.13 DomainNamesNumberOfEntries

This attribute indicates the number of domain name entries.

A.2.3.26.14 OperatorNamesNumberOfEntries

This attribute indicates the number of operator name entries.

A.2.3.26.15 NAIRealmsNumberOfEntries

This attribute indicates the number of NAI realm entries.

A.2.3.27 X_CABLELABS_COM_PasspointVenueNames Object

A table of Venue Name(s) where the access point is installed as shown below.

The X_CABLELABS_COM_PasspointVenueNames object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_Passpoint.VenueNames.{i}.

The device MUST support the X_CABLELABS_COM_PasspointVenueNames object if….

Table 34 - X_CABLELABS_COM_PasspointVenueNames Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Index	unsignedInt	RO				MUST
LanguageCode	string	RW	SIZE (2..3)			MUST
VenueName	hexBinary	RW	SIZE (1..504)			MUST

A.2.3.27.1 Index

Integer Index into the table.

A.2.3.27.2 LanguageCode

This attribute indicates if a 2 or 3 octet ISO-14962-1997 encoded string field that defines the language used in the Venue Name field. The code value is selected from ISO-639.

A.2.3.27.3 VenueName

This attribute indicates the Venue Name where the access point is installed. This additional meta data about the venue is included in the Venue Name ANQP-element. This parameter accepts UTF-8 encoded string represented as hexBinary string.

A.2.3.28 X_CABLELABS_COM_PasspointOperatorNames Object

The Operator Friendly Name element provides zero or more names of operators names who are operating the IEEE 802.11 AP (i.e., the Hotspot Operator).

The X_CABLELABS_COM_PasspointOperatorNames object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_Passpoint,OperatorNames.{i}.

Support for the X_CABLELABS_COM_PasspointOperatorNames object is a CONDITIONAL MUST.

Table 35 - X_CABLELABS_COM_PasspointOperatorNames Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Index	int	RO				MUST
LanguageCode	string	RW	SIZE (1..3)			MUST
OperatorName	hexBinary	RW	SIZE (1..504)			MUST

A.2.3.28.1 Index

Integer Index into the table.

A.2.3.28.2 LanguageCode

This attribute represents a 2 or 3 octet ISO-14962-1997 encoded string field that defines the language used in the Venue Name field. The code value is selected from ISO-639.

A.2.3.28.3 OperatorName

This attribute indicates the UTF-8 encoded (represented as hexBinary) OSU Provider Friendly Name in the human language identified by the language code. This parameter accepts UTF-8 encoded string represented as hexBinary string.

A.2.3.29 X_CABLELABS_COM_PasspointThreeGPPNetwork Object

This Object defines the Mobile Country Code (MCC) and Mobile Network Code (MNC) used by a mobile device to identify its home network.

The X_CABLELABS_COM_PasspointThreeGPPNetwork object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_PasspointThreeGPPNetwork.{i}.

The device MUST support the X_CABLELABS_COM_PasspointThreeGPPNetwork object if ….

Table 36 - X_CABLELABS_COM_Passpoint3GPPNetwork Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Index	unsignedInt	RO				MUST
MCC	string	RW	SIZE (3)			MUST
MNC	string	RW	SIZE (3)			MUST

A.2.3.29.1 MCC

This attribute indicates the 3 digit Mobile Country Code of the 3GPP Network.

A.2.3.29.2 MNC

This attribute indicates the 2 or 3 digit Mobile Network Code of the 3GPP Network.

A.2.3.30 X_CABLELABS_COM_PasspointConsortium Object

This Object defines the group of subscription service providers (SSPs) having inter-SSP roaming agreements. The format is the IEEE defined public organizationally unique identifier (OUI-24 or OUI-36).

The X_CABLELABS_COM_PasspointConsortium object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_ PasspointConsortium.{i}.

The device MUST support the X_CABLELABS_COM_PasspointConsortium object if xxxx.

Table 37 - X_CABLELABS_COM_PasspointConsortium Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Index	unsignedInt	RO				MUST
OI	Octet String	RO	SIZE (3|5)			MUST

A.2.3.30.1 OI

This attribute represents the Organization Identifier field shall contain a public organizationally unique identifier assigned by the IEEE. The Organization Identifier field is 3 octets in length if the organizationally unique identifier is an OUI, or 5 octets in length if the organizationally unique identifier is 36 bits in length.

A.2.3.31 X_CABLELABS_COM_PasspointDomainNames Object

This Object lists the Domain Name of the entity operating the IEEE 802.11 access network.

The X_CABLELABS_COM_PasspointDomainNames object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_PasspointDomainNames.{i}.

The device MUST support the X_CABLELABS_COM_PasspointDomainNames object if xxxx.

Table 38 - X_CABLELABS_COM_PasspointDomainNames Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Index	unsignedInt	RO				MUST
DomainName	Octet String	RO	SIZE (1..255)			

A.2.3.31.1 DomainName

This attribute representing the Domain Name field is of variable length and contains a domain name compliant with the "Preferred Name Syntax" as defined in [RFC 1035].

A.2.3.32 X_CABLELABS_COM_PasspointOSUProviders Object

A table of OSU Providers offering Online Sign Up service. This table is included in the OSU Provider sub-field in the OSU Provider List element.

The X_CABLELABS_COM_PasspointOSUProviders object is defined as a Cablelabs extension to [TR-181i2] as Device.Wi-Fi.AccessPoint.{i}.X_CABLELABS_COM_PasspointOSUProviders.{i}.

