Quality of Service on Carrier Grade Wi-Fi

Source: Quality of Service Working Group
Author(s): WBA Members
Issue date: April 2017
Version: 1.00
Document status: Final

WIRELESS BROADBAND ALLIANCE
DRIVING NEXT WIRELESS EXPERIENCE

ABOUT THE WIRELESS BROADBAND ALLIANCE

Founded in 2003, the mission of the Wireless Broadband Alliance (WBA) is to accelerate global leadership for enabling of wireless services that are seamless, secure and interoperable. Building on our heritage of Next Generation Hotspot (NGH) and carrier Wi-Fi, WBA will continue to drive and support the adoption of Next Generation Wireless services across the entire public Wi-Fi ecosystem, including IoT, Converged Services, Smart Cities, 5G, etc. Today, membership includes major fixed operators such as BT, Comcast and Charter Communications; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Microsoft, Huawei Technologies, Google and Intel.

The WBA Board includes AT&T, Boingo Wireless, BT, China Telecom, Cisco Systems, Comcast, Intel, KT Corporation, Liberty Global, NTT DOCOMO, Orange and Ruckus Wireless. For a complete list of current WBA members, please click here.

Follow Wireless Broadband Alliance at:
www.twitter.com/wballiance
http://www.facebook.com/WirelessBroadbandAlliance
http://www.linkedin.com/groups?mostPopular=&gid=50482
https://plus.google.com/106744820987466669966/posts

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

UNDERTAKINGS AND LIMITATION OF LIABILITY

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement. In addition, the WBA (and all other organizations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organizations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organizations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third-parties.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

CONTENTS

1 Executive Summary 1
2 Introduction and Overview 2
3 Use Cases 5
3.1 Use case 1 – Discovery with Open/known SSID and HTTPS/REST Protocols 6
3.2 Use case 2 – Discovery with HTTPS/SOAP Protocols over any Network 6
3.3 Use case 3 – Discovery with ANQP protocol over HS 2.0 Network 7
3.4 Use case 4 – Discovery with HTTPS/OMA DM Protocols over Wi-Fi Network 8
3.5 Use case 5 – Discovery using LWM2M protocol over DTLS 8
4 QoS Metrics and KPIs 9
4.1 Quality of Service Metrics 9
4.1.1 Metric Categories 9
4.1.2 Metrics Information Flow 10
4.1.3 Metrics Definitions 11
4.1.4 Example Metrics Data Request API 16
4.2 KPI Reporting 21
4.2.1 QoS Dynamic Measurement and Reporting 22
4.2.2 Wi-Fi Network Monitoring Data Feed about the Network 22
4.2.3 Monitoring Data About Wi-Fi Devices 26
4.3 Metrics of Key Network Elements 28
5 QoS Architectural models 29
5.1 Service flow prioritization 29
5.1.1 Introduction 29
5.1.2 Service Classification 31
5.2 QoS Metrics Service Offering 32
5.2.1 QoS Requestor Layer 33
5.2.2 QoS API Specification Layer 34
5.3 QoS Provider Layer 35
5.3.1 QoS Provider Service Framework Layer 37
6 Metrics database and reporting 38
6.1 Service layer 39
6.2 Analysis and Knowledge layer 40
6.3 Collection and organization layer 40
6.4 Wi-Fi Monitored Data Reporting Interface 41
7 Security 42
7.1 Security Purpose by Component 42
7.2 Interface Security 43
Annex A. Desired KPIs 45

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

Tables

Table 4-1 Quality of Service Metrics description 11
Table 4-2 List of network elements and needed metrics 28
Table 5-1 Possible discovery types 34
Table 5-2 Summary recommended Levels of QoS service 37
Table 7-1 Security considerations for various interfaces 44

Figures

Figure 2-1 High level Carrier Wi-Fi QoS architecture 3
Figure 2-2 Flow of sections within whitepaper and topic focus 4
Figure 2-3 Carrier QoS service architectures and networking elements 5
Figure 4-1 Metric Categories 9
Figure 4-2 Wi-Fi Network Metrics Information Flow 11
Figure 4-3 Hierarchy of Wi-Fi network monitoring data objects 23
Figure 4-4 List of Wi-Fi network data objects in the hierarchy 23
Figure 4-5 Hierarchy of monitoring data objects of Wi-Fi devices seen by the network 26
Figure 4-6 List of network data objects of Wi-Fi devices seen by the Wi-Fi network 27
Figure 5-1 End-to-end QoS model 30
Figure 5-2 Controlling downstream QoS over Wi-Fi using DSCP 31
Figure 5-3 WMM Access Categories and back-off slots 32
Figure 5-4 QoS service offering architecture 33
Figure 6-1 expanded view of the QoS Provider Service Framework 39
Figure 6-2 Remote Wi-Fi network monitoring and interface with the QoS Provider Service Framework 41
Figure 7-1 Security consideration for QoS services 43

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

Executive Summary

Wi-Fi Standards are evolving with Carrier grade Wi-Fi deployment steadily picking up. Evolution of existing services and proliferation of new services is causing the industry to emphasize the Quality of Experience delivered to the end user. Also operators would like to offer differentiated services over a Carrier Wi-Fi network with guaranteed Quality of Service (QoS). Unfortunately, the traditional 3GPP style of imperative QoS does not work for WLAN Access technology due to its federated deployment architecture.

It has been long argued and believed that unlicensed spectrum has different characteristics compared to licensed spectrum. Particularly, services (like Wi-Fi) in unlicensed spectrum do not tend to provide the same level of Quality of Experience to the user as with services in licensed spectrum, at least not without having a custom solution developed by service providers. There has been good evolution on industry standards in recent years that allow a device to seamlessly and securely connect to Wi-Fi hotspots broadcasting in unlicensed spectrum. Hotspot 2.0 specifications from Wi-Fi Alliance and the NGH program from WBA have enabled device vendors, service providers, hub providers etc. to follow a set of industry standard protocols to alleviate issues when connecting to Wi-Fi networks and to provide a seamless secure mechanism similar to licensed cellular technologies. These alone will not be sufficient for improved Quality of Experience to the user; the seamless connection does not in any way assure a quality connection and thereby the user may be forced to turn off Wi-Fi in certain scenarios. There are currently several groups (in various industry standard forums and alliances), working to address this gap and there is not a single group that is looking at providing Quality of Experience. There are also custom solutions and setups available to achieve a perceived quality experience to the user.

The focus of this workgroup is to come up with an Industry standards based way to address the following topics:

- Understanding and prioritizing various Quality of Service metrics, so they can be used as a means to communicate the quality of a deployed Wi-Fi venue.
- QoS Service prioritization so traffic can be prioritized for an improved quality experience.
- Mechanism(s) to monitor the various QoS metrics in a deployed Wi-Fi network.
- Understanding the key performance indicators (KPIs) and standardizing them.
- Mechanisms and services to communicate the QoS metrics to a connecting device, allowing the device to learn about the Wi-Fi network before it decides to connect.
- A database structure to maintain the monitored network information, so it can be used to communicate the QoS metrics as well as for reporting.
- Finally, addressing security on all the above topics, so the exchanged information is protected.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

1 Introduction and Overview

Carrier Wi-Fi Quality of Service (QoS) describes a systematic approach consisting of Wi-Fi network performance data, underlying architecture and analytical algorithms to turn unprocessed performance data gathered from mobile devices and Wi-Fi infrastructure into useful metrics to enable Wi-Fi QoS discovery by remote devices accessing the Wi-Fi network.

QoS discovery provides pre-connect information about the Wi-Fi access points to allow a mobile device to decide whether it should connect, or continue to stay connected to Wi-Fi, or not. Hence, discovery can prevent a bad user experience while using the Wi-Fi network. Wi-Fi QoS metrics can be leveraged by mobile applications to improve their traffic flows such as: voice-over-Wi-Fi calling, policy based connection management and enforcement, virtual private networking over unsecured public Wi-Fi, or bi-directional video-based conference and collaboration.

Since Wi-Fi operates over unlicensed spectrum, it is subject to signal interference, utilization congestion, unpredictable degradation of performance and several other conditions. Nevertheless, Wi-Fi has gained significant adoption worldwide and has surpassed cellular data utilization – a usage trend not predicted until a few years ago.

While standards bodies such as Wi-Fi Alliance, IEEE and IETF continue to improve WLAN access and networking performance, WBA has been collaborating with the overall ecosystem consisting of service providers, hub providers, hardware vendors, software vendors and external standards bodies to promote creation or standardization of Wi-Fi QoS metrics and services that can be deployed to improve both user experience and Wi-Fi network performance.

This whitepaper embarks on the initial phase of this ecosystem collaboration effort to help with the following areas:

- Define an overall architecture to support QoS metrics collection, processing and discovery – See Figure 1-1 for the high level Carrier Wi-Fi QoS discovery and service offering architecture.
- Define and describe architectural components, types of data, security, APIs and interfaces within this architecture. See flow diagram Figure 1-2 for sectional flow within this whitepaper and the topic focus of each of the sections.
- Propose architectural details and, where applicable, provide implementation examples to support design, development and interoperability testing among ecosystem vendors, if such architecture is adopted. See Figure 1-3 for Carrier QoS service architectures and networking elements corresponding to the section flow in Figure 1-2.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

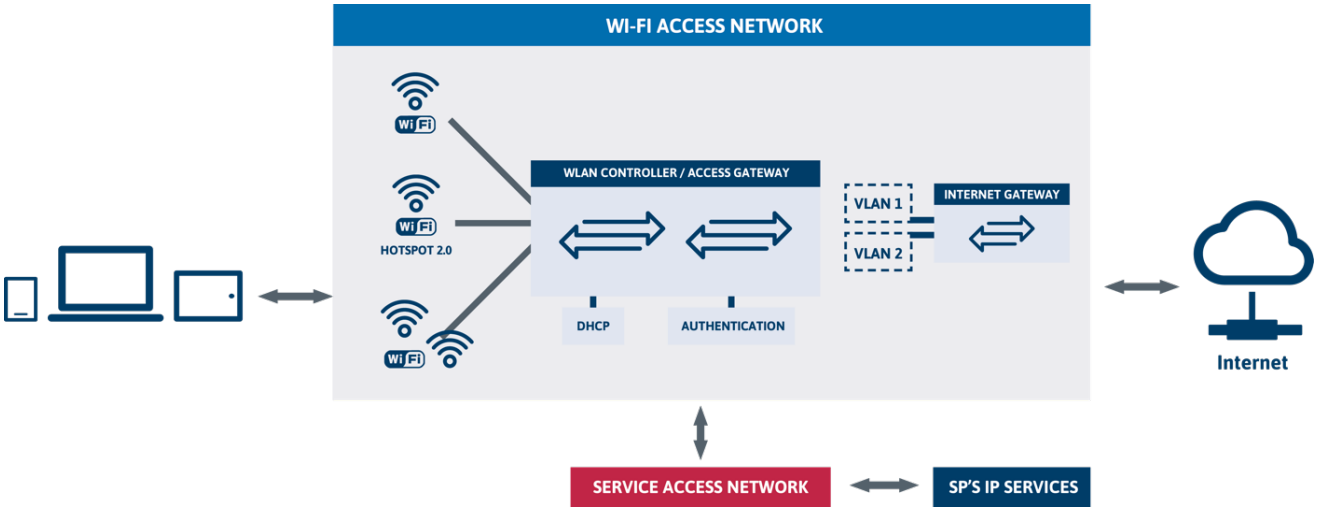


Figure 1-1 High level Carrier Wi-Fi QoS architecture

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

	1 - Executive summary	
0	2 - Whitepaper & architecture introduction	• Introduce Wi-Fi QoS architecture and key contents of various sections
1	3 – Business cases using API and protocols	• 5 API types/protocols: • HTTPS/REST • HTTPS/SOAP • HS 2.0 ANQP • HTTPS/OMA SyncML • DTLS/LWM2M
2	4.1-3 - Proposed types of QoS metrics	• Specify QoS metrics over airlink, venue and external network
3	4.2-3 - Measure and report dynamic QoS	• Remote Wi-Fi network measurement, feeding telemetry. • Describe QoS monitoring API for remote measurement reporting • Sample Wi-Fi performance data capturing
4	5.1.1-2 - Two QoS architectures	A) Service flow prioritization model B) QoS metrics service offering model
5	5.2- QoS service offering details	• QoS metrics service offering 4 key pillars: Requestor, API, Provider, and Provider Service Framework
6	6 - Metrics database & reporting	• QoS metrics service offering 3 layers: Service, analysis & knowledge, and collection & organization. • External interface for Wi-Fi monitored data report interface from telemetry system
7	7 - Security	• Define security proposal for inter-pillar interface API and data exchange
8	Appendix: List of Desired Wi-Fi KPI	• Proposed list of key performance indicators from the QOS framework

Figure 1-2 Flow of sections within whitepaper and topic focus

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

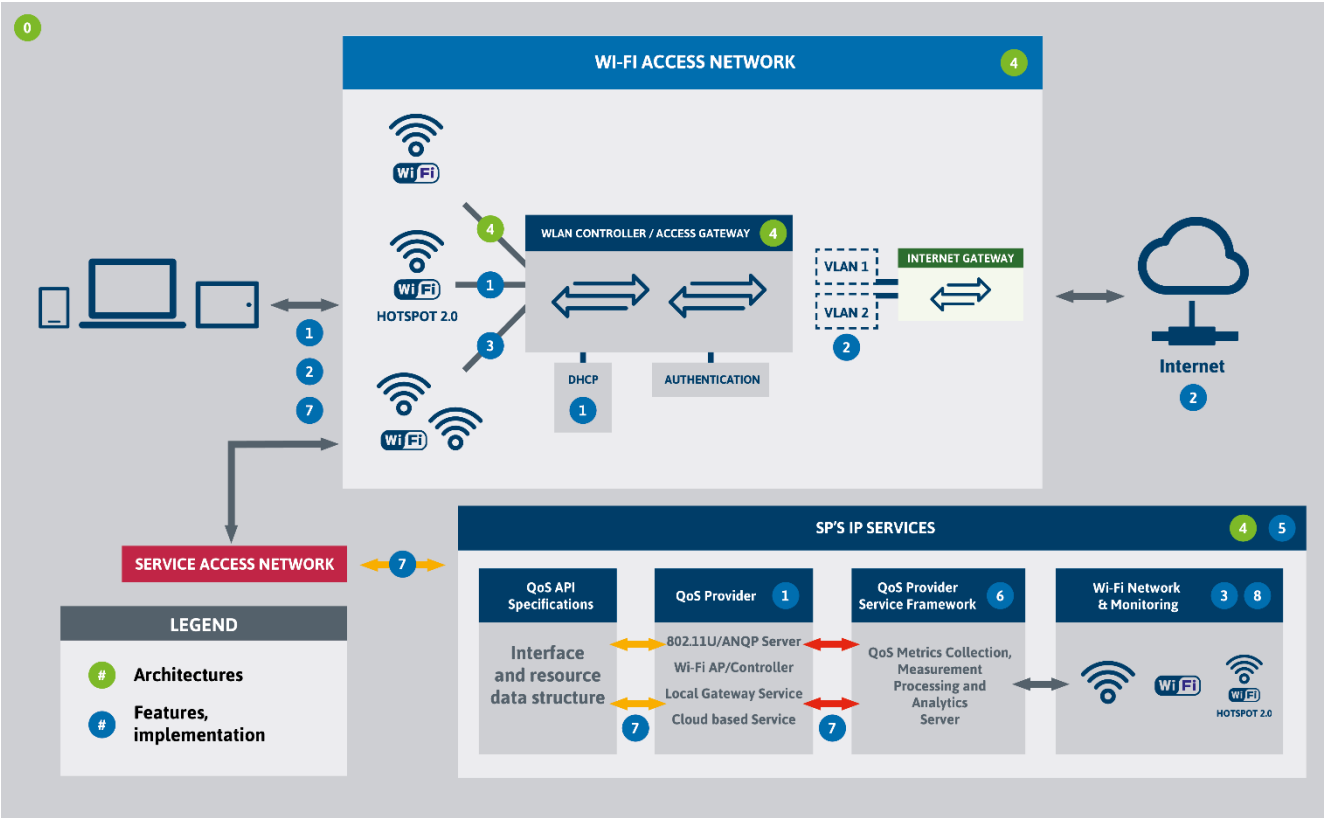


Figure 1-3 Carrier QoS service architectures and networking elements

2 Use Cases

This section provides some use case examples to illustrate the general concepts described in this paper. The examples are variations on the case where a mobile client obtains QoS metrics from a QoS service provider in order to select the best Wi-Fi access network.