The device MUST support the X_CABLELABS_COM_PasspointOSUProviders object if.

Table 39 - X_CABLELABS_COM_PasspointOSUProviders Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
OSUServerURI	string	RW	SIZE (255)			MUST
OSUMethodsList	string	RW	SIZE (1..252)			MUST
OSUNAI	string	RW				MUST
NamesNumberOfEntries	Int	RO				MUST
IconsNumberOfEntries	Int	RO				MUST
ServiceDescriptionsNumberOfEntries	Int	RO				MUST

A.2.3.32.1 OSUServerURI

This attribute represents the URI of the OSU Server that is used for OSU with the Service Provider indicated in the Names table. It is formatted in accordance with the [RFC 3986].

A.2.3.32.2 OSUMethodsList

This attribute represents the comma separated list of OSU Method values represented as integers. The methods are listed in the Service Provider's preferred order with the most-preferred method first. Possible values (integers) are selected from Table 10 of [WFA].

A.2.3.32.3 OSUMethodsList

This attribute represents the NAI that is used for OSU with the Service Provider indicated in the Names table. OSUNAI is formatted in accordance with [RFC 4282].

A.2.3.32.4 NamesNumberOfEntries

This attribute represents the number of name entries.

A.2.3.32.5 IconsNumberOfEntries

This attribute represents the number of icon entries.

A.2.3.32.6 ServiceDescriptionsNumberOfEntries

This attribute represents the number of service description entries.

A.2.3.33 X_CABLELABS_COM_PasspointOSUProvidersNames Object

This Object lists the Online Sign Up list of OSU Providers Friendly Names that are included in the OSU Provider List element.

The X_CABLELABS_COM_PasspointOSUProvidersNames object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_PasspointOSUProvidersNames.

The device MUST support the X_CABLELABS_COM_PasspointOSUProvidersNames object if xxx.

Table 40 - X_CABLELABS_COM_PassPointOSUProvidersNames Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Index	unsignedInt	RO				MUST
LanguageCode	AdminString	RW	SIZE (255)			MUST
OSUProviderFriendlyName	AdminString	RW	SIZE (1..252)			MUST

A.2.3.33.1 LanguageCode

This attribute indicates a 2 or 3 octet ISO-14962-1997 encoded string field that defines the language used in the Venue Name field. The code value is selected from ISO-639.

A.2.3.33.2 OSUProviderFriendlyName

This attribute indicates the UTF-8 encoded (represented as hexBinary) OSU Provider Friendly Name in the human language identified by the language code. This parameter accepts UTF-8 encoded string represented as hexBinary string.

A.2.3.34 X_CABLELABS_COM_PasspointOSUProvidersIcons Object

A table of Icons that are included in the Icons Available subfield of the OSU Provider List element. The Icons Available subfield provides metadata about the OSU provider icon file(s) available for download.

The X_CABLELABS_COM_PasspointOSUProvidersIcons object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_PasspointOSUProvidersIcons.

The device MUST support the X_CABLELABS_COM_PasspointOSUProvidersIcons object if ….

Table 41 - X_CABLELABS_COM_PasspointOSUProvidersIcons Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
IconWidth	unsigned32	RW	SIZE (0..65535)			MUST
IconHeight	unsigned32	RW	SIZE (0..65535)			MUST
LanguageCode	string	RW	SIZE (3)			MUST
IconType	string	RW				MUST
IconFilename	string	RW				MUST

A.2.3.34.1 IconWidth

This attribute indicates the width in pixels of the OSU Provider icon named by the IconFilename.

A.2.3.34.2 IconHeight

This attribute indicates the height in pixels of the OSU Provider icon named by the IconFilename.

A.2.3.34.3 LanguageCode

This attribute represents a 2 or 3 octet ISO-14962-1997 encoded string field that defines the language used in the Icon file if any. The code value is selected from ISO-639. If there is no linguistic content to the icon/logo, the LanguageCode is set to "zxx"LanguageCode.

A.2.3.34.4 IconType

This attribute indicates the IconType is the MIME media type of the binary icon file named by the IconFilename. The IconType field is formatted in accordance with [RFC 6838] and its value is selected from the IANA MIME Media Types registered at http://www.iana.org/assignments/media-types/index.html.

A.2.3.34.5 IconFilename

This attribute indicates the IconFilename is a UTF-8 encoded field whose value contains the filename of the Icon having the metadata provided in this icon instance.

A.2.3.35 X_CABLELABS_COM_PasspointOSUProvidersServiceDescriptions Object

A table of OSU Service Descriptions included in the OSUServiceDescription subfield of the OSU Provider List element.

The X_CABLELABS_COM_PasspointOSUProvidersServiceDescriptions object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_PasspointOSUProvidersServiceDescriptions.{i}.

The device MUST support the X_CABLELABS_COM_PasspointOSUProvidersServiceDescriptions object if xxx.

Table 42 - X_CABLELABS_COM_PasspointOSUProvidersServiceDescriptions Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
LanguageCode	string	RW	SIZE (2 | 3)			MUST
ServiceDescription	Opaque	RW	SIZE (1..504)			MUST

A.2.3.35.1 LanguageCode

This attribute represents a 2 or 3 octet ISO-14962-1997 encoded string field that defines the language used in the Venue Name field. The code value is selected from ISO-639.

A.2.3.35.2 ServiceDescription

This attribute indicates the UTF-8 encoded (represented as hexBinary) string containing the ServiceProviders description of the service offering.