It should be noted that other entities in the network may also request QoS metrics from the QoS service provider. For example, an AAA server could obtain QoS metrics to control network selection on behalf of a client that does not support the procedures described here.

Also note that these use cases are written assuming an application (app) is installed for QoS and other capabilities. These capabilities could also be provided as part of a pre-installed and/or built-in subsystem on the client device, with no significant change to the use case.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

2.1 Use case 1 – Discovery with Open/known SSID and HTTPS/REST Protocols

Background:

- Amy installs a Wi-Fi Calling app on her mobile device. This app is provisioned with information from Amy's service provider, including the QoS service URL to support QoS discovery using an Open or pre-arranged Wi-Fi SSID, using a call style of REST APIs over the HTTP/HTTPS protocol.

Description:

- At the start of use, the Wi-Fi Calling app scans and connects to an open or known SSID (with QoS services), and acquires an IP address.
- The Wi-Fi Calling app calls the QoS service URL using HTTPS / REST API from the Wi-Fi venue without restriction, and receives QoS metrics from the QoS Service Provider server.
- The Wi-Fi Calling app extracts the SSID, BSSID, uplink/downlink throughput, uplink/downlink speed, average round trip latency, average packet loss percentage, BSS loading, location, and time of last update for all available local Wi-Fi access networks.
- The Wi-Fi Calling app scans the Wi-Fi spectrum for usable SSIDs and BSSIDs, disconnects from the open SSID, and connects to an SSID / BSSID with good RSSI level, low latency, low packet loss, and high enough uplink & downlink throughputs.
- The Wi-Fi Calling app establishes a secure session to the SP gateway and starts a voice session.
- During the voice call session, the Wi-Fi Calling app periodically accesses the QoS Service Provider URL to retrieve updates of the QoS metrics. If the QoS metrics begin to fluctuate or indicate network performance trending below the performance thresholds, the Wi-Fi Calling app can select another high performance SSID/BSSID nearby or automatically switch to a 3GPP connection to maintain session continuity.

2.2 Use case 2 – Discovery with HTTPS/SOAP Protocols over any Network

Background:

- John travels to a new location without his SP presence, automatically searches for supported QoS discovery protocol types over 3GPP to identify available Wi-Fi APs in order to connect at the visiting service provider location.
- John's QoS app is configured to only support SOAP API calling convention over HTTP/HTTPS protocol.
- Note: This use case can use open SSID or support the SP's online search for the SP's own SSIDs and SSIDs for partner SPs offering QoS services.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

Description:

- John landed at the airport and turns on his mobile device. The QoS app performs QoS Service discovery by searching his SP's on-line service over a 3GPP connection to find local partner SPs who provide Wi-Fi access and QoS Services.
- The QoS app obtains several partner SP URLs and open SSIDs, the venue's service capability levels, and supported discovery protocol types. The QoS app selects a partner URL highest on the list that supports QoS discovery using SOAP API calling convention over HTTP/HTTPS.
- John walks into the airport terminal, the QoS app connects to the selected partner SP's open SSID, and automatically calls QoS Service URL using SOAP API over HTTPS to retrieve QoS metrics data elements.
- The QoS app parses the data elements and identifies an SSID/BSSID to switch to because it has the best quality metrics. The QoS app automatically connects to the high performance SSID/BSSID.
- If the previous step did not yield an acceptable SSID/BSSID (say, the local Wi-Fi network of the selected partner is congested), then the QoS app will repeat the above selection process using the next-highest partner URL on the list.

2.3 Use case 3 – Discovery with ANQP protocol over HS 2.0 Network

Background:

- Jane's device's QoS app discovers for QoS services to identify venue service capability level and protocol type using HS 2.0 and ANQP protocol.
- Note: This use case uses and proposes extension to ANQP and device HS 2.0 profile / API to discover and select Wi-Fi using more parameters.

Description:

- Jane has a HS 2.0 smartphone and lives in the city. Jane's SP provides HS 2.0 Wi-Fi access throughout the city.
- Jane walks to a coffee shop with a HS 2.0 AP, the QoS app interacts with the HS 2.0 API on the device to probe available networks using ANQP and receives ANQP payload(s) with QoS services fields, such as venue capability level, supported discovery protocol types, and QoS URLs to call, as well as domain, realm and consortium OI information.
- The QoS app further interacts with the device's HS 2.0 API to probe the networks for detailed QoS metrics and retrieves additional payloads, such as SSID/BSSID, BSS loading, average throughput, average latency, and average packet loss.
- The QoS app, using its internal policy preference, configures a dynamic Wi-Fi profile with only relevant Wi-Fi and QoS parameters to facilitate the HS 2.0 component selecting the preferred network and best AP identified by SSID/BSSID and various QoS metrics within acceptable thresholds.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

2.4 Use case 4 – Discovery with HTTPS/OMA DM Protocols over Wi-Fi Network

Background:

- Dave's mobile device already has an OMA DM agent and can receive firmware updates and new protocol updates such as DHCP with extensions.
- The device performs discovery for an OMA DM server, the venue's service capability, and discovery protocol types over Wi-Fi using DHCP protocol. Note: This use case assumes extensions to DHCP's client/protocol and the SP's DHCP server to include an optional field to exchange requests and responses.

Description:

- Dave works in an office building complex with multiple APs provided by a Wi-Fi service provider.
- Upon detecting an SSID to connect to, Dave's device sends a DHCP request with the Optional Request Option (ORO) field to discover the OMA DM Service. The DHCP server responds with OMA DM Service fields (indicated by option code, length, and payload that contains OMA DM Service IP address, venue's service capability level, and supported QoS discovery protocol types).
- The Device's OMA DM agent extracts the fields; it then accesses the OMA DM server using HTTPS and OMA SyncML protocols to update the management object tree with Wi-Fi QoS related parameters.
- Upon detection of new Wi-Fi QoS metrics, the QoS app uses these Wi-Fi management objects to identify the particular SSID/BSSID AP with highest QoS metrics and performance to connect to.

2.5 Use case 5 – Discovery using LWM2M protocol over DTLS

Background:

- The City of San Jose, CA deploys IoT sensors to measure and report air quality using a network of meshed Wi-Fi APs. The sensor devices contain pre-provisioned credentials, and policies with known Wi-Fi SSIDs, and QoS service URL/IP addresses, and known protocols to use for communication (for example DTLS security and OMA LWM2M protocol).

Description:

- The city air sensor periodically monitors air quality and stores data to a local storage buffer. When the buffer is full, it needs to connect with the city's SSID Wi-Fi network to upload data.
- The air sensor first connects to the city's known SSID, establishes DTLS secure session to the QoS service URL, and then uses LWM2M protocol to probe for link metrics (in particular uplink / downlink metrics).
- The QoS Service Provider component responds with link metrics.
- If the sensor determines uplink throughput is fast enough, the sensor uploads data and receives confirmation from the IoT server the data buffer has been

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

received successfully. The air sensor empties the data buffer and continues to monitor for air quality.

3 QoS Metrics and KPIs

3.1 Quality of Service Metrics

In order to make intelligent network selection decisions, a Wi-Fi client needs to know the capabilities and available capacity of its in-range Wi-Fi networks. For example, when a Wi-Fi client first enters an area that is served by Wi-Fi, it should select the network that provides the best performance, and it should avoid networks that are congested, or that block access to the user's mobile services (such as the network containing a firewall that blocks protocols required by VoWiFi). Or, if the Wi-Fi client is already connected to Wi-Fi, then it should monitor the performance of the in-range networks so it can switch to a better Wi-Fi or cellular network if the connected network becomes congested.

3.1.1 Metric Categories

The Wi-Fi network metrics are grouped into four different categories; Airlink, Venue, Backhaul, and End-to-End. These categories represent different segments of the network, as shown in Figure 3-1. For reference, the figure also shows the network segments defined in IEEE and Wi-Fi Alliance specifications.

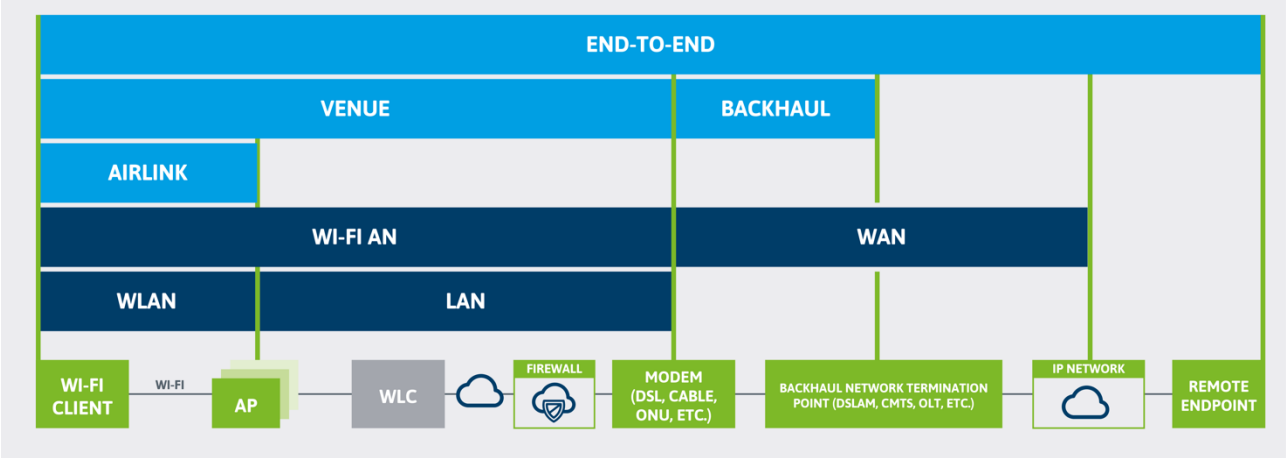


Figure 3-1 Metric Categories

- **Airlink** is the wireless air interface between the Wi-Fi Access Point and Wi-Fi client.
- **Venue** includes the in-venue network; i.e., the network between the AP and the demark point where the in-venue network connects to the external backhaul network. The demark point is normally located at a Cable Modem, DSL Modem, or ONU. The Venue segment may consist of a network of IP switches and routers, and may be shared by other wired or wireless endpoints. The Venue segment may also contain a Firewall that blocks certain types of upstream and downstream traffic.
- **Backhaul** includes the network segment that connects the Venue to the IP network; i.e., the segment from the Modem to the backhaul network termination point.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

End-to-End represents the sum total of all the individual end-to-end networks of the Wi-Fi clients connected to an AP. The end-to-end network of a Wi-Fi client is ephemeral in the sense that it exists only when there is some type of session established between the local and remote endpoint (e.g., a bi-directional real-time voice or video session with a remote phone, or a uni-directional video streaming session with a video content server). The End-to-End metrics of a Wi-Fi AP represent the average of the End-to-End metrics generated by all the clients connected to that AP.

3.1.2 Metrics Information Flow

The high level process for providing Wi-Fi metrics information to the Wi-Fi client is shown in Figure 3-2.

1. The Wi-Fi client, the AP, and other network components measure and collect raw metrics to indicate current network conditions, and send them to a centralized network-based Metrics Server. Some metrics, such as available bandwidth capacity, are dynamic in nature, and therefore need to be collected by the measuring entities and sent to the Metrics Server periodically. Other metrics, such as the firewall rule set, are more static, and can be provided to the server only once.
2. The Metrics Server performs post-processing and analytics on the received raw metrics, converting them into a form that reflects the overall health and capabilities of the Wi-Fi network.
3. The Wi-Fi client can query the Metrics Server when it first arrives at a new location, and periodically while it is connected to Wi-Fi, to ensure that it is always connected to the best available Wi-Fi network.
4. There is a small subset of metrics that does not pass through the Metrics Server. For example, some of the raw metrics that are used to generate Airlink metrics are sent directly from the AP to the Wi-Fi client. In addition, some of the Airlink metrics are collected and consumed locally at the Wi-Fi client.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

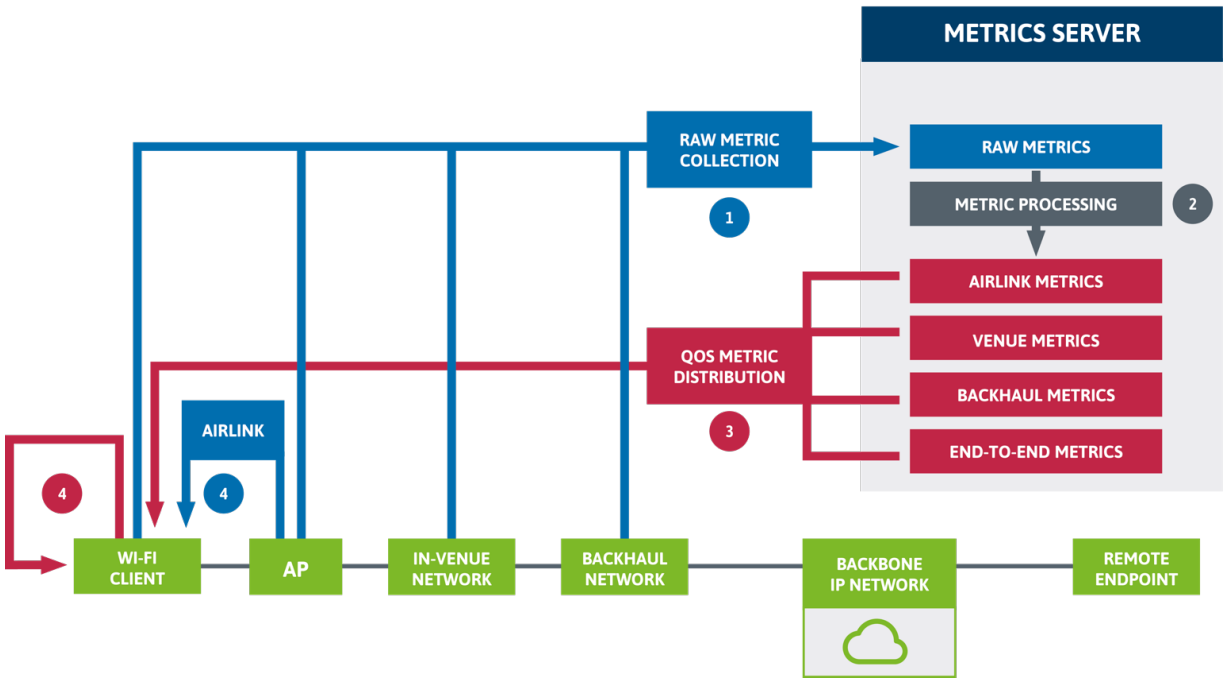


Figure 3-2 Wi-Fi Network Metrics Information Flow

3.1.3 Metrics Definitions

Table 3-1 lists the individual network performance and capability metrics that a Wi-Fi client requires in order to make intelligent network selection decisions.