A.2.3.36 X_CABLELABS_COM_PasspointNAIRealms Object

The NAI Realm ANQP-element provides a list of network access identifier (NAI) realms corresponding to SSPs or other entities whose networks or services are accessible via this AP.

The X_CABLELABS_COM_PasspointNAIRealms object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_PasspointNAIRealms.{i}.

The device MUST support the X_CABLELABS_COM_PasspointNAIRealms object if xxx.

Table 43 - X_CABLELABS_COM_PasspointNAIRealms Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Index	int	RO				MUST
RealmEncodingType	int	RO	SIZE (0 | 1)			MUST
Realm	string	RO	SIZE (1..255)			MUST
EAPMethodsNumberOfEntries	int	RO				MUST

A.2.3.36.1 Index

A unique key for table indexing.

A.2.3.36.2 RealmEncodingType

The NAI Realm Encoding Type attribute is a 1-bit subfield. It is set to zero (0) to indicate that the NAI Realm in the NAI Realm subfield is formatted in accordance with [RFC 4282]. It is set to 1 to indicate it is a UTF-8 formatted character string that is not formatted in accordance with [RFC 4282].

A.2.3.36.3 Realm

This attribute represents the NAI Realm Name.

A.2.3.36.4 EAPMethodsNumberOfEntries

This attribute indicates the number of EAP method entries.

A.2.3.37 X_CABLELABS_COM_PasspointNAIRealmsEAPMethods Object

The list of supported EAP methods and associated parameters for each NAI Realm.

The X_CABLELABS_COM_PasspointNAIRealmsEAPMethods object is defined as a CableLabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_PasspointNAIRealmsEAPMethods.{i}.

The device MUST support the X_CABLELABS_COM_PasspointNAIRealmsEAPMethods object if xxxx.

Table 44 - X_CABLELABS_COM_PasspointNAIRealmsEAPMethods Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
EAPMethod	enum	RW	none(1), EAP-TLS(2), EAP-TTLS(3), PEAP(4), EAP-MSCHAPV2(5)	N/A	N/A	MUST
AuthenticationParametersNumberOfEntries	unsignedInt	RO		N/A	N/A	MUST

A.2.3.37.1 EAPMethod

This attribute indicates the enumerated value of the EAP method. The EAP Type value as given in IANA EAP Method Type Numbers.

A.2.3.37.2 AuthenticationParametersNumberOfEntries

This attribute represents the number of authentication parameter entries.

A.2.3.38 X_CABLELABS_COM_PasspointNAIRealmsEAPMethodsAuthenticationParameters Object

The list of supported EAP methods and associated parameters for each NAI Realm.

The X_CABLELABS_COM_PasspointNAIRealmsEAPMethodsAuthenticationParameters object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_ PasspointNAIRealmsEAPMethodsAuthenticationParameters.

The device MUST support X_CABLELABS_COM_PasspointNAIRealmsEAPMethodsAuthenticationParameters object if xxxx.

Table 45 - X_CABLELABS_COM_PasspointEAPMethodsAuthenticationParameters Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
ExpandedEAPMethodID	string	RO	SIZE (1..255)			MUST
ParameterValue	hexBinary	RW				MUST

A.2.3.38.1 ExpandedEAPMethodID

This attribute identifies the authentication parameter type as follows.

ID	Type
0	Reserved
1	Expanded EAP Method
2	Non-EAP Inner Authentication Type
3	Inner Authentication EAP Method Type
4	Expanded Inner EAP Method
5	Credential Type

ID	Type
6	Tunneled EAP Method Credential Type
221	Vendor Specific

A.2.3.38.2 ParameterValue

This attribute indicates the value encoded in hexBinary (octet string) format as per the section 8.4.4.10 of.[802.11].

A.2.3.39 X_CABLELABS_COM_PasspointWANMetrics Object

The X_CABLELABS_COM_PasspointWANMetrics object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_PasspointWANMetrics.

The device MUST support the X_CABLELABS_COM_PasspointWANMetrics object if xxxx.

Table 46 - X_CABLELABS_COM_PasspointWANMetrics Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
LinkStatus	string	RO	reserved(1), linkUp(2), linkDown(3), linkTest(4)			SHOULD
AtCapacity	boolean	RO				SHOULD
DownlinkSpeed	unsignedInt	RO				MUST
UplinkSpeed	unsignedInt	RO				MUST
DownlinkLoad	int	RO	0..100	percent		SHOULD
UplinkLoad	int	RO	0..100	percent		SHOULD

A.2.3.39.1 LinkStatus

The LinkStatus attribute reflects the status of the WAN Link.

A.2.3.39.2 AtCapacity

This attribute, if set to ‘true’, indicates the WAN link is at capacity and no additional mobile devices will be permitted to associate with the AP. If the value is set to ‘false’, additional mobile devices will continue to be permitted to associate.

A.2.3.39.3 DownlinkSpeed

This attribute is an estimate of the WAN backhaul link's current downlink speed in kilobits per second (kbps). The maximum value of this field is 4,294,967,296 kbps (approx. 4.2Tbps).

A.2.3.39.4 UplinkSpeed

This attribute is an estimate of the WAN backhaul link's current uplink speed in kilobits per second (kbps). The maximum value of this field is 4,294,967,296 kbps (approx. 4.2Tbps).

A.2.3.39.5 DownlinkLoad

This attribute is the current percentage % loading of the downlink WAN connection.

A.2.3.39.6 UplinkLoad

This attribute is the current percentage % loading of the uplink WAN connection.