NO.	METRIC DESCRIPTION	METRIC CATEGORY	PROGRAMS
1.	RSSI	Airlink	WFA MBO
2.	SNR		
3.	Hotspot Operating Class		
4.	Achievable WLAN Throughput		
5.	Load Management Duration	Venue	WFA, SCF, 3GPP
6.	Connection Capabilities a. Ports and Protocols b. Connection drop indicator c. LWA/LWIP support		
7.	Deployment a. Antenna coverage b. Service indicator, c. Mesh/Non-mesh indicator d. Hops count		
8.	WAN Metrics (Downlink and Uplink throughput) Throughput per frequency band	Backhaul	WFA, SCF, 3GPP
9.	Latency	End-to-End	WFA Mobile Multimedia
10.	Packet Loss		
11.	Jitter		

Table 3-1 Quality of Service Metrics description

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

The metrics are defined as follows:

- Airlink metrics:
  - RSSI
    - **Description:** RSSI is the received Wi-Fi signal strength in dBm at the Wi-Fi client. This metric is measured and consumed locally at the Wi-Fi client itself, and is not reported to the network. The Wi-Fi client is able to measure the RSSI of all in-range networks. For non-connected in-range networks, the Wi-Fi client can measure the RSSI of the Beacon.
    - **Granularity:** per Wi-Fi client per AP
    - **Standards reference:** IEEE Std 802.11-2016 [1] BeaconRSSI
  - SNR
    - **Description:** SNR is the received signal-to-noise ratio measured at the Wi-Fi client. This metric is measured and consumed locally at the Wi-Fi client itself, and is not reported to the network. The Wi-Fi client is able to measure the SNR of all in-range networks. For non-connected in-range networks, the Wi-Fi client can measure the SNR of the Beacon.
    - **Granularity:** per Wi-Fi client per AP
    - **Standards reference:** IEEE Std 802.11-2016 [1] BeaconSNR
  - Hotspot Operating Class
    - **Description:** Hotspot Operating Class is a scalar that references pre-defined values for a set of radio parameters supported by an AP; radio parameters such as channel frequencies and channel width.
    - **Granularity:** per AP
    - **Standards reference:** IEEE Std 802.11-2016 [1]
  - Estimated WLAN Throughput
    - **Description:** This metric is an estimate of the downlink and uplink throughput that is available to a specific Wi-Fi client via a specific AP. This metric is calculated and consumed locally at the Wi-Fi client itself. The Wi-Fi client calculates its estimated throughput based on information the Wi-Fi client obtains from the AP, such as fractional available airtime, Block Ack Window size, and target PPDU duration, combined with information known locally by the client (perhaps application-specific), such as average MSDU size, and parameters of the current link to the AP (RSSI, number of spatial streams, and channel bandwidth). This metric provides values for both uplink and downlink throughput. The value of this metric for can vary per application. For example, for a given set of network conditions, the WLAN throughput available for VoWiFi may differ from the WLAN throughput available for video streaming. Implementers must take this into account, so that each application in the Wi-Fi client receives a metric value that reflects the throughput available to that application.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

- **Granularity:** per Wi-Fi client per AP
- **Standards reference:** IEEE Std 802.11-2016 [1]

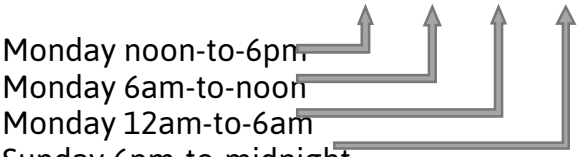
- Venue metrics:
  - Load Management Duration
    - **Description:** A measure of how frequently WAN metrics are collected.
    - **Granularity:** per Wi-Fi client per AP
    - **Standards reference:** Wi-Fi Alliance Hotspot 2.0 [5]
  - Connection Capabilities
    - Ports and Protocols
      - **Description:** Specifies the layer-3 protocols and port ranges that are supported
    - Connection drop indicator
      - **Description:** Indicates the number of Wi-Fi clients that abnormally disconnected from the AP. This metric is based on "abnormal disconnect" events reported by both the UE and the AP. If the UE is abnormally disconnected from the AP (say the AP is turned off), then it can report an abnormal disconnect event once it reconnects (to the same or different AP). Likewise, the AP can report the number of abnormal disconnect events from its perspective.
      - A more detailed description of this metric is left for later specification work. But for illustrative purposes, it could be defined such that the percentage of disconnect events are calculated per some sampling interval, and the results are reported as an array of the most recent 'n' sampling intervals. Both the sampling interval duration and the number of sampling intervals reported could be configurable.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

For example, if the metric is configured to collect 4 sampling intervals per day, then the sampling intervals could be as follows:
1st interval - 12am to 6am,
2nd interval - 6am to noon,
3rd interval - noon to 6pm,
4th interval - 6pm to midnight

If a UE requests this metric mid-day today, then it would receive results for the most recent day's worth of sampling intervals, which would include sampling intervals from today and yesterday. For example, if a UE requests this metric at 8pm on Monday (for example) then it would receive the number of sample intervals, and results of the previous 4 sampling intervals as follows:

Sample count = 4
Results array = [15%, 10%, 25%, 8%]



- LWA/LWIP support
  - **Description:** This is a data element reported by the venue during discovery that indicates the level of support for two link aggregation mechanisms; LWIP (LTE WLAN Radio Level Integration with IPsec Tunnel) and LWA (LTE-WLAN Aggregation).
  - **Granularity:** per AP
  - **Standards reference:** WBA white-paper Unlicensed Spectrum LTE Overview.
- Deployment
  - Antenna coverage
    - **Description:** The main purpose of this metric is to provide information that helps a user navigate to a location where the user will receive optimal performance. For example, the metric could render a "heat map" on the phone's display showing the coverage and health of the multiple nearby networks, thus providing the user with sufficient information to navigate to the best (e.g., least congested) local network. This would be especially useful in a venue covered by AP's supporting directional antennas. In another example, the metric could simply send location information to the user in the form of a text-string; e.g., "the network you're looking for is on the 2nd floor".
  - Service indicator
    - **Description:** this is part of HS 2.0 indicator to allow device to understand the venue support for HS 2.0.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

- **Granularity:** per AP
- **Standards reference:** Wi-Fi Alliance Passpoint specifications [5].

- Network Continuity Indicator
  - **Description:** This metric indicates the level of continuity provided across the APs of a Wi-Fi network (i.e., across the APs for a given SSID). In this context, the term "continuity" refers to two network attributes; support for seamless handover, and uniformity of congestion. A network that reports a "high" Network Continuity Indicator value will provide seamless handover as the UE switches from one AP to another, and will guarantees a relatively uniform level of congestion across all APs in the network. A network that reports a "low" Network Continuity Indicator" will provide neither seamless handover nor uniform congestion. The UE's connection manager can use this information to determine whether it needs to perform session handover procedures when it switches from one AP to another, and to determine the frequency of requesting Wi-Fi metrics. For example, in a low-continuity network, there can be a large change in congestion from one AP to another, in which case the UE should request a new set of Wi-Fi metrics whenever it switches between APs. A high level of continuity is normally provided by mesh Wi-Fi networks, while non-mesh networks provide a low level of continuity.
  - **Granularity:** per SSID
  - **Standards reference:** None.

- Venue Latency
  - **Description:** a measure of the upstream and downstream transit times across the Venue network.
  - **Granularity:** per AP
  - **Standards reference:** None.

- Backhaul Metrics:
  - WAN Downlink and Uplink Throughput
    - **Description:** This metric is a measure of the currently available Downlink and Uplink capacity through the Venue segment for a specific AP. It includes capacity limitations both in the Venue network itself, and in the Backhaul network that connects the Venue to the backbone IP network.
    - **Granularity:** per AP
    - **Standards reference:** The Downlink Speed and Uplink Speed fields in the WAN Metrics Element defined in Hotspot 2.0

- End-to-End metrics:
  - Each Wi-Fi client measures end-to-end metrics for its established sessions, and reports them periodically to a network-based repository. The combined metrics reported by all Wi-Fi clients connected to an AP are then averaged to produce an

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

overall metric for the AP. This averaging technique provides a set of metrics that reflect the health of the local access network. For example, if only one of the many Wi-Fi clients connected to an AP reports high latency numbers, then the latency is likely not being caused by the local access network. But if all of the Wi-Fi clients connected to an AP report high latency numbers, then it is reasonable to assume that the local access network is causing high latency.

- Latency

  Description: A measure of the mean upstream and downstream transit times for packets sent from the remote endpoint to the local Wi-Fi client (averaged across all clients connected to the AP). This metric does not include delays introduced by processes internal to the Wi-Fi client (e.g., jitter buffer or codec encode/decode delays). This metric provides values for both uplink and downlink latency, when available.

  - **Granularity:** per AP
  - **Standards reference:** None. This metric is defined for real-time media (e.g., RFC 3550 [8] and RFC 3611 [9]), but a more generic definition is needed that applies to all services.

- Packet Loss
  - **Description:** A measure of the difference between the packets sent from a remote endpoint and the packets received by the Wi-Fi client over the most recent 10-second interval (averaged across all clients connected to the AP).
  - **Granularity:** per AP
  - **Standards reference:** None. This metric is defined for real-time media (e.g., RFC 3550 [8] and RFC 3611 [9]), but a more generic definition is needed that applies to all services.

- Jitter
  - **Description:** Jitter only has meaning for services such as real-time voice or streaming video, where packets are received at a regular interval. Jitter is a measure of the mean deviation in end-to-end transit time of packets in a received packet stream (averaged across all clients connected to the AP). High levels of jitter can result in either large jitter buffers (thus increasing latency), or discarded packets (resulting in lower quality).
  - **Granularity:** per AP
  - **Standards reference:** None. This metric is defined for real-time media (e.g., RFC 3550 [8]), but a more generic definition is needed that applies to all services.

3.1.4 Example Metrics Data Request API

- **Scenario:** A UE device has been provisioned with a Passpoint profile and is currently in a venue that is broadcasting the Passpoint signal, and the AAA server performs the QoS query on the UE's behalf. The sequence is as follows:
  - UE device starts an automatic connection with the Passpoint network

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

- Request is routed to AAA server
- AAA server successfully authenticates the UE device, but before returning a “success” response, it evaluates the Network QoS for authorization.
- AAA server calls the below qos_getdata API
- AAA server evaluates the returned QoS metrics. If the QoS metrics indicate that the network can support the UE’s services, then the AAA server returns a “success” response indicating that the UE can use the Wi-Fi network. Otherwise, the AAA server returns a “failed” response.
- API Description: Resource end point to read QoS data from the database. The API gets QoS metrics data from the database, based on supplied input data. Data shall always be returned for a particular Access Point. If Access Point specific data is not available, the API defaults to venue data.

- Request
  - URL: https://[host]/[service_request]
  - Host: api.example.com
  - service_request: qos_getdata
  - Method: POST
  - Header: In addition to any security related headers, only Content-Type needs to be set.
  - Content-Type: "application/json"
  - Query String: None
  - Body: JSON object key value pairs with the following format. Note that when a key has no value, it should be set to the JSON keyword null, for both numbers and string. Any missing key shall be treated as null. For values where defaults are defined, if no value is set the default value shall be applied.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

KEY	DESCRIPTION	COMMENT	MANDATORY	JSON TYPE
request_type	Identifies the data request type for WAN Metrics (downlink, uplink and load) 0: (Default) Returns the last recorded data in the database 1: In addition to the last recorded data, an average of upto last 5 entrees shall be returned	The average computation applies only for WAN Metrics data values namely downlink, uplink and load values.	Mandatory, default value is set to 0	Number
ap_bssid	Unique unhashed BSSID value of the Access point	An Access point can broadcast multiple SSIDs and each SSID can have an associated MAC value. Besides these there shall be a BSSID value that shall be unique to the AP and independent of the SSID. AAA Access_Request has a Called-Station-Id, that will contain the BSSID value and this value needs to be passed here.	NO	String
ssid	Identifies the SSID	SSID	NO	String
client_mac	MAC address of the device that is currently requesting for a connection	This value shall be present in Calling-Station-Id of AAA's Access_Request record.	NO	String
venue	Venue Information	Venue access server id	Mandatory	String
version	Identifies the version of the API	Default value is 1.	Mandatory	Integer

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

- JSON Request Sample

```
https://api.example.com/1/qos_getdata
{
      "request_type":0,
      "ap_bssid": "42-80-22-86-14-01",
      "ssid":"Passpoint SSID",
      "client_mac": "97-80-FA-12-72-A2",
      "venue": "lax",
      "version":1
}
```

- Response
  - **HTTP Status:** On success, the API shall answer with an HTTP 200 status. On failure, any other code other than 200 shall be returned, particularly the following ones
  - 400: Bad request: indicates a not well-formed request (ex: Invalid JSON request or required data in the original request is not available)
  - 500: Internal server error
  - 204: The server successfully processed the request and is not returning any content
  - **Header:** In addition to status code, the "Content-Length" and "Content-Type: needs to be set. Any other header may or may not be set.
  - **ErrorType:** Business exceptions are defined by QoS developers which could be NoDataFoundException, BadRequestException or InternalServerException.
  - **ErrorMessage:** In case, request contains invalid or bad formatted contents , also empty data result is returned, the returning JSON ErroMessage should include original request body in addition to error explanation wordings for non-technical users when ErrorType is BadRequestException, error explanation words are "invalid xxxx provided or not formated per specification" when ErrorType is NoDataFoundException, error explanation words are "the server successfully processed the request and is not returning any context" when ErrorType is InternalServerException, error explanation words are "Unable to reach database"
  - **Body:** JSON object with the following format shall be returned.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

KEY	DESCRIPTION	COMMENT	MANDATORY	JSON TYPE
downlink	Downlink speed as recorded at the AP/venue.	In Kbps	Mandatory	Integer
uplink	Uplink speed as recorded at the AP/venue.	In Kbps	Mandatory	Integer
load	Number of connected (associated) clients on the Access Point	Integer value	Mandatory	Integer
lmd	Load Management duration, saying how frequently WAN data (downlink, uplink) gets computed	Integer value in minutes	NO	Integer
rssi	Received Signal Strength indicator	In decibels	NO	String
snr	Signal to Noise Ratio	In decibels	NO	String
downlink_avg	Same as downlink, except that the data shall be an average of the last 5 entrees	Shall be returned only request_type in request is set to 1	NO	Integer
uplink_avg	Same as uplink, except that the data shall be an average of the last 5 entrees	Shall be returned only request_type in request is set to 1	NO	Integer
load_avg	Same as load, except that the data shall be an average of the last 5 entrees	Shall be returned only request_type in request is set to 1	NO	Integer

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

- JSON Response Sample

```
Cache-Control: no-cache, no-store
Content-Type: application/json;charset=UTF-8
Date: Fri, 28 Apr 2016 12:21:55 GMT
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Transfer-Encoding: chunked
{
	"downlink": "5055",
	"uplink": "3000",
	"load": "15",
	"lmd": "20",
	"rssi": "-80dB",
	"snr": "60",
	"lat":"-34.1112",
	"long":"-36.186"
}
```

In case where request_type is 1, then the response format shall be as follows

```
Cache-Control: no-cache, no-store
Content-Type: application/json;charset=UTF-8
Date: Fri, 28 Apr 2015 12:21:55 GMT
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Transfer-Encoding: chunked
{
	"downlink": "5055",
	"uplink": "3000",
	"load": "15",
	"lmd": "20",
	"downlink_avg": "5055",
	"uplink_avg": "3000",
	"load_avg": "15",
	"rssi": "-80dB",
	"snr": "60",
	"lat":"-34.1112",
	"long":"-36.186"
}
```

3.2 KPI Reporting

Wi-Fi network Key Performance Indicators (KPI) provide the Wi-Fi service provider with important data points and patterns about its network health, performance and availability.

Wi-Fi network KPI data can be derived from network measurement metrics that are generated from probing, measuring, testing, collecting, and monitoring actions against network components (for example: use ICMP to measure round trip time in milliseconds between AP and network core, collect signal and noise levels from all AP within a location, collect number of concurrent device sessions by AP, and so forth) - see Annex A for a list of proposed KPI.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

The following sections describe sample operations to retrieve network metrics to generate needed KPI.

3.2.1 QoS Dynamic Measurement and Reporting

Wi-Fi network performance monitoring and reporting is a critical operation of the QoS Service Provider Framework component where raw and processed Wi-Fi network and device performance data objects are collected and entered into the system for analysis. Frequent and dynamic measurements from Wi-Fi networks and devices contribute to providing near real time view and discovery of QoS metrics data.

Dynamic measurements of Wi-Fi performance should facilitate subsequent transfer of monitoring data objects to the QoS Service Provider Framework using sample API such as those in section 3.2.2 and 3.2.3. Dynamic monitoring data objects can be pulled from or pushed to the QoS Service Provider Framework on a regular basis.

Computation of such dynamic monitoring data once reported can be performed on a real-time or deferred-mode basis to enable discovery and consumption of QoS metrics data. Refer to sections 4.2 and 5 for information on architecture, data organization, aggregation, visualization and intra-system communication interfaces, in which algorithmic functions play an important role in turning monitored data objects into QoS metrics for consumption by QoS Requestors.

3.2.2 Wi-Fi Network Monitoring Data Feed about the Network

The Collection and Organization Layer of the QoS Service Provider Framework should interface with the Wi-Fi monitoring system to process such data streams. Such monitoring data streams can be posted or periodically requested depending on the capability of the system. The following diagrams depicts groups of data objects and web based API to transmit data securely from the Wi-Fi monitoring system to the QoS Service Provider Framework component.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

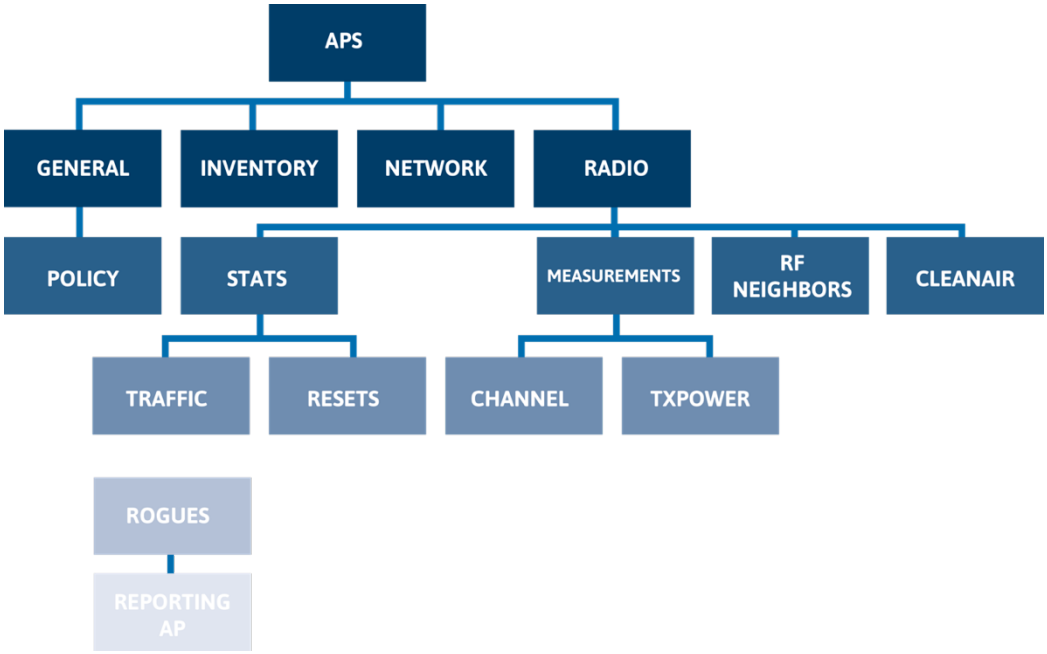


Figure 3-3 Hierarchy of Wi-Fi network monitoring data objects

AP	MAC Address, Ethernet MAC
General	Name, WLC, AP Group, Flex Group, Mode, Submode
General – Policy	ATF, AVC Policy
Inventory	Serial Number, Model, Location
Network	IPv4, IPv6, CDP, LLDP
Radio	Slot, Frequency, Protocol, State, Admin Status, CleanAir Status
Radio – Stats - Traffic	Data Rate, Tx Bytes, Rx Bytes
Radio – Stats - Reset	Reason, Crash Count, Soft Reset Count
Policies - QoS	Level, WMM, UAPSD, mDNS
Measurements - Channel	RSSI, Noise
Measurements – TxPower	Interference, Air Quality, Client Count, Join Time
RF Neighbours	MAC, Channel, Channel Width, Tx Power, Avg. RSSI
Clean Air	MAC, device, RSSI, Status

Rogues	Rogue MAC, Wired
Reporting AP	AP MAC, Channel, Channel width, SSID, RSSI, SNR

Figure 3-4 List of Wi-Fi network data objects in the hierarchy

- **Sample QoS Monitoring REST API**
  - It is recommended that the protocol be implemented, between the Wi-Fi monitoring system and the QoS Service Provider Framework, using one or more of the following protocols:

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

a) web security transport such as HTTPS/TLS/DTLS with mutual authentication if possible

b) virtual private networking gateway (VPN) with mutual authentication secure tunneling

c) protocols within service provider's private networks

- **REST API Example**
  - **Sample Request from QoS Service Provider Framework to the Wi-Fi Monitoring system to Retrieve Wi-Fi data objects**

```
POST / QoSMonReq HTTP/1.1
Accept: application/json
Content-Type: application-json
Content-Length: ###
{
      "MonParms":
      {
      "general": {"APgroup":"PasspointGroup", "WLC":"SP_WLC_1"},
      "policy": {"ATF":"Wi-FiPPPolicy_1", "AVCPolicy":"AVCPolicy_2"},
      "inventorylocation":"Philadelphia, PA 19101",
      // other fields .....
      }
}
```

- **Sample Error Response from Wi-Fi Monitoring system – error event**

```
HTTP/1.1 400 Bad Request
Content-Type: application-json
Content-Length: ###
{
        "error": {"code":12345, "message":"[Unknown or Incorrect WLC group ID]"},
}
```


Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

- **Sample Response to a Request from Wi-Fi Monitoring system to the QoS Service Provider Framework with data objects**

```
HTTP/1.1 200 OK
Content-Type: application-json
Content-Length: ###
{
        “resultstatus”: 200,
        "Wi-FiPerfResp:
        {
                “general”:  {“SSID”:”SP_Passpoint1”, “BSSID”:”AA:34:2C:BC:78:A1”},
                “APgroup”: {”PasspointGroup”:”1”, “WLC”:”SP_WLC_1” , “submode”:”modePP”},
                “generalpolicy”: {ATF:”Wi-FiPPPolicy_1”, AVCPolicy:”AVCPolicy_2”} ,
                “inventorylocation”:
                [
                        {“serial”:”1HGAF8723”, “Model”:”Cisco7567”, “lat”:”39.9526 N”,
                         “long”:”75.1652W”},

                        {“serial”:”45452BD23”, “Model”:”RuckusZD510”, “lat”:”39.9406 N”,
                        “long”:”75.1722W”},
                        // repeat as many as available….
                ],
                “radiotraffic”: {“datarate”:”500mbps”,”txbytes”:2338942334, “rxbytes”:3479832478},
                “channelmeasure”: {“rssi”:”-87dbm”, “noise”: -20},
                “txpower”: {“airquality”:7, “interferencepercent”:0.30, “clientcount”:60},
                “RFneighbor”: {“MAC”:”45:34:23:DF:12:C1”,“channel”:”6”, “channelwidth”:”20MHZ”,
                “avgrssi”:”-80dbm”},
        }
}
```


Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

- **Sample Post from Wi-Fi Monitoring system to the QoS Service Provider Framework with data objects (Posting occurs when monitored data is available)**

```
POST / QoSMonPost HTTP/1.1
Accept: application/json
Content-Type: application-json
Content-Length: ###
{
        "Wi-FiPerfPost:
        {
                "general":   {"SSID":"SP_Passpoint2"}, {"BSSID":"BB:34:6D:BC:78:A1"},
                "APgroup": {"PasspointGroup":"0", "WLC":"SP_WLC_2" ,  "submode":"modePP"},
                "generalpolicy": {ATF:"Wi-FiPPPolicy_3", AVCPolicy:"AVCPolicy_2"} ,
                "inventorylocation":
                [
                        {"serial":"1HGAF83JK3", "Model":"Aruba9345", "lat":"40.9526 N",
                        "long":"76.1652W"},
                        {"serial":"JSYU452BD23", "Model":"RuckusZD700", "lat":"40.9406 N",
                        "long":"76.1722W"},
                        // repeat as many as available.....
                ],
                "radiotraffic": {"datarate":"100mbps", "txbytes":234582334, "rxbytes":347122478},
                "channelmeasure": {"rssi":"-80dbm", "noise":-24},
                "txpower": {"airquality":7, "interferencepercent": 0.40, "clientcount": 50},
                "RFneighbor": {"MAC":"56:34:23:DD:12:C1","channel": 1, "channelwidth": "20MHZ",
                "avgrssi": "-70dbm"},
        }
}
```

3.2.3 Monitoring Data About Wi-Fi Devices

In addition to monitoring and reporting of Wi-Fi network access point performance, it is possible that the Wi-Fi network function can report performance of Wi-Fi devices associated with Wi-Fi APs. The following diagrams depict hierarchy of Wi-Fi devices and a few relevant performance data objects.

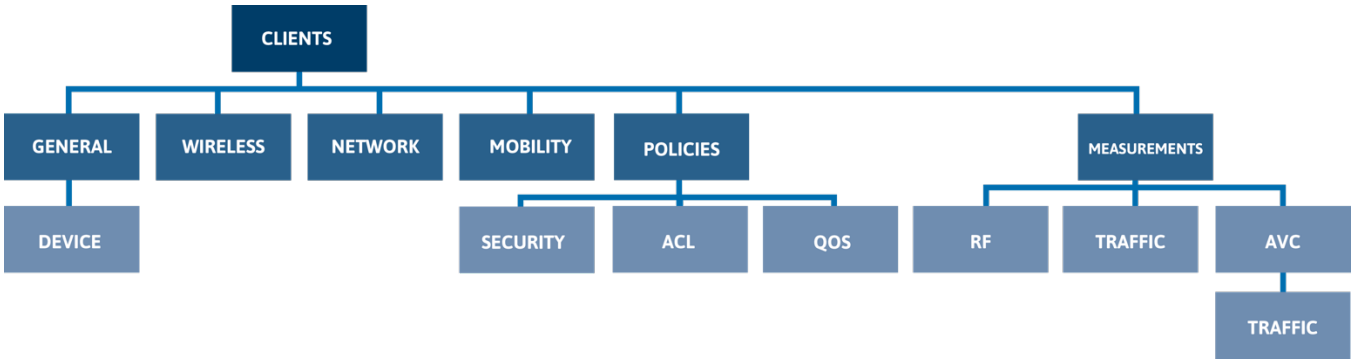


Figure 3-5 Hierarchy of monitoring data objects of Wi-Fi devices seen by the network

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

Client	MAC Address
General	State, Assoc Time, Username, CX info
Device	Hostname, Type, OS
Wireless	WLAN ID, AP MAC, Protocol, Client Retry Count
Network	IPv4, IPv6, VLAN
Mobility	Mobility Role
Policies – Security	Policy ID, Cipher, Key Management, EAP Type, AAA Role
Policies – ACL	IPv4, IPv6
Policies - QoS	Level, WMM, UAPSD, mDNS
Measurements - RF	SNR, RSSI, Spatial Stream, Speed
Measurements – Traffic	Rx Bytes, Tx Bytes
Measurements - AVC	Application ID, AVC Name Traffic – Rx Bytes, Tx Bytes

Figure 3-6 List of network data objects of Wi-Fi devices seen by the Wi-Fi network

- **API to Report Attached Device Wi-Fi Performance**
  - The API used to report Wi-Fi network monitoring data objects can be extended to include similar call and structures to report data objects of Wi-Fi devices seen associated with Wi-Fi AP.

```
POST / QoSMonPostWDevices HTTP/1.1
Accept: application/json
Content-Type: application-json
Content-Length: ###
{
    "Wi-FiPerfPostDev:
    {
        “general”:  {“SSID”:”SP_Passpoint2”, “BSSID”:”BB:34:6D:BC:78:A1”},
        “APgroup”: {”PasspointGroup”:”0”, “WLC”: ”SP_WLC_2”, “submode”: ”modePP”},
        “inventorylocation”:
        {“serial”:”1HGAF83JK3”, “Model”:”RuckusZD520”, “lat”:”40.9526 N”, “long”:”76.1652W”},
        “attacheddevices”:
        {
            {“hosttype” : ”iOS”, “OSver”:”9.0”,”MAC”:”AA:BD:89:34:5D:23”,
                “duration”:”0:15:20”, “Tx”:”23234534”, “Rx”:”2342384923”, “freq”:”5.0GHz”},
            {“hosttype” : ”Android”, “OSver”:”6.0.1”,”MAC”:”34:89:DE:78:AA:89”,
                “duration”:”0:60:00” , “Tx”:”23453454”, “Rx”:”23233244”, “freq”:”2.4GHz”},
            {“hosttype” : ”Android”, “OSver”:”7.0”,”MAC”:”AA:BB:76:89:A4:00”,
                “duration”:”1:34:45” , “Tx”:”1232311”, “Rx”:”45456456”, “freq”:”2.4GHz”},
            {“hosttype” : ”WINS10”, “OSver”:”1.1”,”MAC”:”34:89:65:23:AB:78”,
                “duration”:”2:30:15” , “Tx”:”1231234”, “Rx”:”343345545”, “freq”:”5.0GHz”}
        }
    }
}
```


Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

- **Sample Request from QoS Service Provider Framework to the Wi-Fi Monitoring system to retrieve mobile device data objects**

```
POST / QoSMonDevReq HTTP/1.1
Accept: application/json
Content-Type: application-json
Content-Length: ###
{
    "DevParms":
    {
        "wireless": { "APMAC":"AA:34:2C:BC:78:A1", "WLC":"SP_HotspotID"},
        "device": [{"hosttype":"iOS"}, {"hosttype":"Android"}],
        // Request Wi-Fi system to report all iOS and Android devices
        // served by an access point identified by its
        // MAC=AA:34:2C:BC:78:A1", and SSID = SP_HotspotID
    }
}
```

3.3 Metrics of Key Network Elements

Besides capturing the key QoS metrics values from the network gears and mobile devices to derive KPI, the service provider usually includes many other network elements in its network to support overall operation, such as authentication service, IP address assignment, domain name resolution, on-line signup portal access, secure gateway to connect with access points and controllers, and so forth.