A.2.3.40 X_CABLELABS_COM_PasspointOSU Object

The X_CABLELABS_COM_PasspointOSU object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_PasspointOSU.{i}.

The device MUST support X_CABLELABS_COM_PasspointOSU object if xxx.

Table 47 - X_CABLELABS_COM_PasspointOSU Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
OSUProvidersNumberOfEntries	unsignedInt	RO				MUST

A.2.3.40.1 OSUProvidersNumberOfEntries

This attribute represents the number of OSU provider entries.

A.2.3.41 AC

This object contains parameters related to Wi-Fi QoS for different 802.11e access categories (priorities).

The AC object is defined in [TR-181] as Device.WiFi.AccessPoint.{i}.AC{i}.

The AC object MUST be supported.

Table 48 - AC Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
AccessCategory	enum	RO	BE(1), BK(2), VI(3), VO(4)			MUST
Alias	string	RW	SIZE (64)			MUST
AIFSN	unsignedInt	RW	2..15			MUST
ECWMin	unsignedInt	RW	0..15			MUST
ECWMin	unsignedInt	RW	0..15			MUST
TxOpMax	unsignedInt	RW	0..255			MUST
AckPolicy	boolean	RW				MUST
OutQLenHistogramIntervals	string	RW				MUST
OutQLenHistogram	unsignedInt	RW				MUST

A.2.3.42 ACStats

This object contains statistics for different 802.11e access categories (priorities).

The ACStats object is defined in [TR-181i2] as Device.Wi-Fi.AccessPoint.{i}.AC{i}.Stats.

The ACStats object MUST be supported.

Table 49 - ACStats Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
BytesSent	unsignedLong	RO				MUST
BytesReceived	unsignedLong	RO				MUST
PacketsSent	unsignedLong	RO				MUST
PacketsReceived	unsignedLong	RO				MUST

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
ErrorsSent	unsignedInt	RO				MUST
ErrorsReceived	unsignedInt	RO				MUST
DiscardPacketsSent	unsignedInt	RO				MUST
DiscardPacketsReceived	unsignedInt	RO				MUST
RetransCount	unsignedInt	RO				MUST
OutQLenHistogram	string	RO				MUST

A.2.3.43 Accounting

This object contains the parameters related to RADIUS accounting functionality for the access point.

The Accounting object is defined in [TR-181i2] as Device.Wi-Fi.AccessPoint.{i}.Accounting.

The Accounting object SHOULD be supported.

Table 50 - Accounting Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Enable	boolean	RW				MAY
ServerIPAddr	string	RW	SIZE (45)			MAY
SecondaryServerIPAddr	string	RW	SIZE (45)			MAY
ServerPort	unsignedInt	RW				MAY
SecondaryServerPort	unsignedInt	RW				MAY
Secret	string	RW				MAY
SecondarySecret	string	RW				MAY
InterimInterval	unsignedInt	RW	0..60			MAY

A.2.3.44 X_CABLELABS_COM_RadiusSettings

This object is used to configure the additional Radius Server settings required for Wi-Fi Access Points.

The X_CABLELABS_COM_RadiusSettings object is defined as a Cablelabs extension to [TR-181i2] as Device.WiFi.AccessPoint.{i}.X_CABLELABS_COM_RadiusSettings.

The X_CABLELABS_COM_RadiusSettings object MUST be supported.

Table 51 - X_CABLELABS_COM_RadiusSettings Object

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
RadiusServerRetries	unsignedInt	RW			3	MUST
RadiusServerRequestTimeout	unsignedInt	RW		seconds	5	MUST
PMKLifetime	unsignedInt	RW		seconds	28800	MUST
PMKCachingEnable	boolean	RW	false true		false	MUST
PMKCachingInterval	unsignedInt	RW		seconds	300	MUST
MaxAuthenticationAttempts	unsignedInt	RW			3	MUST
BlacklistTableTimeout	unsignedInt	RW		seconds	600	MUST
IdentityRequestRetryInterval	unsignedInt	RW		seconds	5	MUST
QuietPeriodAfterFailedAuthentication	unsignedInt	RW				MUST

A.2.3.44.1 RadiusServerRetries

This attribute indicates the number of retries for Radius requests.

A.2.3.44.2 RadiusServerRequestTimeout

This attribute represents the Radius request timeout in seconds after which the request must be retransmitted for the number of retries available.

A.2.3.44.3 PMKLifetime

This attribute represents the default time after which a Wi-Fi client is forced to re-authenticate.

A.2.3.44.4 PMKCachingEnable

This attribute represents whether the caching of PMK is enabled or disabled.

A.2.3.44.5 PMKCachingInterval

This attribute indicates the time interval after which the PMKSA (Pairwise Master Key Security Association) cache is purged.

A.2.3.44.6 MaxAuthenticationAttempts

This attribute indicates the number of times a client can unsuccessfully attempt to login within incorrect credentials. When this limit is reached, the client is blacklisted and not allowed to attempt to login to the network. Setting this parameter to 0 (zero) disables the blacklisting feature.

A.2.3.44.7 BlacklistTableTimeout

This attribute indicates the time interval for which a client will continue to be blacklisted one it is marked so.

A.2.3.44.8 IdentityRequestRetryInterval

This attribute represents the time interval between identity request retries. A value of o (zero) disables retry interval.

A.2.3.44.9 QuietPeriodAfterFailedAuthentication

This attribute indicates the enforced quiet period (time interval) following a failed authentication attempt. A value of 0 (zero) disables quiet period.

A.2.3.45 X_CABLELABS_COM_SNMP

The Object represents an SNMP Agent on this device.

The X_CABLELABS_COM_SNMP object is a new object and does not extend any existing TR-181 objects.

The X_CABLELABS_COM_SNMP object MUST be supported.

Table 52 - X_CABLELABS_COM_SNMP

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Enable	boolean	RW			0	MUST
NMStationAccessNumberOfEntries	unsignedInt	RO				MUST

A.2.3.45.1 Enable

This parameter when set to 'true' enables the SNMP agent for this device.

A.2.3.45.2 NMStationAccessNumberOfEntries

This parameter defines the number X_CABLELABS_COM_NmStationAccess objects that currently exist.

A.2.3.44 X_CABLELABS_COM_NmStationAccess

The object controls access to SNMP objects by network management stations.

The X_CABLELABS_COM_NmStationAccess object is a new object and does not extend any existing TR-181 objects.

The X_CABLELABS_COM_NmStationAccess object MUST be supported if SNMP management is enabled.

Table 53 - X_CABLELABS_COM_NmStationAccess

Attribute Name	Type	Access	Type Constraints	Units	Default	Requirement
Alias	string	RW	SIZE(1..64)			MUST
StationAddress	IPAddress	RW				MUST
CommunityString	string	RW	SIZE(0..64)			MUST
AccessControl	enum	RW	none(1), read(2), readWrite(3), roWithTraps(4), rwWithTraps(5), trasOnly(6)			MUST

A.2.4 IEEE 802.11 MIB modules Requirements

Table 54 shows the compliance for IEEE [802.11] MIB objects. Unless otherwise noted, support for IEEE MIBs is deemed optional as current operator requirements for Wi-Fi requirements are included in Annex A.

The column Support indicates compliance requirement, with values MAY, MUST and NA (not applicable).

The column Access indicates the compliance requirement for access via SNMP request PDU messages. Possible values [RFC 2578] include 'read-only', 'read-write' and 'read-create'.

Table 54 - 802.11 MIB Requirements

802.11 MIB Objects	Support	Access
dot11StationConfigTable	MAY	read-only
dot11AuthenticationAlgorithms	MAY	read-only
dot11WEPDefaultKeysTable	MAY	read-only
WEPKeyMappings	MAY	read-only
dot11PrivacyTable	MAY	read-only
dot11MultiDomainCapability	MAY	read-only
dot11SpectrumManagement	MAY	read-only
dot11RSNAConfigTable	MAY	read-only
dot11RSNAConfigPairwiseCiphersTable	MAY	read-only
dot11RSNAConfigAuthenticationSuitesTable	MAY	read-only
dot11RSNAStatsTable	MAY	read-only
dot11RegulatoryClassesTable	MAY	read-only
dot11RRMRequestTable	MAY	read-only
dot11ChannelLoadReportTable	MAY	read-only
dot11NoiseHistogramReportTable	MAY	read-only
dot11BeaconReportTable	MAY	read-only

802.11 MIB Objects	Support	Access
dot11FrameReportTable	MAY	read-only
dot11STAStatisticsReportTable	MAY	read-only
dot11LCIReportTable	MAY	read-only
dot11TransmitStreamReportTable	MAY	read-only
dot11APChannelReportTable	MAY	read-only
dot11RRMNeighborReportTable	MAY	read-only
dot11HTStationConfigTable	MAY	read-only
dot11OperationTable	MAY	read-only
dot11CountersTable	MAY	read-only
dot11GroupAddressesTable	MAY	read-only
dot11EDCATable	MAY	read-only
dot11QAPEDCATable	MAY	read-only
dot11QosCountersTable	MAY	read-only
dot11ResourceInfoTable	MAY	read-only
dot11PhyOperationTable	MAY	read-only
dot11PhyOperationTable	MAY	read-only
dot11PhyAntennaTable	MAY	read-only
dot11PhyTxPowerTable	MAY	read-only
dot11PhyFHSSTable	NA	-
dotPhyDSSSTable	MAY	read-only
dot11PhyIRTable	NA	-
dot11RegDomainsSupportedTable	MAY	read-only
dot11AntennasListTable	MAY	read-only
dot11SupportedDataRatesTxTable	MAY	read-only
dot11SupportedDataRatesRxTable	MAY	read-only
dot11PhyOFDMTable	MAY	read-only
dot11PhyHRDSSSTable	MAY	read-only
dot11HoppingPatternTable	NA	-
dot11PhyERPTable	MAY	read-only
dot11PhyHTTable	MAY	read-only
dot11SupportedMCSTxTable	MAY	read-only
dot11SupportedMCSRxTable	MAY	read-only
dot11TransmitBeamformingConfigTable	MAY	read-only
dot11FastBSSTransitionConfigTable	MAY	read-only
dot11LCIDSETable	MAY	read-only

Annex B Events Content and Format

This section contains the definitions of events related to the Wi-Fi functionality. The events can be reported via different mechanisms, for example, Local Log, syslog, SNMP notifications, etc. Depending on the managed device containing the Wi-Fi component, the event mechanism varies. For example, a DOCSIS CM may report the events as part of a syslog message, an entry in the CM local log, or an SNMP notification.

Each row in Table 55 specifies a Wi-Fi GW event definition.

The "Process" and "Sub-Process" columns indicate in which stage the event happens. The "Priority" column indicates the priority the event is assigned. These priorities are defined in the docsDevEvLevel object of the Cable Device MIB [RFC 4639] and in the LEVEL field of the syslog.