Table 4-2 summarizes a potential list of all network elements and their target metrics to be collected and reported into the QoS Service Provider Framework to help generate service provider KPIs.

WI-FI VENUE COMPONENTS	CAPABILITIES TO TRACK	METRICS TO TRACK
Access Point	• Poor RF • Large Retry counter • Too many Clients • High Noise and/or High Interference on AP on 2.4 or 5 GHz bans • DFS Events	• Check the RSSI value on the clients and within limits for proper connectivity • Check packet retries on the client • Check if there are too many clients connected on one AP, check AP density and deployment • Check High co-channel interference on the Access Point on both bands • Track too many DFS events
Wireless LAN Controller	• High CPU • High memory utilization	• Track more than 60 % CPU utilization • Track more than 60 % memory utilization
Radius Server	• AAA failure or slow AAA 802.1x failure • Wrong password	• Track more than 10 % failure in 802.1x auth failure • Track more than 10 % failure on password authentication failure
DNS	• Unreachable DNS • Slow DNS	• Track DNS query failure, alarm above 2-3 % failure • Track DNS response, anything above 20-30 msec time should be tracked
ANQP server	• Service not available	• Track ANQP server response, anything above 20 msec should generate alarm
DHCP server	• IP address exhaustion • DHCP client interop issues	• Track IP address assignment/reply from DHCP server • DHCP offer not received by client
Gateway Reachability	• Default Gateway Reachability issues	• PING, traceroute default gateway periodically to see if they are up and available
OSU Server	• Check if the profile is available • Check if policy is available	• Check https response for profile • Check https response for profile • Access and response time limits

Table 3-2 List of network elements and needed metrics

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

4 QoS Architectural models

The following sections describe two complementary architectural models to provide and manage Carrier Wi-Fi QoS services.

- **Service flow prioritization model**
  - The service flow prioritization model provides real time traffic management and prioritization of IP traffic. In this model, associated Wi-Fi clients are called QoS consumers while all the other networking functions (e.g. Access Points, Wi-Fi Access Gateways (WAG), WLAN controllers etc) are collectively called QoS actors.
  - An end-to-end coordination of QoS by the QoS actors and consumers can provide effective traffic management and prioritization capable of providing acceptable QoS that matches the expectation of the applications being used by the QoS consumer.
- **QoS Metrics Service Offering model**
  - The QoS service offering model identifies QoS metrics and defines how such metrics are processed by the system and discovered by the QoS Requestor. The QoS Requestor is defined to be mobile phone, tablet, laptop, mobile router, network management agent, and so forth. The QoS Requestor can retrieve such QoS metrics information prior to connection, during the connection, and on an ad-hoc as-needed basis over any network connection.
  - This QoS metrics service offering model proposes using standard based over-the-top communication mechanisms and protocols for ease of adoption, besides the proposed 802.11u/ANQP extension, to support discovery over any network transport, such as 3GPP, standard Wi-Fi and HS 2.0 Wi-Fi with ANQP/802.11u.

4.1 Service flow prioritization

4.1.1 Introduction

Carrier Wi-Fi networks are deployed in unlicensed band that are prone to interference. Interference from other users of the same unlicensed band such that 3rd party, un-coordinated access points can have negative impacts on Quality of experience of the user.

Hence the challenge is to provide real time traffic management and prioritization of IP traffic such that the end user can experience best possible quality of experience possible. Figure 4-1 shows the end to end QoS model for a carrier Wi-Fi network.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

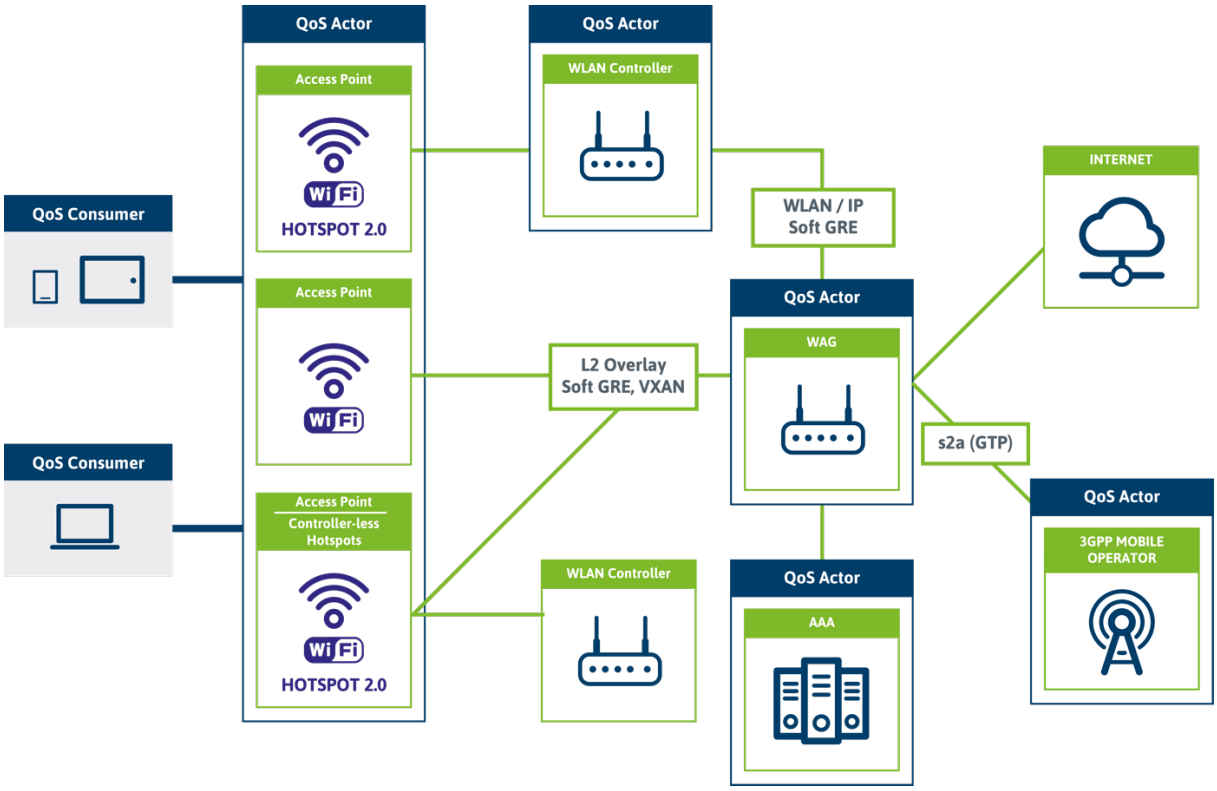


Figure 4-1 End-to-end QoS model

In such a model, associated Wi-Fi clients are called QoS consumers while all the other networking functions (e.g. Access Points, Wi-Fi Access Gateways (WAG), WLAN controllers etc) are collectively called QoS actors.

An end to end coordination of QoS by the QoS actors and consumers can provide effective traffic management and prioritization capable of providing acceptable QoS that matches the expectation of the applications being used by the QoS consumer (Wi-Fi clients).

Different QoS actors play different roles in QoS delivery. Wi-Fi devices are each responsible individually for access to the RF medium. Most widely used medium – or 'channel' – access is done via the Distributed Coordination Function (DCF) channel access rules that dictate use of the shared wireless channel resource, i.e., airtime.

DCF was designed to provide roughly equal channel access to all STAs in the network. Thus, assuming all Wi-Fi clients have the same physical layer rate, all clients get an equal opportunity to use the airtime.

Further, the physical layer rate used by a Wi-Fi client determines the amount of time the client will hold the shared channel once it gets access. For example, a client sending a maximum size data frame takes 9.8 ms of airtime at a physical layer rate of 6.5 Mbps (MCS 0) versus just 0.55 ms at 130 Mbps (MCS 15). This means a client at the edge of AP coverage and that can only achieve a maximum of MCS 0 link, will use approximately 20 times the airtime of a client that is in close proximity of the AP that can achieve a MCS 15, thus lowering cell throughput collectively for all the clients.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

Thus, Wi-Fi APs can provide much more effective QoS if it can optimize air time scheduling by considering application requirements based on combining metrics like client location and service classification.

4.1.2 Service Classification

Service classification usually requires deep packet analysis techniques which are computationally expensive. Wi-Fi APs are computationally constrained to perform such functions whereas abundant computational resources are available in the core network.

QoS actors in the core network e.g. WAG (Wi-Fi Access Gateway) or WLAN Controllers that provide IP subscriber management are capable of providing application detection and service classification capabilities. Also, 3GPP QoS enforcement points such as the ePDG can infer service classification from the received QoS control settings.

Once IP service flows are classified, such information can be provided to the Wi-Fi APs via DSCP marking using methods described in RFC 2474 [6] & RFC 2475 [7].

Wi-Fi APs can use the DSCP values as marked by the core network to provide appropriate channel access timing and thus control the QoS for downstream packets sent to Wi-Fi clients.

Figure 4-2 shows a deployment example where the ePDG sets the DSCP value in the outer layer-3 header of downstream packets based on 3GPP QoS control information it received during bearer channel establishment. The AP uses the received DSCP value to apply the correct level of QoS as described above. One problem with this QoS mechanism is that the IP network between the ePDG and the AP may modify the DSPC values (say, an untrusted IP network that is managed by some 3rd party provider). Obviously changing the DSCP values en-route between the ePDG and AP would beak the mechanism.

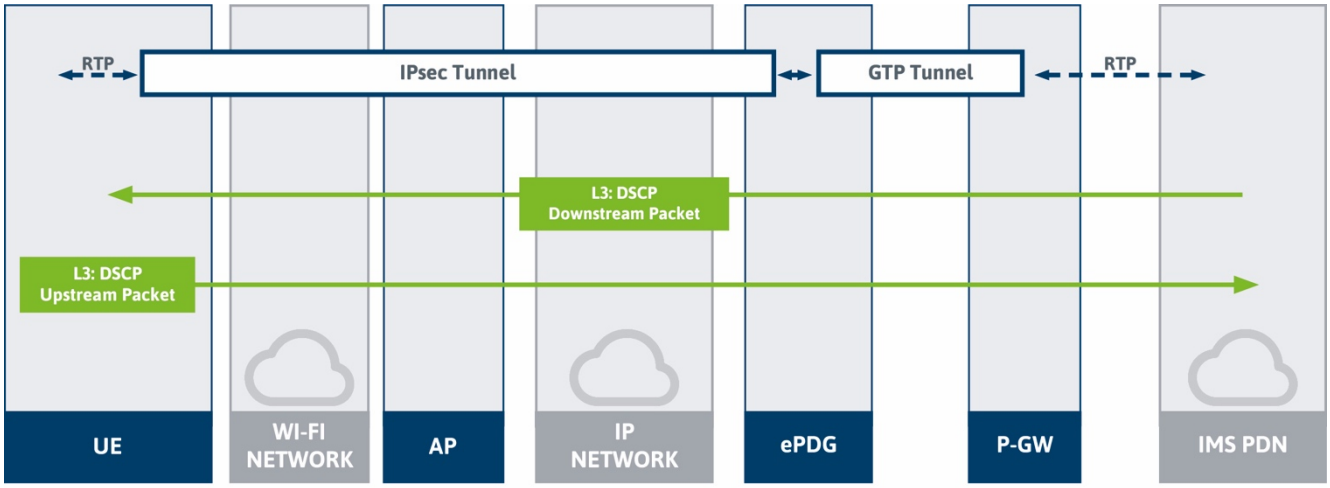


Figure 4-2 Controlling downstream QoS over Wi-Fi using DSCP

Wi-Fi clients can perform a similar mechanism internally, where applications running in the client set the DSCP value to indicate the traffic classification level to the client's Wi-Fi subsystem. The Wi-Fi subsystem uses the DSCP value or other internal signalling received from the client application to control channel access timing, thus providing the correct level of QoS for upstream packets sent to the AP.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

The Wi-Fi Alliance's Wi-Fi Multimedia (WMM) [2][3] allows for the creation of multiple Access Categories that are generally mapped to specific application types: Voice, Video, Best Effort, Background. Based on traffic class provided by the core network to the AP, or provided by the application to the client's WLAN stack (and based on WMM capabilities) the respective device can provide dynamic adjustment of the WMM channel access parameters, e.g., AIFS & CWmin, and can thus be used to provide differentiated services over the airlink.

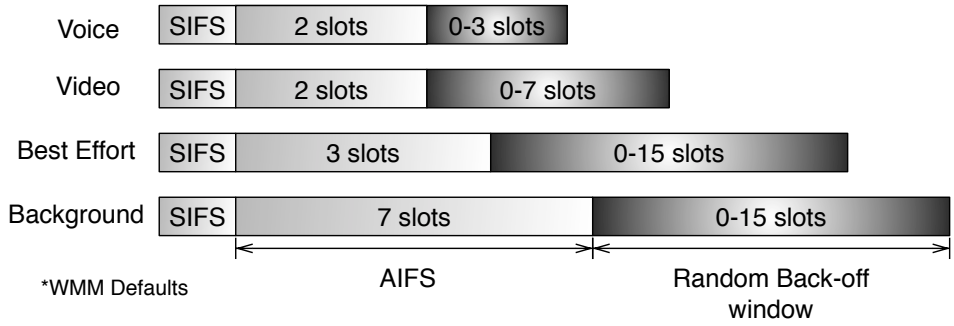


Figure 4-3 WMM Access Categories and back-off slots

The Wi-Fi Alliance WMM Technical Specification [3] also includes the WMM-Admission Control (WMM-AC) facility. WMM-AC it targeted to voice, video and other real-time media flows. It allows an AP to manage the available bandwidth, and prevent oversubscription of the high priority Access Categories.

NOTE – WMM also defines a facility called WMM Power Save (WMM-PS). WMM-PS is a method that allows client devices control over when the AP transmit frames toward the client, which in turn allows the client to save power by idling between frames. As such, it is not directly a QoS facility. However, some clients also use this facility to be able to schedule such things as background scanning, and mitigate interference from co-located radios such as Bluetooth. In this way, WMM-PS provides an indirect benefit to QoS, by generally increasing link quality with minimal disruption.