The "Event Message" column specifies the event text. The Event Message text may include the symbols <TAGS> and any other tag, e.g., <BSSID> as defined below. Before the first tag there is always a space character. Tags are always separated by commas.

The "Message Notes and Details" column provides additional information about the event text in the "Event Message" column. Some of the text fields include variable information. The variables are explained in the "Message Notes and Details" column. For some events the "Message Notes and Details" column may include the keyword <Deprecated> to indicate this event is being deprecated and its implementation is optional.

For events where the "Event Message" or "Message Notes and Details" column includes other parameters such as <P1>, <P2>, …, <Pn>. There is a single space before and after any parameter <Px> in the Event Message text.

This specification defines the tags in Table 55 as part of the "Event Message" column:

Table 55 - Wi-Fi GW Event Definition

TAG	Description	Format*
<WG-MAC>	Wi-Fi GW MAC Address;	"WG-MAC=xx:xx:xx:xx:xx:xx", xx in lowercase
<STA-MAC>	MAC Address of the wireless station	"STA-MAC=xx:xx:xx:xx:xx:xx", xx in lowercase
<BSSID>	MAC Address of AP (e.g., neighbor AP);	"BSSID=xx:xx:xx:xx:xx:xx", xx in lowercase
<SSID>	SSID value (e.g., neighbor AP);	"BSSID=xx:xx:xx:xx:xx:xx", xx in lowercase
<IF>	Wi-Fi Interface Name	"IF=wlan0"
<ANPI>	Average Noise Plus Interference	"ANPI=nnn"
<ANPI>	Average Noise Plus Interference	"ANPI=nnn"
<ANPI-THRSHLD>	ANPI threshold	"ANPI-THRSHLD=mmm"
<SNR>	Signal to Noise Ratio	"SNR=nnn"
<SNR-THRSHLD>	SNR threshold	"SNR-THRSHLD=mmm"
<REASON-CODE>	Reason code of an indication of Disassociation, Deauthentication, DELTS, ELBA, or DLS Teardown per [802.11] Reason Code field section.	"REASON-CODE=nn"
<REASON-CODE-DESCR>	The meaning of the REASON-CODE per [802.11] Reason Code field section.	"REASON-CODE-DESCR=meaning Reason Code text"
<STATUS-CODE>	Status code in response to a request massage from a station per [802.11] Status Code field section.	"STATUS-CODE=nn"
<STATUS-CODE-DESCR>	The meaning of the STATUS-CODE per [802.11] Status Code field section.	"STATUS-CODE-DESCR=meaning Reason Code text"

Example Event Message:

Rouge IP Detected: WG-MAC=00:54:aa:3:78:01;BSSIS=00:af:e3:5b:55:89;SSID=Free Internet

The "Error Code Set" and Event ID are defined per [OSSIv3.0].

The "Requirement" Column indicates the normative requirement of the event.

The "Notification Name" Column indicates the identifier of the notification being sent e.g., SNMP Notification.

The Wi-Fi WG MAY append additional vendor-specific text to the end of the event text.

Table 56 - Event Format and Content

Process	Sub-Process	Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID	Require-ment	Notification Name
Connection	Association	Warning	Rouge AP Detected: <WG-MAC>;<BSSID>;<SSID>		X001.1	88.000101	SHOULD	SNMP: clabWIFIWIFIEventNotif
Connection	Association Termination	Warning	<REASON-CODE-DESCR>;<REASON-CODE>;<WG-MAC>;<STA-MAC>;<IF>	See Section B.1.1	X001.2	88000102	MUST	SNMP: clabWIFIWIFIEventNotif
Connection	Association Failure	Warning	<STATUS-CODE-DESCR>;<STATUS-CODE>;<WG-MAC>;<STA-MAC>;<IF>	See Section B.1.2	X001.3	88000103	MUST	SNMP: clabWIFIWIFIEventNotif
Connection	Authentication Failure	Warning	Station exceeds Authentication attempts: <WG-MAC>;<STA-MAC>;<IF>	See Section B.1.3	X001.4	88000104	SHOULD	SNMP: clabWIFIWIFIEventNotif
Connection	Association Failure	Warning	Station exceeds Association: <WG-MAC>;<STA-MAC>;<IF>	See Section B.1.4	X001.5	88000105	SHOULD	SNMP: clabWIFIWIFIEventNotif
Connection	Association	Warning	Station exceeds non-authenticated traffic: <WG-MAC>;<STA-MAC>;<IF>	See Section B.1.5	X001.6	88000106	SHOULD	SNMP: clabWIFIWIFIEventNotif
Connection	Association	Warning	Black Address List Detected: <WG-MAC>;<STA-MAC>;<IF>		X001.7	88000107	SHOULD	SNMP: clabWIFIWIFIEventNotif
Connection	Association	Warning	Black Address List Changed by operator <WG-MAC>		X001.8	88000108	SHOULD	SNMP: clabWIFIWIFIEventNotif
Operation	Failure	Error	Radio Failure: <WG-MAC>;<IF>		X002.1	88000201	MUST	SNMP: clabWIFIWIFIEventNotif
Operation	Thresholds Exceeded	Warning	Noise plus Interference exceeded threshold: <ANPI>;<ANPI-THRSHLD>;<IF>		X002.2	88000202	MUST	SNMP: clabWIFIWIFIEventNotif
Operation	Threshold Exceeded	Warning	SNR below threshold: <SNR>;<SNR-THRSHLD>;<STA-MAC>;<IF>		X002.3	88000203	MUST	SNMP: clabWIFIWIFIEventNotif
Operation	Failure	Warning	Interface Reset (Link Up/Down)		X002.4	88000205	MUST	linkUp, linkDown [RFC 2863]
Configuration	Updated	Information	Configuration Changed <P1>	P1: Config File | Management	X003.1	88000301	MUST	SNMP: clabWIFIWIFIEventNotif
Accounting	Failure	Error	Radius Failure:<STA-MAC>, Reason: <P1>	P1 = Vendor specific text	X003.1	88000301	MUST	SNMP: clabWIFIWIFIEventNotif

B.1 Special Event Requirements

This section details requirements of certain events of Table 56.

B.1.1 Requirements for Event X001.2

This section details management events generated when the Wi-Fi GW sends certain [802.11] unsolicited notifications to the station with particular Reason Code field value.

These events are specified per [802.11] notification occurrence, or per aggregation or threshold condition of those [802.11] notification messages as noted in Table 57.

The Wi-Fi GW MUST generate events of type X001.2 for the reason codes and conditions listed in Table 57.

Table 57 - Requirements for Event X001.2

Reason Code	Meaning	Occurrence	Policy	Additional Details
34	Disassociated because excessive number of frames need to be acknowledged, but are not acknowledged due to AP transmissions and/or poor channel conditions.	Per Occurrence	None	
5	Disassociated because AP is unable to handle all currently associated STAs	Per Occurrence	None	
23	IEEE 802.1X authentication per [802.1X] failed	Per Occurrence	None	
35	Disassociated because STA is transmitting outside the limits of its TXOPs	Per Occurrence	None	

B.1.2 Requirements for Event X001.3

This section details the management events generated by the Wi-Fi GW that relates to [802.11] responses to request messages from the client station with particular Status Code field value.

These events are specified per 802.11 response message occurrence, or per aggregation or threshold condition of those [802.11] notifications messages as noted in Table 58.

The Wi-Fi GTW MUST generate events of type X001.3 for the reason codes and conditions listed in Table 58.

Table 58 - Requirements for Event X001.3

Status Code	Meaning	Occurrence	Policy	Additional Details
13	Responding STA does not support the specified authentication algorithm.	Per occurrence	None	
17	Association denied because AP is unable to handle additional associated STAs.	Per occurrence	None	
34	Association denied due to excessive frame loss rates and/or poor conditions on current operating channel.	Per occurrence	None	

B.1.3 Requirements for Event X001.4

This section details the conditions to generate an event to report exceeding Authentication failures.

The Wi-Fi GW SHOULD generate events of type X001.4 for the reason codes and conditions listed in Table 59.

Table 59 - Requirements for Event X001.4

Reason Code	Meaning	Occurrence	Policy	Additional Details
14	Message integrity code (MIC) failure	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	

Reason Code	Meaning	Occurrence	Policy	Additional Details
15	4-Way Handshake timeout	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
16	Group Key Handshake timeout	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
17	Information element in 4-Way Handshake different from (Re)Association Request/Probe Response/Beacon frame	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
18	Invalid group cipher	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
19	Invalid pairwise cipher	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
20	Invalid AKMP	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
21	Unsupported RSN information element version	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
22	Invalid RSN information element capabilities	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
24	Cipher suite rejected because of the security policy	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
39	Requested from peer STA due to timeout	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
45	Peer STA does not support the requested cipher suite	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
14	Received an Authentication frame with authentication transaction sequence number out of expected sequence	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
15	Authentication rejected because of challenge failure	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
16	Authentication rejected due to timeout waiting for next frame in sequence	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
41	Invalid group cipher	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
42	Invalid pairwise cipher	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
43	Invalid AKMP	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
44	Unsupported RSN information element version	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
45	Invalid RSN information element capabilities	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	
46	Cipher suite rejected because of security policy	Count towards reaching Threshold	Threshold defined by the AuthenticationFailures attribute	

B.1.4 Requirements for Event X001.5

This section details the conditions to generate an event to report exceeding Association failures.

The Wi-Fi GTW SHOULD generate events of type X001.5 for the reason codes and conditions listed in Table 60.

Table 60 - Requirements for Event X001.5

Status Code	Meaning	Occurrence	Policy	Additional Details
18	Association denied due to requesting STA not supporting all of the data rates in the BSSBasicRateSet parameter.	Count towards reaching Threshold	Threshold defined by the AssociationFailures attribute	
19	Association denied due to requesting STA not supporting the short preamble option	Count towards reaching Threshold	Threshold defined by the AssociationFailures attribute	
20	Association denied due to requesting STA not supporting the PBCC modulation option	Count towards reaching Threshold	Threshold defined by the AssociationFailures attribute	
21	Association denied due to requesting STA not supporting the Channel Agility option	Count towards reaching Threshold	Threshold defined by the AssociationFailures attribute	
22	Association request rejected because Spectrum Management capability is required	Count towards reaching Threshold	Threshold defined by the AssociationFailures attribute	
23	Association request rejected because the information in the Power Capability element is unacceptable	Count towards reaching Threshold	Threshold defined by the AssociationFailures attribute	
24	Association request rejected because the information in the Supported Channels element is unacceptable	Count towards reaching Threshold	Threshold defined by the AssociationFailures attribute	
25	Association denied due to requesting STA not supporting the Short Slot Time option	Count towards reaching Threshold	Threshold defined by the AssociationFailures attribute	
26	Association denied due to requesting STA not supporting the DSSS-OFDM option	Count towards reaching Threshold	Threshold defined by the AssociationFailures attribute	

B.1.5 Requirements for Event X001.6

This section details the conditions to generate an event to report exceeding request from non-authenticated or non-associated station.