4.2 QoS Metrics Service Offering

This section describes the overall QoS service offering which covers the reference architecture, protocols, capability levels, and discovery to such services.

The QoS service offering framework should identify QoS metrics and define how such metrics can be accessed by the QoS consumers. The QoS consumer, hereafter referred to as the QoS Requestor, such as mobile phone, tablet, laptop, mobile router, network management agent, and so forth, can retrieve such information prior to connection, during the connection, and on an ad-hoc basis.

The QoS service offering architecture is recommended to include the following pillars or layers:

- QoS Requestor
- QoS API Specification
- QoS Provider
- QoS Provider Service Framework

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

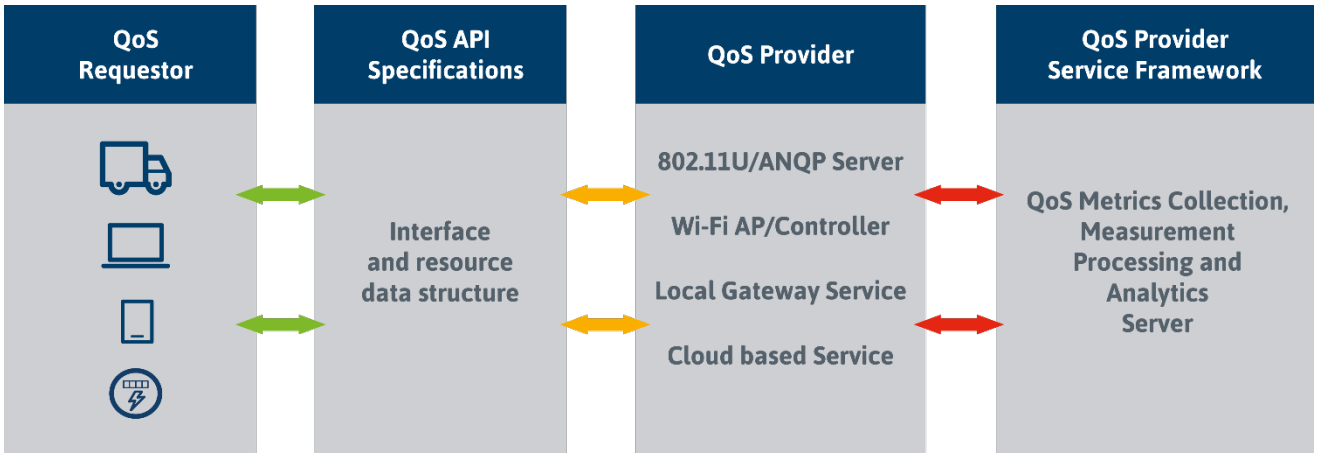


Figure 4-4 QoS service offering architecture

The QoS Requestor and the QoS Provider communicate via the QoS API interface and supported protocols which are recommended in the following sections.

The QoS Provider and the QoS Provider Service Framework communicate via an internal interface and supported protocols which are to be defined in the future section.

4.2.1 QoS Requestor Layer

The QoS Requestor is the consumer or user of the QoS metrics. The requesting device or application should discover for the availability of the QoS service, available protocols, and API versions before issuing a request.

The QoS API can provide more than one specifications for the supported QoS data. The QoS Requestor should discover and select an appropriate protocol and API version to facilitate efficient and secure retrieval of QoS metrics data.

It is feasible that the QoS request and processing can be in the form of:

- Request-Response
- Request-Callback-Response

With the Request-Response approach, the QoS Requestor sends a request in synchronous mode and will typically retrieve QoS response data in the same operation with minimal delay.

With the Request-CallBack-Response approach, the QoS Requestor sends a request and resumes its own operation. When the QoS Provider can provide the QoS metrics data, it will call back the QoS Requestor's specified call-back interface to forward the result or alert the QoS Request to retrieve the result.

The API Specification level should allow the CallBack API be included as part of the request to the QoS Provider. Defining QoS Requestor's interface is considered out of the scope of this whitepaper.

The QoS Requestor shall be able to discover the QoS Provider entity and the protocols it supports. For example, the QoS Requestor discovers whether there is support for QoS in the Wi-Fi network and whether the OMA DM protocol is implemented by the QoS

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

Provider; the QoS Provider should respond with a confirmation for QoS service availability and whether the OMA DM protocol is supported, and the supported protocol or API versions.

Table 4-1 depicts possible discovery of QoS services and supported protocols for use by the QoS Requestor.

DISCOVERY TYPE	PROTOCOL & SUPPORT	COMMENTS
Discovery for QoS Provider presence and supported protocols	ANQP, DHCP, and HTTPS/HTTP, or specific TCP/UDP port	Use ANQP to probe or listen to beacon Use DHCP to look for a particular field Use HTTP/HTTPS to probe a URL for a standard response code or message field Use socket communication to obtain a standard response code or message field.
Discovery for Protocol Type 1	ANQP	Discover if QoS fields are available via ANQP using one of the Discovery protocols recommended above.
Discovery for Protocol Type 2	RESTful	Discover if QoS fields are available via RESTful method using one of the Discovery protocols recommended above.
Discovery for Protocol Type 3	SOAP	Discover if QoS fields are available via SOAP method using one of the Discovery protocols recommended above.
Discovery for Protocol Type 4	OMA DM	Discover if QoS fields are available via OMA DM method using one of the Discovery protocols recommended above.
Discovery for Protocol Type 5	LWM2M	Discover if QoS fields are available via LWM2M method using one of the Discovery protocols recommended above.
Discovery for Protocol Type 6	DHCP	Discover if QoS fields are available via DHCP using one of the Discovery protocols recommended above.
Discovery for Protocol Type 7	DSCP	Discover if DSCP is supported by the AP / QoS Provider using one of the Discovery protocols recommended above.
Discovery for Protocol Type 8	WMM	Discover if 802.11e is supported by the AP/ QoS Provider using one of the Discovery protocols recommended above.
Discovery for Protocol Type N > 8	For future use	

Table 4-1 Possible discovery types

4.2.2 QoS API Specification Layer

The QoS service interface should include at least the following definitions, collectively referred as QoS API specifications:

- Data handshake and protocol
- Exchange format
- States
- Data structure

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

The QoS API Specification should use, as much as possible, best practices and protocols that have been adopted by the Wi-Fi Alliance, OMA DM, IEEE, and W3 technical specifications. The QoS API and/or its related data structures should be defined to support the following protocols:

- GAS/ANQP for HS 2.0
- DHCP
- WMM
- RESTful with XML/JSON structure
- SOAP with XML structure
- OMA DM with XML management object
- LWM2M with XML/TLV management object

The QoS API shall support access to the QoS services via protocols operating at the Wi-Fi network level (such as 802.11e, 802.11u, ANQP/GAS) and at the TCP/UDP/IP based levels, such as HTTPS, DHCP and so forth.

Any QoS Requestor should be allowed to utilize such API to discover for QoS services and supported protocols before making a connection or during a Wi-Fi connection to the Wi-Fi network.

The QoS API, when defined, should recommend proper usage of the interface for implementation by ecosystem vendors and service providers.

4.3 QoS Provider Layer

The QoS Provider can be a hardware or software entity or both that expose and support the API, and can function as one or more of the following entities:

- A Wi-Fi Access Point (possibly with Controller/Gateway) with basic 802.11 protocol, enhanced WMM QoS protocol, and HS 2.0 802.11u/ANQP discovery probe and beacon capabilities
- A Wi-Fi Access Point (possibly with Controller/Gateway) with DHCP custom field generation and DSCP prioritized traffic marking.
- Local or remote gateway with support for TCP/UDP/IP and higher level protocols such as HTTPS/DTLS/LWM2M/REST/SOAP protocols to transport QoS fields.

It is recommended that the QoS capabilities be established and grouped in levels to describe their evolution and to facilitate their discovery and support.

The following initial 4 levels are recommended to be established to show increments of QoS services to be made available by the Wi-Fi infrastructure, such as at the Wi-Fi access points/controller, local software entity or remote web software entity.

The QoS Requestor shall independently be able to discover QoS services and protocols supported by the QoS Provider layer. The discovery process should allow one or more supported protocols be discovered along with pertinent API type, versions and baseline information as described in the QoS Requestor section.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

This section defines the recommended capabilities to support functions defined for the QoS Provider functions. It is expected that that these protocols will not be able to support function parity across all protocol types (i.e. same QoS API or data fields may not available in all supported protocols), the following grouping suggests multiple levels of implementation as part of the QoS Provider layer.

- **Level 1** – This level is recommended to support QoS discovery via the HS 2.0 ANQP protocol alone. This level depends on successful collaboration with the Wi-Fi Alliance to expand the ANQP protocol to include applicable QoS fields. If the Level 1 functions support only a subset of the QoS fields that are fully available in other protocols, it is recommended that the Level 2 capability or higher be established by the QoS Provider layer to support additional capabilities.
- **Level 2** – This level is recommended to offer full QoS services data fields using the RESTful protocol, to augment the ANQP protocol which may provide partial QoS support. Level 2 provides the advantages of supporting HS 2.0 and non-HS 2.0 devices, and when a full set of QoS fields cannot be included or implemented in the ANQP.
- **Level 3** – In this level, Level 2's functions are expanded to support additional protocols. The Level 3 supports a more diverse population of devices. It is also expected that different protocols will require different security enforcement or the provisioning steps required by the standards. For example: for RESTful and SOAP protocol support, a secure HTTPS session should be established with a web server whose digital certificate has been signed by a trusted certificate authority. While, with the OMA DM protocol for use by a 3GPP compliant mobile device, the HTTPS secure session can be similarly established to securely transfer QoS management objects, but the QoS Requestor device and the OMA DM server should previously have mutually authenticated as part of the bootstrap process to allow the mobile device to receive QoS management objects/QoS data fields.
- **Level 4** – Level 4 offers additional methods for QoS services. Additional protocols such as LWM2M, DHCP, 802.11e and DSCP provide specific transport format. Constrained devices with limited processing ability is recommended to use a lighter protocol such as LWM2M in lieu of the session oriented protocols such as RESTful/SOAP/HTTPS. The DHCP protocol takes advantage of custom fields to carry a small amount of fields but may lack dynamic QoS values over time, while the 802.11e and DSCP marking depends on the QoS Requestor and the QoS Provider's compliance to the basic Wi-Fi and IP networking to take advantage of prioritized traffic handling.

CAPABILITIES	QOS PROVIDER	QOS PROVIDER SERVICE FRAMEWORK
Level 1- NGH/Wi-Fi HS 2.0	GAS/ANQP for HS 2.0	Passive, active monitoring and reporting Algorithm to combine QoS data and convert to usable data structure Back end server and DB
Level 2 – Wi-Fi, NG Wi-Fi HS 2.0 and OTT API access	GAS/ANQP for HS 2.0 RESTful with XML/JSON SOAP with XML	Above, plus basic encoding / decoding/translation function of services. Optional improvement of QoS analytics to improve service

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

Level 3 – Wi-Fi, HS 2.0, local / remote API access, multiple exchange formats	**GAS/ANQP for HS 2.0 RESTful with XML/JSON SOAP with XML OMA DM with SYNCML/XML management object LWM2M with device / Gateway JSON/TLV**	**Above, plus: Optional improvement of QoS analytics to improve service Optional local and remote service framework deployment**
Level 4 – Wi-Fi, HS 2.0, local / API access, multiple exchange formats, enhanced Wi-Fi QOS	**GAS/ANQP for HS 2.0 DHCP, 802.11e, DSCP RESTful with XML/JSON SOAP with XML OMA DM with XML management object defined LWM2M with device / Gateway JSON/TLV**	**Above, plus: Policy definition to support DHCP customer fields and DSCP marking**

Note**: highlighted text** in column 2 indicates recommended minimum capabilities for each level

Table 4-2 Summary recommended Levels of QoS service

4.3.1 QoS Provider Service Framework Layer

The QoS Provider layer is recommended to be the entity to offer QoS services to the QoS Requestor, while the QoS Provider Service Framework layer is the companion entity to process network performance data to provide QoS metrics to the QoS Provider layer.

The preliminary architecture depicted in Figure 4-4 above serves as a model to define such services, and to facilitate implementation, deployment, improvement and management by the service provider, enterprises and ecosystem players.

The QoS Provider layer should support dynamic QoS data field updates to allow the requesting devices to consume most current QoS metrics data and as often as possibly can be provided.

The QoS Provider layer may choose to provide an optional API, referred herein as Device QoS reporting API, as a method for the QoS Requestor to report Wi-Fi network experience, performance and perception, allowing the QoS Provider and the Service Framework layers to improve their QoS discovery support. This QoS reporting API should be defined to support both near-real time reporting and deferred reporting (aka batch reporting) depending on the data types to be used to improve overall freshness and quality of QoS discovery data.

For example:

- Near real time reporting use case: The QoS Requestor retrieves QoS data and identifies that the QoS Provider supports throughput and latency robust enough for a Wi-Fi Calling session, however, if during the Wi-Fi Calling session, the device experiences call drop or echo, the QoS Requestor can access this optional QoS reporting API to report such experience and perceived performance to the QoS Provider Layer for later processing (possibly by the QoS Provider Service Framework layer).
- Deferred reporting use case: The QoS Requestor discovers and retrieves QoS metrics for Wi-Fi network. It later connects to one of the Wi-Fi access points and continues to stay connected for a long while because the access point provides high quality connection. The device can occasionally measure Wi-Fi performance and saves in a local file until the specific time or file size condition changes to trigger an event to

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

send a group of device analytics records over the QoS reporting API to the QoS Provider component and QoS Provider Service Framework components.

The QoS Provider Service Framework layer should implement robust algorithms, flexible storage, secure data access control, and horizontally scalable services for access by a large number of devices.

The QoS analytics algorithms should facilitate processing of Wi-Fi performance data by dimensions such as time, date, device categories, and other Wi-Fi performance categories, to accurately quantify QoS metrics or predict how QoS metrics may evolve based on historical data.

The robust storage requirement of the QoS Provider Service Framework component should provide large scale storage, storage redundancy, access protection and manipulation of data to support the QoS Provider layer needs.

5 Metrics database and reporting

The QoS Provider Service Framework component should provide functions to process data feeds, store unstructured and structured data, organize data for access, analyse data per business rules, create network QoS knowledge, and publish such knowledge for actions.

The published knowledge can represent network KPIs and QoS metrics for viewing and processing requests from the QoS Provider component. These operations can be grouped in the following three layers:

1) Service layer
2) Analytics and knowledge layer
3) Collection and organization layer

Figure 5-1 depicts functional layers within the QoS Provider Service Framework.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

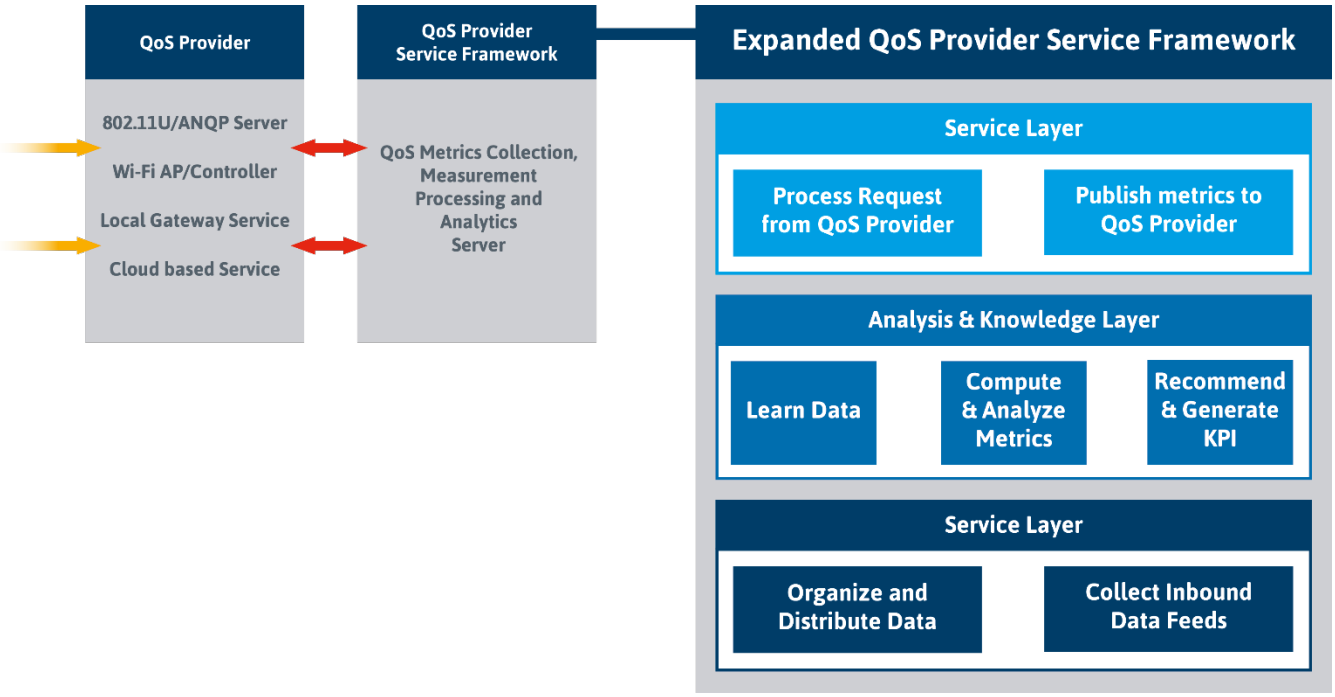


Figure 5-1 expanded view of the QoS Provider Service Framework

5.1 Service layer

The Service layer provides web services to process requests for new or updated QoS metrics measurements. This Service layer should process requests from and post data to the QoS Provider component asynchronously to improve its performance. The Service layer may choose to support processing of requests and posting synchronously if desired or in scenarios when request or posting traffic load is light.

This layer should interface with the QoS Provider to process requests and to post metrics results.

The QoS Provider can send request to this Service layer to retrieve data to refresh its storage or cache. The Service layer can also process device's request for immediate processing if the cache requires a refresh or the QoS provider allows pass-through processing of device requests.

The Service layer can post QoS metrics to the QoS Provider when there is new information to be made available from the Analysis and Knowledge layer.

The QoS request and response should contain JSON payload for RESTful calls and XML payload for SOAP calls to simply parsing.

This architecture recommends the use of HTTPS protocol with optional validation of server digital certificate to ensure the secure tunnel is established with the correct server destination.

Refer to section 6 for security recommendations.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

5.2 Analysis and Knowledge layer

The Analysis and Knowledge layer functions as the computation engine to produce various network QoS and performance metrics.

This function of this component can vary depending on various network feeds that are needed for the computation and production of network QoS metrics to be effective. Network feeds can consist of historical and up-to-date performance data collected from Wi-Fi access points, Wi-Fi controllers, wireless gateways, backhaul capability, loading, downlink throughput, uplink throughput, traffic latency, device reported Wi-Fi performance, date, time, and location of deployment.

This layer at the minimum should consist of the following functions:

- Data learning - This function represents preparatory functions to enable the algorithms in the machine learning subcomponent to recognize new data values, adapt to metrics values reported by devices and network feed, and work toward certain expected results.
- Machine learning - This function continuously computes and analyses QoS related and environmental data points from devices and network feeds to discover, estimate, validate, correlate, aggregate, model, predict and generate needed network knowledge; for example, Wi-Fi network QoS metrics, peak-hour expected loading, daily average throughput, Wi-Fi network health indicators, and access point replacement recommendation and so forth. This component should consist of statistical, special or heuristic algorithms to meet service provider Wi-Fi operations.
- Recommendation & KPI report generation - This function enables data mining, reporting, extraction, recommendation, and visualization of various networking performance indicators as feedback for consumption by network administrators and the Service layer. The recommendation output can facilitate immediate actions such as alerting or posting to updated actions and data to the QoS Provider component, while the KPI report can be in a form of graphs, charts and aggregated data dashboard display of the Wi-Fi network performance and health.

5.3 Collection and organization layer

This component manages and protects raw and processed data in various formats for use by the Analysis & Knowledge and Service layers.

This layer at the minimum should consist of the following functions:

- Collect inbound data feeds – this function is an important step in the process of obtaining device, field and network data points (which can be unstructured, loosely coupled, or unrelated) and organize them for processing. Processing can be immediate or deferred actions to meet the need of providing network QoS metrics to devices or network administrators in a timely or cost effectively manner.
- Organize and distribution – this function optimizes large scale data access, manipulation, search, distribution, and replication using appropriate data architecture models to meet the need of the service and analysis and knowledge layers. This functional subcomponent should leverage tools and networking

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

services to provide distributed storage system, in-memory caching, SQL relational database, NOSQL data base, graph data base, cross-regional replication and inter-service data exchange formats. This function should be designed to minimize I/O latency that are normally associated with external storage devices and network accesses. This function should be designed to contain both historical and current-state data records to support machine learning and data management functions of the above layers.

5.4 Wi-Fi Monitored Data Reporting Interface

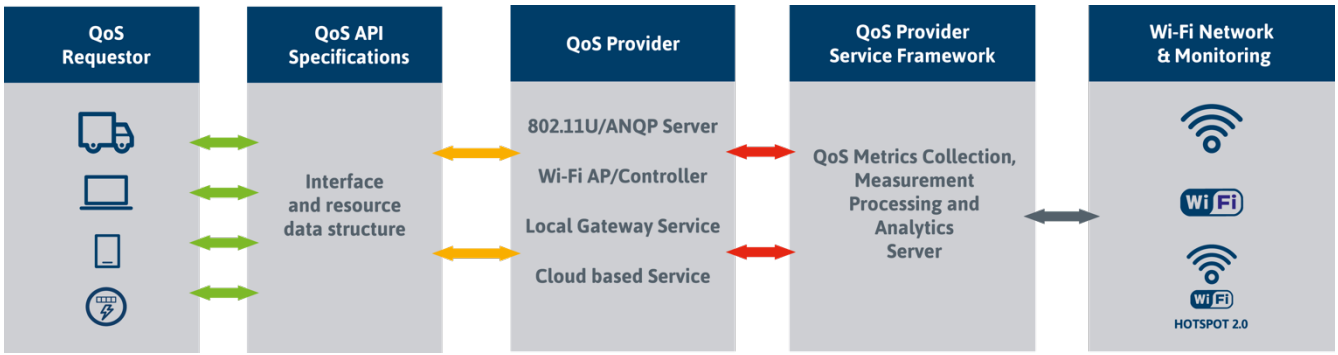


Figure 5-2 Remote Wi-Fi network monitoring and interface with the QoS Provider Service Framework

The QoS Provider Service Framework contains a Metrics Server that collects raw metrics from Wi-Fi network entities, and applies processing on the collected raw metrics in order to produce a set of well-defined metrics that accurately describe the overall health and capabilities of the Wi-Fi network. Optionally, more advanced analytics may also be applied to the gathered metrics, to spot patterns and trends, and other high-level observations from the data; this is out of scope of this whitepaper.

To produce usable QoS metrics as a result of collection and computation of data from multiple feeds, it is necessary to provide a portable interface to post monitored data collected from the Wi-Fi network to the QoS Provider Service Framework. This Wi-Fi monitored data reporting interface should be abstracted and extensible to allow the Wi-Fi monitoring functions, which are expected to be diverse among Wi-Fi infrastructure vendors, to post needed raw performance data.

This interface needs to be very robust to accommodate frequent streams of data posting from a potentially large number of Wi-Fi nodes consisting of Wi-Fi access points, controllers and wireless gateways. This interface should be implemented as a horizontally scalable web service by a group of servers capable of filtering, dispatching, streaming, and storing data for immediate or batch processing.

The inbound data feed function of this interface should ingest inbound data on an as-needed basis from the monitoring component described in section 3.2above. Data ingestion operation should be performed in near real time, whenever possible, to support data analysis and QoS metrics update posting.

Due to the distributed architecture design for the QoS Metrics Service framework, it is recommended that this monitored data reporting web service should be designed as secure web and file services. However, if the remote Wi-Fi monitoring systems coexist in the same service provider secure intranet or in the same virtual private cloud environment, the web

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

and file services can rely on the internal network security already in place to protect traffic while in transit.

- Web call function and interface - this function is recommended to use web REST protocol with JSON formatted payload to accommodate a variety of field and value definition. This format provides attribute-value pairs and structured data objects to be transmitted or converted prior to consumption. This component can optionally provide an interface in SOAP web protocol and XML formatted payload if needed.
- File posting function and interface – this function should allow the remote monitoring system to post a file containing monitored data elements, and should support the HTTP multi-part / resumable protocol or the FTP protocol. It is also possible that the service provider or implementer can substitute the native HTTP and FTP protocols with other commercial or open source solutions that can provide similar file upload and resumable operation in the event of network disconnection; it is outside the scope of this whitepaper to recommend commercial or open source solutions to support file transfer or file upload with resumable capability.

6 Security

This section describes security requirements and recommendations for QoS service discovery, delivery and collection. This section does not describe capabilities for protection of data at rest or within the hardware and software environment to be implemented by service providers and vendors.

6.1 Security Purpose by Component

The Carrier Wi-Fi QoS service should be architected to allow secure and unsecure access to the QoS Provider gateway facing the QoS Requestors such as mobile devices, laptops and constrained IoT devices.

Secure access provides authentication, integrity and confidentiality of requests and responses. Unsecure access provides discovery of QoS metrics only in the event for devices can only leverage standard protocol such as ANQP/GAS. It is not recommended to provide unsecure access to and from the QoS Provider other than using ANQP/GAS protocol.

This QoS section recommends security practices as well as promote improved ANQP/GAS security through future liaison with the Wi-Fi Alliance or IEEE standard bodies.

This section recommends security that can be implemented today with future improvement path. As the security process changes, so are the algorithms and processes used to support such security profile.

The general security objectives for each component are summarized below:

- QoS Provider: This component, represented by Wi-Fi access point, ANQP server, remote web gateway, and local LAN gateway, should support at the minimum: ANQP/GAS, HTTPS, device authentication, user authentication, digital certificate based validation, key generation, and cryptographic algorithms. Note: IoT constrained devices may leverage DTLS due to efficiency reason, it is possible to have QoS Provider supports DTLS protocol between the QoS Requestor and QoS Provider.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

- QoS Requestor: This component, represented by various devices with diverse security protocols and functions, should support at the minimum: ANQP/GAS, HTTPS, optional DTLS (TLS over Datagram), gateway authentication, digital certificate based validation, key generation, and cryptographic algorithms.
- Interface & resource data structure: This component, represented by API convention and payload being transmitted between the QoS Requestor and the QoS Provider, should be protected by a secure session between the QoS Requestor and the QoS Provider component. However, the QoS Requestor device may transmit contents to the nearest gateway to be forwarded to the final destination for device analytics reporting, it is recommended that the payload in this interface should be further protected with signature and/or data encryption depending on the requirements defined by the QoS Provider or a visiting QoS Provider that receive such payload. If such payload level protection is needed, the device and the end service provider should utilize pre-shared key, dynamically generated key or public/private key method for use either as signing key or encryption / decryption key or both.
- QoS Provider Service Framework: This component consists of several functions for use with north bound and south bound interfaces. Security implementation depends on the communication directions and with the intended entities (device – QoS Provider Service Framework, QoS Providers Service Framework – Wi-Fi Network Monitoring). This component should provide HTTPS, device authentication, digital certificate based validation, key generation, cryptographic algorithms, and virtual private tunnelling (VPN) or layer 2/3 tunnelling.

6.2 Interface Security

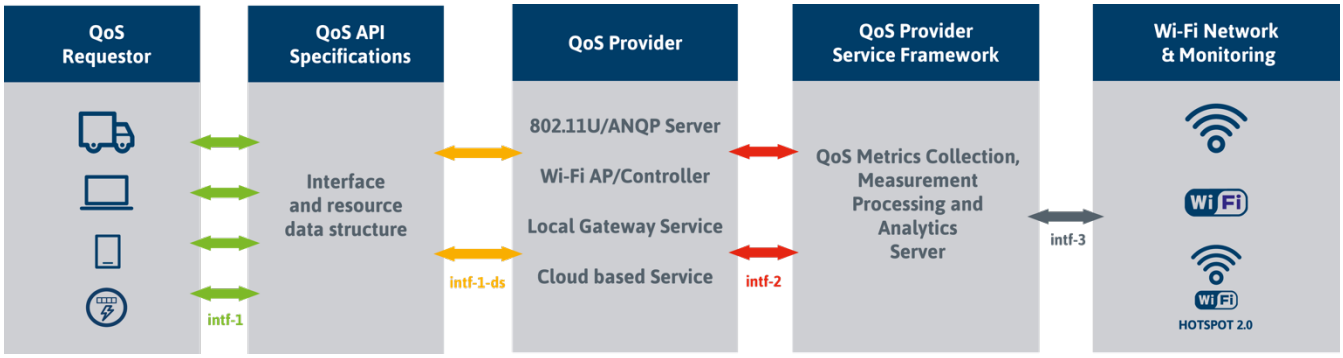


Figure 6-1 Security consideration for QoS services

The Wi-Fi QoS services should be architected to provide QOS metrics discovery and submission of device analytics to the QoS service system with simplicity to accommodate devices such as handset, laptop, appliances, and constrained internet of things devices with and without HS 2.0 capabilities. Security shall be implemented to support these operations, especially the communications flows (i.e. interface and data payload) between devices and network elements, as well as among internal network elements within the overall architecture.