The Wi-Fi GTW SHOULD generate events of type X001.6 for the reason codes and conditions listed in Table 61.

Table 61 - Requirements for Event X001.6

Reason Code	Meaning	Occurrence	Policy	Additional Details
6	Class 2 frame received from nonauthenticated STA	Count towards reaching Threshold	Threshold defined by NonAuthenticatedTraffic	
7	Class 3 frame received from nonassociated STA	Count towards reaching Threshold	Threshold defined by NonAuthenticatedTraffic	
9	STA requesting (re)association is not authenticated with responding STA	Count towards reaching Threshold	Threshold defined by NonAuthenticatedTraffic	

Appendix I Acknowledgements

This specification reflects the work and contributions of many individuals. On behalf of CableLabs and its participating member companies, we would like to extend our sincere appreciation to all those who have contributed to the development of this specification. Special thanks are given to the following, ordered alphabetically by company name and individual's first names in each company.

Contributor(s), (Company Affiliation)

Azita Manson, Dan Torbet, Eli Baruch, Kurt Lumbatis (Arris)

Dave Park, Yong Chen (Belair Networks)

John Dickinson, Victor Blake (Bright House Networks)

Gordon Li, John McQueen (Broadcom)

Bernard McKibben, Eduardo Cardona, Josh Redmore, Luther Smith, Mark Poletti, Neeharika Allanki, Thomas Nogues, Vikas Sarawat (CableLabs)

Paul Hess, Michael Lariccio (Cablevision)

Charles Moreman (Cisco)

Doug Berman, Mark Harris, Theodore Cyril, Wajeeh Butt, Vinayak Bhat (Comcast)

John Coppola, Michael Gillin, Steve Dotson (Cox)

Keith Carter (Ruckus Wireless)

Linmei Shu, Yan Huang (SMC)

Matt Osman (Technicolor)

Satish Kumar (Texas Instruments)

Kevin Noll, Praveen Srivastava (Time Warner Cable)

Dawn Xie (ZTE USA)

Stephen Burroughs (CableLabs)

Appendix II Revision History

II.1 Engineering Change for WR-SP-WiFi-MGMT-I02-101005

ECN	ECN Date	Summary
WiFi-MGMT-N-10.0002-4.doc	9/27/2010	WiFi GW TR-69 support

II.2 Engineering Change for WR-SP-WiFi-MGMT-I03-120216

ECN	ECN Date	Summary
WiFi-MGMT-N-0006-5	1/6/2012	Clarifications and constraints to SNMP and TR-069 date models of the device gateway.

II.3 Engineering Changes for WR-SP-WiFi-MGMT-I04-140311

ECN	ECN Date	Summary	Author
WiFi-MGMT-N-12.0009-1 (superseded by WiFi-MGMT-N-14.0017-2)	6/25/2012	Correction in data type for WiFi GW MIB	Cardona
WiFi-MGMT-N-12.0013-1	2/4/2013	Correct the requirement strength for some MIB tables	Li
WiFi-MGMT-N-12.0014-1 (partially superseded by WiFi-MGMT-N-14.0017-2)	2/4/2013	Add provisioning support for 802.11ac	Li
WiFi-MGMT-N-14.0017-2	3/3/2014	Updates to Wifi Management Information Model and SNMP MIB for new objects and attributes	Hedstrom

II.4 Engineering Change for WR-SP-WiFi-MGMT-I05-141201

ECN	ECN Date	Summary	Author
WiFi-MGMT-N-14.0022-5	11/3/2014	Updates for Wireless Specification Suite	Burroughs

II.5 Engineering Changes for WR-SP-WiFi-MGMT-I06-160111

ECN	ECN Date	Summary	Author
WiFi-MGMT-N-15.0028-2	12/2/2015	WiFi MGMT Update to Object and Req Tables	Schnitzer
WiFi-MGMT-N-15.0029-1	12/2/2015	Annex A	Schnitzer
WiFi-MGMT-N-15.0030-1	12/2/2015	Updates to CLAB-WIFI-MIB	Schnitzer
WiFi-MGMT-N-15.0031-2	12/2/2015	CLAB-WIFI-EXT-TR-181 Update	Burroughs

II.6 Engineering Changes for WR-SP-WiFi-MGMT-I07-150512

ECN	ECN Date	ECN Title	Author
WiFi-MGMT-N-16.0032-1	3/16/2016	CLAB-WIFI-EXT-TR-181 Update	Schnitzer
WiFi-MGMT-N-16.0033-1	3/16/2016	Removal of section A.2.5	Schnitzer
WiFi-MGMT-N-16.0034-1	3/30/2016	Wifi Management MIB Update	McQueen

II.7 Engineering Change for WR-SP-WiFi-MGMT-I08-161213

ECN	ECN Date	ECN Title	Author
WiFi-MGMT-N-16.0035-3	8/3/2016	TR-181 Extensions Refinement	Burroughs

II.8 Engineering Change for WR-SP-WiFi-MGMT-I09-220621

ECN	ECN Date	ECN Title	Author
WiFi-MGMT-N-22.0036-2	6/2/2022	Update to Support TR-369	Burroughs

* * *