Security implementation should be provided for the following interface and components:

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

INTERFACE	FUNCTION	PURPOSE	DESCRIPTION
Intf-1	Discovery Wi-Fi QoS	Enable devices to discover QoS before and during connections.	For Discovery - Use HTTPS with server certificate validation if possible, recommended certificate to be signed by one of the three recommended CA for HS 2.0 subscription management services.
Intf-1	Submit QoS from devices	Enable devices to submit QoS before and during connections	For analytics submission – device application and QoS Provider should mutually authenticate in advance if possible. Should support devices with Pre-Shared Key (PSK) or enforce API key/value for API POST/PUT call. Should allow support for OAuth authorization process to allow QoS Requestor to validate with name/password. Not recommend to allow non-authorized devices or applications to submit analytics.
Intf-1-ds	Authenticate QoS metrics data	Ensure data payload is protected to prevent tampering and confidentiality if needed	In event HTTPS is not established with server certificate validation, the payload should be validated using algorithm HMAC-SHA-1 when Pre-Shared Key (PSK) is provisioned
Intf-2	Refresh QoS metrics	Enable transport level security with authentication, confidentiality, integrity between components	Recommended to use VPN or layer 3 secure tunnelling in SP space or with trusted partners. Three other alternatives are acceptable depending on infrastructure deployments: a- HTTPS with mutual authentication of certificates between the QoS Provider and QoS Service Provider Framework for inter-SP b- Service access authentication using API with key / secret value for all calls c- Mutual challenge response during application session establishment.
Intf-3	Monitor and input network performance	Enable transport level or physical level security with authentication, confidentiality, integrity between components	Recommend to use VPN or layer 2/3 secure tunnelling in SP space or with trusted partners. Three other alternatives are acceptable depending on infrastructure deployments: a- HTTPS with mutual authentication of certificates between the QoS Provider and QoS Service Provider Framework for inter-SP b- Service access authentication using API with key / secret value for all calls Mutual challenge response during application session establishment.

Table 6-1 Security considerations for various interfaces

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

Annex A. Desired KPIs

The following lists some example Key Performance Indicators (KPIs) that can be produced from the QoS Provider Service Framework. These indicators can be used by the network provider for network performance monitoring and reporting, as described in section 3.2:

The frequency of measurement and reporting, and which element(s) in network should be responsible for each metric, is for further study. Also for further study is specification of which metrics should be mandatory, optional or highly-desirable, especially considering the applications in use such as voice or video versus various data services.

KPI	DEFINITION	MEASUREMENTS
WI-FI ACCESSIBILITY		
Wi-Fi Association Failure Rate	Measures the probability for an end-user to not successfully complete authentication and key management procedures	Unsuccessful attempts are compared with total attempts in percent
Wi-Fi Association Requests	Measures the volume of association requests on the network	
Wi-Fi Association Successes	Measures the volume of association successes on the network	
Wi-Fi Association Failures	Measures the volume of Association Failures on the network. Association failures include EAP authentication failures	

WI-FI CLIENT/USER		
Number of Unique Clients	Measures the number of unique client connected	
Number of Unique Users	Measures the number of unique users connected	
Number of Unique APs	Measures the number of unique APs connected	
Number of Sessions	Measure the number of sessions	
Average Connected Clients Per AP	Measures the average number of unique client connected per AP	
Average Connected Unique Users Per AP	Measures the average number of unique users connected per AP	
Total Session Time	Measure total session time	Hours
Average Session Time	Measures average session time	Minutes
Average Session Time Per User	Measures average session time per user	Minutes
Average Session Time Per Client	Measures average session time per client (Minutes)	Minutes

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

KPI	DEFINITION	MEASUREMENTS
WI-FI CLIENT TRAFFIC		
Wi-Fi DL Data Volume	Measures the downlink data volume on the network in MB (8,000,000 bits)	
Wi-Fi UL Data Volume	Measures the uplink data volume on the network in MB (8,000,000 bits)	
Wi-Fi DL Binary Data Volume	Measures the downlink data volume on the network in MB (8,388,608 bits)	
Wi-Fi UL Binary Data Volume	Measures the uplink data volume on the network in MB (8,388,608 bits)	
DL Maximum Data Rate	Measures the DL maximum throughput provided in Mbps (1,000,000 bits / second)	
UL Maximum Data Rate	Measures the UL maximum throughput provided in Mbps (1,000,000 bits / second)	
DL Minimum Data Rate	Measures the DL minimum throughput provided in Mbps (1,000,000 bits / second)	
UL Minimum Data Rate	Measures the UL minimum throughput provided in Mbps (1,000,000 bits / second)	
DL Average Data Rate	Measures the DL average throughput provided in Mbps (1,000,000 bits / second)	
UL Average Data Rate	Measures the UL average throughput provided in Mbps (1,000,000 bits / second)	
Number of authentication requests from clients	Measures number of authentication requests sent to a managed APs by clients	
Number of authentication requests sent by client	Measures number of authentication requests sent by client	
Number of authentication responses from a managed access point	Measures number of authentication responses sent to clients by a managed access point	
Number of authentication responses sent to a client	Measures number of authentication responses to a client sent by a managed access point	
Authentication Failure Rate	Measures the failure of the client(s) to successfully authenticate to the WLAN	

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

KPI	DEFINITION	MEASUREMENTS
WI-FI TRAFFIC BY PROTOCOL		
Percent of Sessions by Protocol	Measures the percent of sessions by protocol	%
Percent of Clients by Protocol	Measures the percent of clients by protocol	%
Percent of Users by Protocol	Measures the percent of users by protocol	%
Percent of Session Time by Protocol	Measures the percent of session time by protocol	%
Percent of Traffic by Protocol	Measures the percent of traffic by protocol	%

AVAILABILITY		
AP Total Unavailable Time	Measures the amount of time the cell is unavailable for network usage. AP unavailable time does include manual or automatic unavailable durations due to operator intervention or backhaul outages.	Seconds per Hour
AP Outside of maintenance Window (OMW) Availability	Measures the equipment availability for network usage. AP OMW availability is reflective of equipment power status and does not include manual or automatic unavailable durations due to operator intervention or backhaul outages. Available time is compared with total time for the reporting duration.	Hours
AP OMW Unavailable Time	Measures the amount of time the cell is unavailable for network usage. AP OMW Unavailable Time does not include manual or automatic unavailable durations due to operator intervention or backhaul outages.	Seconds/Hour

SUSTAINABILITY & QOS		
Number of all radio retry or retransmission attempts	Number of retransmitted WLAN RF frames divided by the number of all the frames sent to uplink in system level (All Aps)	
Number of AP radio retry or retransmission attempts	Number of retransmitted WLAN RF frames divided by the number of all the frames sent to uplink by an AP	
System Client radio retransmission rate	Measure the number of retransmitted frames divided by the number of all the frames sent to all AP uplink by a client	
AP Client radio retransmission rate	Measure the number of retransmitted frames divided by the number of all the frames sent to an AP uplink by a client	

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

KPI	DEFINITION	MEASUREMENTS
Downlink Jitter	Measures the downlink jitter for real-time services such as video and VoWiFi services	milliseconds
Uplink Jitter	Measures the uplink jitter for real-time services such as video and VoWiFi services	milliseconds
System Average Signal to noise ratio	Measures the average signal to noise ratio for all APs. This can be measured at APs, at some point away from APs, or both.	dB
AP Average Signal to noise ratio	Measures the average signal to noise ratio for each AP. This can be measured at AP, at some point away from AP, or both.	dB
AP Channel noise	Measures the average channel noise on the channel, per AP	dBm
AP beacon availability	Measures beacon signal transmission from each monitored AP. The KPI is the relative amount of received and expected beacons.	
Beacon traffic air time utilization	Measures beacon air time percentage of total air time	%
Radio channel congestion	Measures the utilizations of the AP channels	
Ping round-trip-time	Measures the round trip time between AP and server. The test pings a server N times with zero wait time between the pings. The default ping packet size is 32 kilobytes. The default ping count N is 10.	milliseconds
Handover success Rate between Aps on same system	Measure the handover success rate between APs on same system	%
AP Ethernet Port Utilization	Measures the Tx and Rx utilization of AP Ethernet ports	%
Client L2 Roaming Failure Rate between Aps	Measures the failure rate of the client(s) session to be successfully maintained during roaming event	
Layer 2 Retransmission Rate	Measures Layer 2 retransmissions rate	%
Packet Loss Rate (%)	Measures packets that are lost during transmission; important for APs running VoWiFi; generally measured on downlink	
Average Latency	Measure average latency (important for APs running VoWiFi)	milliseconds
Average Noise Level (noise floor)	Measures the average noise level	dB
Session (Connection) Drop Rate	Measures the failure rate of the client(s) to successfully maintain a session	%
Channel Utilization	Measures the channels utilization	%

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

REFERENCES

[1] IEEE Std 802.11-2016: https://standards.ieee.org/findstds/standard/802.11-2016.html

[2] W-Fi Alliance Wi-Fi Multimedia program: http://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm-programs

[3] Wi-Fi Alliance WMM Technical Specification: http://www.wi-fi.org/file/wmm-specification-v12

[4] Wi-Fi Alliance Hotspot 2.0 Technical Specification: http://www.wi-fi.org/file/hotspot-20-release-2-technical-specification-package-v110-0

[5] Wi-Fi Alliance Passpoint Program: http://www.wi-fi.org/discover-wi-fi/wi-fi-certified-passpoint

[6] IETF RFC 2474 (Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers): http://www.rfc-base.org/rfc-2474.html

[7] IETF RFC 2475 (An Architecture for Differentiated Services): http://www.rfc-base.org/rfc-2475.html

[8] IETF RFC 3550 (A Transport Protocol for Real-Time Applications): http://www.rfc-base.org/rfc-3550.html

[9] IETF RFC 3611 (RTP Control Protocol Extended Reports (RTCP XR)): http://www.rfc-base.org/rfc-3611.html

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

ACRONYMS AND ABBREVIATIONS

TERM OR ACRONYM	DEFINITION
3GPP	3rd Generation Partnership Project
802.11i	Protocol for air interface encryption referenced by HOTSPOT 2.0 specifications. Now part of IEEE Std 802.11-2012.
802.11u	IEEE standard ratified in 2010. Section of the IEEE 802.11u standard deals with automatic network discovery and selection and part of HOTSPOT 2.0 ANQP procedures. Now part of IEEE Std 802.11-2012.
802.1X	IEEE standard for network and subscriber authentication. Requires EAP-methods for authentication.
ANQP, GAS/ANQP	"Access Network Query Protocol " Part of the 802.11u IEEE standard referenced in the Passpoint™ specification used by the 2011 NGH Trials
AP	Access Point
API	Application Programming Interface
BSSID	Basic Service Set Identifier
DCF	Distributed Coordination Function
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DTLS	Datagram Transport Layer Security
HS 2.0	Hotspot 2.0 (HOTSPOT 2.0) [4] - A set of capabilities, including enhanced discovery that enable a 3G cellular or better experience for Wi-Fi users.
IoT	Internet of Things
KPI	Key Performance Indicator
LAN	Location Area Network
LWA	LTE-WLAN Aggregation
LWIP	LTE WLAN Radio Level Integration with IPsec Tunnel
MCS	Modulation and Coding Schemes
MSDU	Medium Access Control (MAC) Service Data Unit: Information that is delivered as a unit between MAC service access points (SAPs).
NAI	Network Access Identifier
Next Generation Hotspot (NGH)	Hotspot that implements Wi-Fi Alliance Passpoint™ technical specifications for Wi-Fi equipment. Detailed description is as follows: Next Generation Hotspot is a set of capabilities, including enhanced discovery and supporting seamless and secure Auto-Authentication by building on the Passpoint™ initiative setup by the Wi-Fi Alliance to deliver this common set of standards that would bring a 3G-like end-user experience to Wi-Fi authentication and roaming. In a WBA context we will be defining and testing operator requirements for NGH to support implementation of secure and seamless EAP based authentication to Wi-Fi in a "real world" environment (i.e. including but not limited to SIM)

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

OI	Organizational Identifier
OMA DM	Open Mobile Alliance (OMA) Device Management (DM)
ONU	Optical Network Unit
ORO	Optional Request Option
OTT	Over the top
Passpoint™	Program in the Wi-Fi Alliance to address Wi-Fi ease-of-use that will deliver HOTSPOT 2.0-certified equipment. See the HOTSPOT 2.0 specification [4].
PPDU	Physical Layer (PHY) Protocol Data Unit : The unit of data exchanged between two peer PHY entities to provide the PHY data service.
PSK	Pre-Shared Key
QoS	Quality of Service
REST, RESTful	Representational State Transfer
RSSI	Received Signal Strength Indicator
Rx	Receive/receiver
SHA-1	Secure Hash Algorithm 1
SNR	Signal Noise Ratio
SOAP	Simple Object Access Protocol
SP	Service Provider
SQL, NOSQL	Not Only Structured Query Language
SSID	Service Set Identifier
TLV	Type-Length-Value encoding style
Tx	Transmit/transmitter
UE	User Equipment
UL	Uplink
VoWiFi	Voice over Wi-Fi
WAG	Wi-Fi Access Gateway
WAN	Wide Area Network
WBA	Wireless Broadband Alliance
WFA	Wi-Fi Alliance
WFA MBO	Wi-Fi Alliance Multiband Operations program
Wi-Fi AN	Wi-Fi Access Network
WLAN	Wireless Local Area Network
WMM	W-Fi Alliance Wi-Fi Multimedia program [2] [3]
XML/JSON	eXtensible Markup Language / JavaScript Object Notation

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

EDITORIAL TEAM

NAME	ROLE	COMPANY
Kishore Raja	Project Leader & Editorial team member	Boingo Wireless
Mark Hamilton	Project Co-Leader & Chief editor	Ruckus Wireless
David Hancock	Editorial team member	CableLabs
Dzung Tran	Editorial team member	Smith Micro
Florin Baboescu	Editorial team member	Broadcom
Mike Parsel	Editorial team member	Sprint
Rajat Ghai	Editorial team member	Benu Networks
Bruno Tomas	Editorial team member	WBA

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

PARTICIPANT LIST

NAME	COMPANY
Thierry Van de Velde	Alcatel-Lucent
Peter Thornycroft	Aruba Networks
Rajat Ghai	Benu Networks
Jose Luis Esteban	Benu Networks
Kishore Raja	Boingo Wireless
Jeffrey Ziembicki	Boingo Wireless
Brian Shields	Boingo Wireless
Florin Baboescu	Broadcom
Michael Sym	BSG Wireless
Betty Cockrell	BSG Wireless
David Hancock	CableLabs
Umamaheswar Kakinada	Charter Communications
Sujit Ghosh	Cisco
Malcolm Smith	Cisco
Gaetan Feige	Cisco
Rodrigo Partearroyo	Fon
David Valerdi	Fon
Marco Spini	Huawei Technologies
Steve Namaseevayum	iPass
Stephen Kelly	Liberty Global
Rajesh Goyal	Nokia
Nigel Bird	Orange
Mark Hamilton	Ruckus Wireless
Kanwal Sangha	Shaw Communications
Chris Ratzlaff	Shaw Communications
Dzung Tran	Smith Micro Inc.
Sachin Saranathan	Spirent
Nick Baustert	Sprint

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2017 Wireless Broadband Alliance

PARTICIPANT LIST (CONTINUED)

NAME	COMPANY
Mike Parsel	Sprint
Ihab Guirguis	Sprint
Markus Wenzel	Syniverse Technologies
Srinivasa Rao	Tata Teleservices
Qiang Zhang	Time Warner Cable
Mick Conley	UL
Barbara Judge	UL
Tiago Rodrigues	WBA
Bruno Tomas	WBA

For other publications please visit:
wballiance.com/resources/wba-white-papers

To participate in future projects, please contact:
pmo@wballiance.com

READ MORE